Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

A Critical Review of Intrusion Detection Systems in WSN: Challenges & Future Directions

Navjot Kaur[1], Punam Rattan[2]

[1]Department of Computer Science & Engineering CT University, Ludhiana, Punjab, India.

E-mail: navkaurtoor@gmail.com

[2]Department of Computer Application CT University, Ludhiana, Punjab, India. E-mail: punamrattan@gmail.com

ABSTRACT

Since the last decade, with rapid advances in electronics and wireless communication technology, the landscape of wireless sensor network applications has grown to a giant scale. Wireless sensor networks have great potential to be employed in monitoring, tracking, and controlling applications; due to their distinct features such as self-organizing capability, fault tolerance, high sensing power, quick deployment, and less cost. Mission critical WSNs are deployed in inaccessible terrain and communicate over wireless channels, require effective and good security policy. Limited memory, processing power, and communication range are constraints of sensor nodes make prevention based security mechanisms like encryption and authentication technologies, firewall, and cryptography infeasible. As a result, the issue of how to secure such highly vulnerable sensor networks emerges. IDS come into prominence as a second line of defence for such issues. Keeping this in mind, a pervasive review is required to study various IDSs that have been proposed in recent years for WSN to highlight shortfalls they have along with the challenges in designing a lightweight IDS and solutions to set the future research directions in the field of IDS for WSN. Therefore, an extensive study is provided in this review paper into possible directions for future work in intrusion detection involving different aspects in sensor networks.

INDEX TERMS

Intrusion Detection, Wireless Sensor Networks, Security, Misuse-based Detection, Specification-based Detection, Reputation-based Detection.

Introduction

Wireless sensor networks (WSNs) are infrastructure-less wireless network consists of a few to hundreds or even thousands of interconnected sensor nodes to sense, collect, process and then communicate the information [1]. A sensor node is consists of memory, processor, storage, location finder, mobilizer, battery, and transceiver. All these units are not mandatory because Senor Networks primarily designed for a particular application [2]. WSNs had a wide range of application in various fields of science and technology, health care applications, commercial applications, to supervise ecological phenomena such as ocean water quality, pollution, earthquake, to monitor industrial sites such as industrial quality control, observation of critical infrastructure, and smart buildings, etc. [3], [4], [5], [6]. These networks have distinct features such as self-organizing capability, fault tolerance, high sensing power, quick deployment, and less cost [7]. Owing to these features, WSNs become more promising technology for mission-critical applications such as military surveillance, intelligent communication where sensor nodes are deployed in a hostile and unattended environment [8]. On the other hand, they have broadcast nature of communication with limited resources such as limited power supply, the low transmission bandwidth, small memory size and limited power which makes them more susceptible to various security attacks [9]. Security gap in the network would affect the overall performance of the system [10]. Nowadays timely prevention and detection of various attacks in wireless sensor networks has become an important area of research all over the world. For complete security of the network both prevention and detection based techniques have to work together. IDS planned for wired/ ad-hoc networks cannot be implemented completely to sensor networks due to its unique features [11]. In light of all these concerns, IDS should be robust enough to detect variety of known and unknown attacks in energy efficient manner before they cause damage to the whole network. Considering these reasons, various IDS have been developed for WSN in recent years. This paper is organized as follows: Section II Background of security in WSN. Section III gives brief description of the intrusion detection system and its techniques. Section IV presents an overview of the various existing intrusion detection system in WSN. Section V various challenges for the intrusion detection system. Section VI finally concludes the paper on the basis of the study.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

Background of Security in WSN

A. Security Attacks

In WSN, Security attacks are set of tactics that are used to cause damage to a network by exploiting flaws in it [12]. WSNs are vulnerable to a variety of security attacks. They are classified on the basis of different parameters as in [13], [14], [15] [16].

1. *Attack's Source:* According to attack's Source, they are classified as internal attacks and external attacks. In an external attack, the intruder node is not a legitimate sensor network member. The aim of this attack is to create network congestion, distribute incorrect routing information, or close the network entirely.
2. *Attack's Nature:* According to attack's nature, attack's can distinguish in active attacks and passive attacks. At- tacks against privacy like eavesdropping, traffic analysis is considered passive in nature because an unauthorized user listens and monitors the communication channel to collect information in these attacks. In active attacks, the unauthorized attacker monitor, listen and modify the data stream from the communication channel, Denial of service attacks, sinkhole attacks, node replication attacks, selective forwarding, etc. is all known as active attacks. These types of attacks are harder to detect.
3. *Attacker's Potential:* According to attacker's potential, attacks are classified in mote class attacks and laptop class attacks. In mote-class attacks, an adversary attacks a WSN with a few nodes that have equivalent capabilities to the network nodes while in laptop-class attacks, an adversary can target a WSN with more powerful machines such as a laptop, computer, etc.

B. Solutions to Security Attacks

In recent years, various security mechanisms have been proposed to recover and prevent different security attacks and these security mechanisms can be categorized as low-level and high-level mechanisms [17], [18], [19], [20], [21], [22].

1. A low-level mechanisms: A low-level mechanisms or prevention based techniques such as Authentication, encryption, and firewalls are primarily used to prevent any attack before it happen. Intrusion prevention techniques are capable of protecting WSNs against external attacks but are unable to detect internal attacks and act as the first level of defence. If authorized network members become Intruders, intrusion prevention systems cannot stop them and they can easily by-pass these traditional techniques. Attackers always try to launch new attacks unknown or less-known to the protection systems. However, these low-level security mechanisms alone cannot ensure the security of WSN from both active and passive attacks.
2. A high-level mechanisms: A high-level mechanisms or detection based techniques are required when an attacker manages to pass the measures taken by the prevention step. This necessitates the establishment of the second line of defence like Intrusion Detection System which aims to provide a high level of security against both internal and external attacks.

C. WSN's Constraints

In WSN, Each node is inherently resource constrained. They have minimal computing power, storage space, and bandwidth for communication [23]. It is very challenging to ensure security in WSN while considering following constraints men- tioned in [24]:

1. *Sensor Node's Constraint:* WSN nodes have very small storage, processing and computational capabilities. Since they are battery powered and also they have little memory and size.
2. *Deployment Area's Constraint:* Sensor nodes are de- ployed in potentially unsecured areas either in fixed manner or in random manner and are remotely supervised. Weather conditions also effect the performance and life of WSNs.
3. *Communication channel's Constraint:* WSNs communi- cate through radio transmissions, and the majority of them use the unlicensed ISM band, which is often used for a variety of other applications. Co-existence of various wireless standards is a big challenge for secured communication.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

Intrusion Detection System in WSN

An Intrusion is an active or passive unauthorized activity in the network to compromise the integrity, confidentiality, or availability of resources [25].While Intrusion Detection System (IDS) is a collection of tools and methods to identify the intrusion and notify the network administrator about it or tries to isolate it from the network [26]. It cannot be considered as a stand-alone security system but is one of the components of the complete protection system [27]. To get a low false positive rate as well as a high true positive rate during the detection phase, IDS that is being developed should satisfy the following requirements as mentioned in [28].

- It should not introduce any kind of new weakness in the system and be reliable.
- It should not increase overheads in the system which results in the degradation of the performance of the system and require little system resources.
- Run continuously while remaining transparent to the system as well as users.
- It should use only cooperative and open standards.

Because of the resource constraints of the nodes in such networks, IDS implementations in sensor networks is presently in a premature stage and have not achieved complete automation till date. However, as new technologies emerge, such as mobile sensor nodes, fuzzy logic, neural network, data mining techniques, Machine learning, etc., the use of IDS technology in sensor networks will become more efficient.

State-of-Art IDS in WSN

Based on detection methodology, the IDS can be categorized into: Misuse / Signature based intrusion detection, Anomaly based intrusion detection, Specification based intrusion detection, and Reputation/Trust based intrusion detection as mentioned in [29], [30].

A. Misuse/Signature based Intrusion Detection

The misuse/signature-based detection relies on attack sig- natures to detect future attacks. An alarm is activated when an intrusion signature matches a previous intrusion signature that is already in the intrusion database. Misuse detection has the advantage of correctly detecting known attacks with a low False Positive rate (FPR). However, the drawback of this detection method is that it is inefficient against unknown attacks, and someone must continuously update the database of attack patterns. Using misuse detection technique is a difficult job for WSN because of constraints and challenges of WSN. For instance, keeping signatures of attacks is extremely difficult and is ineffective.

Chi and Cho [31] propose a fuzzy logic-based intrusion detection scheme. The fuzzy rules were developed using the following features of the traffic: node energy level, message transmission rate, neighbour nodes list, and transmission error rate. The base station or other neighbouring nodes will be in charge of gathering information messages from the neighbourhood, and the fuzzy controller will determine the detection value based on the above mentioned four parameters. The need for an expert or adequate experience to prepare the rule causes inability of the scheme to detect new emerging threats. Another disadvantage is that if the selected monitor node is compromised, it may become a point of failure.

Zamani et al. [32] proposed an IDS using a signature based detection technique to inspect data from a traffic-based collection process that was motivated by immunology and danger theory. The signature analogues in this design are Molecular Patterns (MPs). Two type of agents, stationary agent act like body tissues and mobile agents act as immune cells. The identification parameters was based on costimulation, which is the weighted number of the sums of healthy con- centration levels, risk concentration levels, and the density of corresponding molecular patterns. They report false negative rate of 40% and false positive rates of 8.23%, respectively. Their attack strategy focuses only on DDoS.

Lemos et al. [33] suggested a collaborative IDS system to detect node repetition attacks. This scheme is focused on identifying certain nodes as monitored nodes for the purpose of monitoring the activity of other nodes in the network based on a series of predefined rules that are appropriate for a given attack type. These nodes are then monitored by supervisor nodes. To begin with, if the supervisor nodes have been corrupted, they may be a cause of failure. Another

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

disadvantage is linked to generality, which is a serious concern for the most rule-based intrusion detection system is the need for manual rule setting.

Silva et al. [34] proposed a rule-based intrusion detection system for WSN to detect a wide variety of attacks in different layers. Three main phases are included in this scheme data acquisition phase in which the monitor nodes are listening of the messages and filtering the important information for the analysis; the rule phase applied pre-defined rules to the stored information, if the message review failed any of the rules test, a failure alarm is raised and the counter increased by one in the intrusion detection phase. If the total number of the raised failures is greater than a certain threshold, intrusion alarm is produced. However, this scheme has a significant flaw: difficulty in deciding the number of monitoring nodes devoted to the detection mechanism, how to choose them, and how to ensure that the selection method covers the whole network. Furthermore, this scheme is limited to some kinds of attacks.

B. Anomaly based Intrusion Detection

The anomaly-based identification is based on behavioural approaches, which distinguish between two forms of node behaviour: normal and abnormal. This method starts by explaining the usual behaviour features, which are generated by automated training. Any deviation from normal behaviours is considered an intrusion. Anomaly detection is suitable to detect unknown attacks. This scheme has the benefit of being able to reliably detect internal attacks. On the other hand, the disadvantage of this scheme is that system can exhibit legitimate but unseen behaviour, which could lead to a substantial false positive alarm rate as mentioned in [30].

Almomani et al. [35] developed a new dataset specialized for WSN called WSN-DS which consist of four different DoS attacks: Black hole, Gray hole, Flooding and Scheduling attacks and the Normal Traffic class. LEACH protocol, a hierarchical routing protocol was considered for its creation using NS2 network simulator. A WEKA data mining tool was used to build ANN-MLP model to detect the attacks. 10 folds cross-validation and held-out splitting techniques were used to classify attacks and the study achieved a satisfactory results. But it suffers from imbalanced problem in which detection rate of Gray hole attack was up to 75.6% which was very low.

Diyashree Sherly [36] proposed a NIDS based on ensemble CVM approach which works on minimum enclosing ball concept. KDD cup99 dataset was used for training and testing of classifier. A CVM classifier was modelled for each type of attacks like U2R, R2L, DoS and Probe attacks. Chi square test was used to select relevant feature of each attack and a weighted function was applied to these feature for dimensionality reduction. The model achieved high efficiency with less computation time. It has a detection rate of 99% and a false positive rate of 27%.

Moon and Cho [37] suggested a fuzzy logic-based intrusion detection technique. Two features related to the directed diffusion protocols are used which are the reinforcement ratio and the radius. These two features will be used as inputs by the fuzzy logic controller to produce its output, which is the detection value. The controller will raise an alert if the result detection value is greater than a predefined protection threshold, signalling that a sinkhole attack has occurred in the region. The fuzzy rules should be set by an expert according to the signs of sinkhole attacks before the detection value is calculated. Using fuzzy logic gives the flexibility of detection sinkhole attacks since the input values are not always sharp values. The key issue with this fuzzy-based system, though, is the need for manual rule setting.

Manzoor and Kumar [38] proposed an Intelligent Intrusion Detection System. Pre-processing of KDD CUP'99 data set was done to remove duplicate and redundant data from the data set. Information Gain (IG) and Correlation Algorithm were combined for feature selection and the reduced features were fed to feed forward neural network algorithm for training and testing purpose on KDD CUP' 99 data set. System was tested using five different subsets of KDD CUP'99 data set. Achieved results were outperforming.

Tan et al. [39] proposed a method of intrusion detection based on SMOTE and the Random Forest (RF) Algorithm. SMOTE (synthetic minority sampling technique) was used to balance the data set and then RF algorithm was used to train the classifier. The simulation was conducted on the benchmark data set i.e. KDD cup99 and the accuracy of classification by RF algorithm had reached 92.39%, which was higher other comparison classification algorithms. The accuracy of RF Algorithm was further improved to 92.57% after combining it with SMOTE. In future, other new classification methods used to further improve the recognition of intrusion data of WSNs.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

C. Specification based Intrusion Detection

The specifications that describe what can be considered as normal behaviour are defined manually and action is to be considered with respect to these specifications. Certain IDSs, on the other hand, enable all detection strategies to coexist and communicate in a single detection agent. That is, those agents would employ automated training-based anomaly detection techniques and human-created rule-based misuse detection techniques. These approaches are called hybrid systems. As previously said, the major drawback of this strategy is that attack or protocol specification are developed by humans. In this case, the network administrator manually specifies the requirements that identify what constitutes correct activity and control any actions in relation to those restrictions. The key disadvantage of this approach is manual development of all specifications is time consuming and it cannot detect malicious behaviours outside the scope of these specifications of the protocol as mentioned in [30].

Ravale et al. [40] suggested a hybrid approach through the combination of K-means clustering algorithm and SVM classifier. The performance of the technique was evaluated using KDD CUP 99 dataset. K-means clustering was used to reduce large heterogeneous dataset to a number of small homogenous subsets and then RBF Kernel function of SVM was used for classification purpose. Simulation results proved that accuracy and detection rate increased and false alarm rate decreased for reduced attribute set but overall detection rate still need to be improved.

Yassine Maleh et al. [41] proposed a hybrid lightweight intrusion detection system for cluster based sensor network architecture to reduce energy consumption which improved the life of network. Model performed anomaly detection using support vector machine (SVM) algorithm and a set of detection rules to detect malicious nodes. Simulation results show that it can detect abnormal nodes efficiently and had high detection rate with low false alarm. The performance of this hybrid model was evaluated using KDDcup'99 dataset and it achieved high intrusion detection rate almost 98% and reduced false alarm upto 2%.

D. Reputation/Trust based Intrusion Detection

Reputation is defined as "the opinion of a sensor node about the other node" and Trust is the derivation of the reputation of a sensor node. The primary function of a trust manager is to detect nodes that exhibiting selfish behaviour. It detects trustworthy nodes on the basis of multiple trust factors like direct trust, indirect trust, or mutual trust. These systems use both reputation and trust to make effective decisions to select relay nodes and analyzing data from other nodes to detect malicious nodes as mentioned in [30]

Zawaideh and Salamah [42] to identifying malicious nodes timely in an effective manner author proposed an efficient weighted trust-based malicious node detection (WT-MND) scheme for clustered WSN. Based on LEACH protocol, the proposed scheme computed trust value of a node from its reputation among its cluster members. If the trust value below the preset minimum acceptable trust (MAT), then node was said to be malicious node. The proposed scheme was based on adaptive trust-update process means trust of temporarily malfunction nodes can be updated depending on its behaviour. This scheme sustained higher detection ratio (DR) and low Misdetection ratio (MDR) without power consumption over- heads compared to related schemes. In future this scheme can be examined in heterogeneous networks subjected to powerful attacks like Sybil, wormhole attack etc.

Tayyab Khan et al. [43] To improve cooperation, trustworthiness and security for large scale WSN, author proposed a novel and comprehensive trust estimation approach (LTS) which operates on intra cluster and inter cluster along with distributed as well as centralised approach to make accurate trust decision of Sensor nodes with minimum overheads. A timing window mechanism was employed to monitor successful and unsuccessful interactions. The punishment to the malicious nodes and harshness of the trust function can be tuned according to application requirements. Author introduced a simple averaging scheme to aggregate the trust values for cluster heads. LTS is platform independent and not affected by chosen of any specific route scheme. The proposed work did not consider memory overhead, the weight and frequency of misbehaviour. LTS was not detecting On-Of attack, DoS attacks and Collusion attacks. LTS is suitable for only homogeneous WSN but not for heterogeneous WSN and IOT.

Wang et al. [44] proposed a protocol layer trust-based intrusion detection scheme for WSN. Trust metrics was calculated per-layer and combined it to determine the overall trust of a sensor node. The trust value was compared with a pre-defined threshold to decide whether the node is compromised or not. This scheme was outperformed in term of detection i.e. false negative as well as false positive probability as compared to state-of-art schemes. The

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

weakness of the scheme was communication overhead increased. In future, the scheme can be implemented to detect cross-layer attacks initiated at transport layer and application layer. To assess the performance of the scheme in its real time it can be tested on real WSN test bed.

Table I. Summary of the Proposed IDSS

Authors	Techniques	Dataset	Remarks
Chi and Cho [31]	Fuzzy logic	——	The need for an expert or adequate experience to prepare the rule causes inability of the scheme to detect new emerging threats
Zamani et al. [32]	Agent approach	——	This approach has high percentages of false negative and false positives, respectively. Their attack strategy relies only on DDoS attacks.
Lemos et al. [33]	Rule-based approach	——	Serious concern for this most rule-based intrusion detection system is the need for manual rule setting
Silva et al. [34]	Rule-based approach	——	This scheme is limited to some kinds of attacks
Almomani et al. [35]	Artificial neural network (ANN)	WSN-DS	This study achieved satisfactory results. But it suffers from imbalanced dataset problem in which detection rate of Gray hole attack was very low.
Diyashree & Sherly [36]	Core Vector Machine (CVM)	KDD cup'99	The model achieved high detection rate efficiency with less computation time. On the other hand, it has high a false positive rate of about 27%.
Moon and Cho [37]	Fuzzy logic	——	The key issue with any fuzzy-based system is the need for manually rule settings.
Manzoor and Kumar [38]	Artificial neural network (ANN)	KDD cup'99	Performance depends on selected features and training phase is time consuming
Tan et al. [39]	Random forest algorithm	KDD cup'99	New classification methods used to further improve the recognition of intrusion as well as reduces its complexity
Ravale et al. [40]	k-means clustering and support vector machine	KDD cup'99	Accuracy increased but the overall detection rate still needs to be improved
Yassine Maleh et al. [41]	Support vector machine (svm)	KDD cup'99	Computation overhead increases. Author does not provide any information about attacks
Zawaideh and Salamah [42]	Trust-based	——	This scheme can't be applicable to heterogeneous networks
Tayyab Khan et al. [43]	Trust-based	——	LTS was not detecting On-Of attack, DoS attacks and Collusion attacks. LTS is suitable for only homogeneous WSN but not for heterogeneous WSN
Wang et al. [44]	Trust-based	——	The weakness of the scheme was communication overhead increased

Challenges in Proposed IDSS

According to the above Table 1, following challenges are faced by IDSs proposed for WSN.

- Most of the IDS for WSN are rule based but the performance of these systems is highly dependent on the decision rules designed by the researchers. These rule based systems employ misuse detection technique and not adaptive for novel attacks. They have the capability to reduce false-positive alarm rate but in a dynamic changing computer environment this kind of IDS needs regular updating which is a time consuming task. However, the network traffic is huge and is having large number of features and it is very difficult to specify some intrusion using the rules. Therefore, the process of encoding rules is expensive as well as slow. • To overcome the limitation of rule-based systems in WSN, Data Mining approaches are employed which mainly focus on learning based IDS. These were very successful and still providing effective results by using different classification techniques. But the main drawback found during the study is that for use of classification approaches, data set were used. Those data set were having a number of features to train the systems. This makes network system more complex utilizes excess sensor's resources.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

- Traditional Data Mining and Learning Based approaches are effective enough for known types of attacks as per the dataset given to them for the training. But it is almost impossible for unknown attacks.
- Another major issue observed is that most of the IDS are limited to only one or two specific attacks and also limited to one or two layers of network.
- Very little work has been done on IDS for mobile sensor nodes in WSNs.

Conclusion and Future Directions

Security is a top priority for most of the applications in WSN. Traditional security mechanisms such as authentication, encryption and firewalls are having high overheads and are not feasible for these resource constraint networks because of their unique characteristics like limited power supply, small memory size and data storage. In this paper, existing security attacks, solutions to security attacks and constraints in WSN are discussed in section 'Background of security in WSN'. Then various proposed ids in WSN are presented according to their detection methodology. Finally, on the basis of all these observations and findings, various challenges in IDS for WSN are summarized. To overcome these challenges in future, more work is need to be done on those IDS that should be lightweight for resource constraint WSNs and should utilize least amount of energy. Also it should be cross-layer IDS that can detect both known and unknown attacks to provide maximum detection accuracy.

References

[1] J. Sen, "Security in wireless sensor networks," *Wireless Sensor Net- works: Current Status and Future Trends*, vol. 407, p. 408, 2012.

[2] Y.A. Bangash, Y.E. Al-Salhi *et al.*, "Security issues and challenges in wireless sensor networks: A survey." *IAENG International Journal of Computer Science*, vol. 44, no. 2, 2017.

[3] M. Aboelaze and F. Aloul, "Current and future trends in sensor networks: a survey," in *Second IFIP International Conference on Wireless and Optical Communications Networks, 2005. WOCN 2005.* IEEE, 2005, pp. 551–555.

[4] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," 2006.

[5] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications surveys & tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[6] C.F. Garc´ıa-Herna´ndez, P.H. Ibarguengoytia-Gonzalez, J. Garc´ıa- Herna´ndez, and J.A. Pe´rez-D´ıaz, "Wireless sensor networks and applications: a survey," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, no. 3, pp. 264–273, 2007.

[7] S. Duhan and P. Khandnor, "Intrusion detection system in wireless sen- sor networks: A comprehensive review," in *2016 International Confer- ence on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE, 2016, pp. 2707–2713.

[8] A. Alemdar and M. Ibnkahla, "Wireless sensor networks: Applications and challenges," in *2007 9th International Symposium on Signal Processing and Its Applications*. IEEE, 2007, pp. 1–6.

[9] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks," *Journal of sensors*, vol. 2015, 2015.

[10] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[11] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 34–40, 2008.

[12] M.L. Messai, "Classification of attacks in wireless sensor networks," *arXiv preprint arXiv:1406.4516*, 2014.

[13] O. Can and O.K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in *2015 6th international conference on modeling, simulation, and applied optimization (ICMSAO)*. IEEE, 2015, pp. 1–6.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

[14] M.A. Rassam, M. Maarof, and A. Zainal, "A survey of intrusion detection schemes in wireless sensor networks," *American Journal of Applied Sciences*, vol. 9, no. 10, p. 1636, 2012.

[15] F. Shahzad, M. Pasha, and A. Ahmad, "A survey of active attacks on wireless sensor networks and their countermeasures," *arXiv preprint arXiv:1702.07136*, 2017.

[16] Y. El Mourabit, A. Bouirden, A. Toumanari, and N. Moussaid, "Intrusion detection techniques in wireless sensor network using data mining algo- rithms: comparative evaluation based on attacks detection," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 9, pp. 164–172, 2015.

[17] D.G. Padmavathi, M. Shanmugapriya *et al.*, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576*, 2009.

[18] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks and countermeasures," in *The first IEEE international conference on system integration and reliability improvements*, vol. 25. Citeseer, 2006, p. 94.

[19] K. Ioannis, T. Dimitriou, and F.C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proc. of the 13th European Wireless Conference*. Citeseer, 2007, pp. 1–10.

[20] A. Mahmood and A.H. Akbar, "Threats in end to end commercial deployments of wireless sensor networks and their cross layer solution," in *2014 Conference on Information Assurance and Cyber Security (CIACS)*. IEEE, 2014, pp. 15–22.

[21] A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: A survey," in *Managing Cyber Threats*. Springer, 2005, pp. 19–78.

[22] A. Abduvaliyev, A.S.K. Pathan, J. Zhou, R. Roman, and W.C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[23] A. Alemdar and M. Ibnkahla, "Wireless sensor networks: Applications and challenges," in *2007 9th International Symposium on Signal Processing and Its Applications*. IEEE, 2007, pp. 1–6.

[24] Y. Wang, G. Attebury, and B. Ramamurthy, *"A survey of security issues in wireless sensor networks,"* 2006.

[25] K. Kaur and N. Kaur, "A hybrid approach of fuzzy c-mean clustering and genetic algorithm (ga) to improve intrusion detection rate," *International Journal of Science and Research*, 2015.

[26] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy and survey of intrusion detection system design techniques, network threats and datasets," *arXiv preprint arXiv:1806.03517*, 2018.

[27] R. Sharma and V.A. Athavale, "Survey of intrusion detection techniques and architectures in wireless sensor networks," *International Journal of Advanced Networking and Applications*, vol. 10, no. 4, pp. 3925–3937, 2019.

[28] I. Butun, S.D. Morgera D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

[29] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 56–63, 2007.

[30] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1–23, 2014.

[31] S.H. Chi and T.H. Cho, "Fuzzy logic anomaly detection scheme for directed diffusion based sensor networks," in *International Conference on Fuzzy Systems and Knowledge Discovery*. Springer, 2006, pp. 725– 734.

[32] M. Zamani, M. Movahedi, M. Ebadzadeh, and H. Pedram, "A ddos- aware ids model based on danger theory and mobile agents," in *2009 International Conference on Computational Intelligence and Security*, vol. 1. IEEE, 2009, pp. 516–520.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 3020 – 3028
Received 05 March 2021; Accepted 01 April 2021.

[33] M.V. de Sousa Lemos, L.B. Leal, and R. Holanda Filho, "A new collaborative approach for intrusion detection system on wireless sensor networks," in *Novel Algorithms and Techniques in Telecommunications and Networking*. Springer, 2010, pp. 239–244.

[34] A.P.R. da Silva, M.H. Martins, B.P. Rocha, A.A. Loureiro, L.B. Ruiz, and H.C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 2005, pp. 16–23.

[35] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "Wsn-ds: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. 2016, 2016.

[36] S.Y. Moon and T.H. Cho, "Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks," *International Journal of Computer Science and Network Security*, vol. 9, no. 7, pp. 118–122, 2009.

[37] I. Manzoor, N. Kumar *et al.*, "A feature reduced intrusion detection system using ann classifier," *Expert Systems with Applications*, vol. 88, pp. 249–257, 2017.

[38] X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo, X. Sun, and L. Li, "Wireless sensor networks intrusion detection based on smote and the random forest algorithm," *Sensors*, vol. 19, no. 1, p. 203, 2019.

[39] U. Ravale, N. Marathe, and P. Padiya, "Feature selection based hybrid anomaly intrusion detection system using k means and rbf kernel function," *Procedia Computer Science*, vol. 45, pp. 428–435, 2015.

[40] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.

[41] F. Zawaideh and M. Salamah, "An efficient weighted trust-based mali- cious node detection scheme for wireless sensor networks," *International Journal of Communication Systems*, vol. 32, no. 3, p. e3878, 2019.

[42] T. Khan, K. Singh, M. Abdel-Basset, H.V. Long, S.P. Singh, M. Manjul *et al.*, "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks," *IEEE Access*, vol. 7, pp. 58 221–58 240, 2019.

[43] J. Wang, S. Jiang, and A.O. Fapojuwo, "A protocol layer trust- based intrusion detection scheme for wireless sensor networks," *Sensors*, vol. 17, no. 6, p. 1227, 2017.