Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7760083

TK-OID: TRUST KNOWLEDGE BASED OUTLIER AND INTRUSION DETECTION FOR IOT ENABLED WSN

D. Princy[1], Dr.D.Kalaivani[2]

[1] Research Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science

[2] Associate Professor and Head, Department of Computer Technology, Dr. SNS Rajalakshmi College of Arts and Science

Email: [1]princy08george@gmail.com, [2]dkalaivani77@gmail.com

Abstract

To build efficient Internet of Things (IoT) communications between various applications, the Wireless Sensor Network (WSN) is incorporated with smart technologies. The IoT-enabled WSN is susceptible to a range of attacks because of its environment and intrinsic untrustworthy transmission. Intrusion detection systems (IDSs) are commonly used in WSN to protect against attacks to safeguard their protection. Outliers impair sensor information excellence and consistency due to the impact of environments and the restriction of sensors computing and transmission capacities. An efficient outlier and intrusion detection method are therefore necessary to provide efficient communication. Previous approaches are not practical in terms of the undue burden of computing and energy consumption on sensors. This paper proposes an efficient trust knowledge-based outlier and intrusion detection (TK-OID) for IoT enabled WSN. In this work, two trust knowledge base is used to detect outliers and intrusion. The first trust knowledge base is located at the small gateway node, collecting the sensed information from the sensor and detecting the local outliers. The next is situated at the base station, used to collect and analyze the small gateway's data and detect the intruder sensors. The experimental results indicate that this work performance improved detection accuracy compared to other existing methods.

Keywords: Trust, Outlier Detection, Intrusion Detection, Trust, Knowledge Base.

1. Introduction

Wireless Sensor Network (WSN) is the arrangement of different kinds of energy-constrained small devices that detect the physical incident of the environment and send out the data through diverse communication channels to the base station. The sensed data is transmitted to the base station for further processing in compliance with the applicable specifications. WSN can be used in surveillance, healthcare, industrial and different environmental applications [1]. In contrast, the Internet of Things (IoT) consists of various smart devices which provide Internet-based services and applications with the aid of physical-connected smart devices for data collection through different types of sensors for process control [2]. In many applications, IoTs are used in various fields [3].

The proper functioning of the sensors inside the IoT device plays a crucial role in the performance of associated applications [7]. IoT sensors are always installed in horrible circumstances; it is challenging to ensure the sensor's proper functioning and anticipate malfunctions. Also, sensors are usually the cheapest electronic components that are typically vulnerable to malfunctions within the IoT. A faulty sensor provides degraded information or incorrect measurements or contradictory data to the IoT device [8]. These kinds of data are known as outliers.

Initially, the word outlier, also known as an anomaly, was taken from the field of statistics. Owing to human error, computer error, mechanical failures, and system behaviour changes, outliers may be elevated or may be due to natural environmental variance [4]. Although outlier detection is the method of identifying patterns that greatly vary or deviate from the regular or average data set from a given set of data. Outlier detection is characterized as finding abnormalities in unexpectedly-behaving information [5]. The goal of outlier detection is to classify devices in IoT [6] by their activity that varies from the predicted and previously observed ones.

A significant explanation for security problems is the massive set of nodes, i.e. hosts or devices connected to the IoT, as a security flaw in a single node can lead to system-wide failure. Botnets, distributed denial of service (DDoS) attacks, malware, remote monitoring, forwarding attacks and information leakage [9] are the most prevalent security risks encountered by the IoT system. Using a firewall is regarded as the first line of protection to prevent attacks on IoT devices. Still, due to variations and sophistication of IoT architectures, it is not an efficient solution. To detect nodes' suspicious activity [10], intrusion detection systems (IDS) may be used. The definition of IDSs is to find intruders in an environment. In an IoT world, an intruder may be a host who attempts to access some other nodes without permission. To detect suspicious behaviour of the internal nodes of networks, IDS-based systems are very successful, protecting the entire network from different types of malicious attacks. Over time, the IDS agents can accumulate and evaluate the abnormal activity of nodes and then apply appropriate measures. There is numerous outlier, and intrusion detection methods are proposed for WSN and IoT.

This paper proposes an efficient trust knowledge-based outlier and intrusion detection (TK-OID) for IoT enabled WSN. In this work, two trust knowledge base is used to detect outliers and intrusion. The first trust knowledge base is located at the small gateway node, collecting the sensed information from the sensor and detecting the local outliers. Another one is located at the base station, used to collect and analyze the small gateway's data and detect the intruder sensors.

The remaining part of the paper is planned as follows: Section 2 review the related work. Section 3 explains the Outliers and Intrusion in IoT. The proposed TK-OID explains in section 4, and section 5 evaluate the performance of the proposed work. Finally, section 6 concludes the paper with future direction.

2. Related Work

In this section, the earlier outlier and intrusion detection methods are explained.

A. Outlier Detection Methods

Because of security risks and bizarre incidents, data analysts have always identified and fixed data outliers. Outlier detection is an essential field in data mining studies and analysis and has numerous applications for a network, such as a climate modelling, fraud detection and interference identification. This section explains various outlier detection techniques in WSN and IoT.

Zhang et al., [11] suggest an artificial neural network (ANN) outlier identification and recovery method that can be used to assess if the temperature obtained values by the sensors in the WSNs are anomalies. Wang et al., [12] suggest a distributed outlier detection system based on isolation using nearest-neighbour ensembles (iNNE) to identify outliers in WSN effectively. In each node, local detectors are built by the iNNE algorithm. A new combination approach is proposed that takes advantage of the spatial correlation for local detectors between sensor nodes. The procedure is based on the principle of weighted voting. A sliding window is inserted to upgrade local detectors, which allows the adaptation of complex environmental changes.

By analyzing received signal strengths using the combination of supervised, unsupervised and ensemble machine learning techniques, Bhatti et al., [4] developed an outlier detection technique known as iF Ensemble for Wi-Fi indoor localization environment. Isolation forest (iForest) is used in this research as an unsupervised method of learning. Support vector machine, K-nearest neighbour and random forest classifiers with stacking, an ensemble learning process, are used in the supervised learning method.

Zhu et al., [13] propose a new framework to support KNN-Based outlier detection over IoT streaming data called GAAOD. This introduces a grid-based index for the management of data stream summary information. It can modify the resolution of cells self-adaptively and achieve the objective of effectively filtering artefacts that are almost unable to become outliers. It utilizes a min-heap-based algorithm to measure the upper-/lower-bound distance among objects and their nearest neighbours. It uses a k-sky band based algorithm to sustain outliers and candidate outliers.

B. Intrusion Detection Methods

Selvakumar et al., [14] suggested intellectual IDS focused on temporal reasoning, using a self-designed scheme based fuzzy and rough set-based nearest neighbourhood. It was used to decrease the complexity as it eliminated the redundant properties. Alaparthy and Morgera [15] developed a multilevel IDS based on the human immune system's idea. A few nodes were positioned near the sink node. It executes a pathogen-associated molecular pattern examination to identify the attack. Sun et al., [16] suggested multilevel IDS using the benefits of the adverse selection algorithm and an enhanced V-detector algorithm to reduce the complexities of resource-constrained WSN.

By considering a network of resource-limited nodes, Jan et al., [17] introduced a lightweight IDS to prevent the most common DOS attack in IoT. This work may not have provided the desired outcome in the network with steady traffic flow. Sharma et al., [18] developed a lightweight framework for IoT-embedded cyber-physical systems named behaviour rule specification-based misbehaviour detection. It recognized the existence of an intruder via misbehaviour of an established network node. A blockchain-driven collaborative signature-based intrusion detection framework was developed for IoT by Li et al., [19]. IDS rules and signatures based on a combined signature were used to detect the intruder's malicious behaviour. This data was exchanged with the other network nodes to update their database and increase the intrusion detection rate.

3. Outlier and Intrusion in IoT

In the sense of IoTs, in contrast to its previous activity or readings, the sensor's outlier is usually considered an irregularity or deviation in sensor behaviour during archiving unique parameters or events. Thierer et al., [20], defined "an outlier is a data point that is considerably different from other pieces of information, or does not correspond to the predicted normal behaviour, or corresponds well to a specified abnormal behaviour". Pachauri et al., [21] defined, "An outlier is an observation or subset of measurements which appears to be incompatible with the rest of the data set". There are three primary IoT-relevant triggers of sensor outliers.

Immutable Sensor Failures: This form of error is linked to impaired readings or observations from an IoT device-embedded defective sensor. They often unexpectedly fail and quit functioning without any sign of deteriorating efficiency. This type of sensor failure supplies the IoT system's data analysis method to either no observations or null measurements.

Sensor incidents: Since the sensor is deployed in real-world situations or events to gather data, there is a chance of an unexpected alteration in the event triggered by unlikely circumstances that severely impact the sensor, creating outliers.

Recurrent Sensor Mistakes: Often triggered by intermittent events such as hacking, vicious assault and sensor tampering. A circumstance where a faulty connection in the sensor or elsewhere inside the sensing hardware may also lead the sensor to generate data processing algorithms with sporadic, sparse data [22].

There are typically five classes of outlier detection techniques used in IoT. They are statistical, nearest neighbour, artificial intelligence, cluster and classification based techniques.

Information from sensors is formulated through the use of a probabilistic distribution in statistical technique. When the probability of the data instance created by this method is very low, the sensors' data points can be classified as outliers or faults. This method utilizes prior sensed data to estimate and construct a model of a sensor's specific activity. However, suppose new measurements are obtained from the same sensor. In that case, this data point is then compared with the sample to verify whether the latest data point is theoretically inconsistent with the standard. If the model is incompatible with the new sensor reading, the outlier or a defective measurement is labelled.

The notion of proximity relies explicitly on the nearest neighbour technique for sensor fault and outlier identification. The nearest neighbour approach works to distinguish between the irregular and good readings by depending on the ranges among sensor data observations. The neural network methodology is a conceptual model that offers a systematic concept that, through analyzing the entire sensor dataset, helps the decision-making process. The fuzzy logic method uses transition values to be restricted between the standard/correct sensor readings. The fuzzy logic approach can be used in IoTs to enhance decision-making, boost the choice of clustering heads, and enhance network protection and data compression.

By splitting the data into clusters of identical sensor data points, each data cluster contains data points similar to each other and differ from the data points in other cluster classes. This strategy is a subset of proximity method. The preliminary sensor data are first used to establish the clusters. The new sensor observations are then labelled as irregular readings assigned to small and remote data clusters or sensor measurements that are very far from the centroid of the primary cluster. The classification method is appropriately suitable to the faults, outlier detection in IoTs. This strategy appears to work under the general assumption that a classifier can be trained to distinguish normal, and outlier classes from a given space function. It needs to be formed into two phases of training and testing to establish this technique. The methodology aims to learn a classifier during the training process using the appropriate labelled training data, followed by an experimental phase that classifies a test instance as a normal or outlier or sensor fault.

To control and examine unwanted activity, "Intrusion Detection System (IDS)" is introduced to secure smart IoT devices from different attacks. An IDS scans all traffic flows in a WSN and IoT-based interaction environment and looks for any interference signs. The deployed mechanism takes appropriate action if it detects any threat. In WSN and IoT environment, it is also probable that an opponent could physically snatch some devices. The attacker obtained the data from the compromised devices. To initiate various attacks [23] [24], these vulnerable devices can be preloaded with some malicious script.

When these attacks are executed, data packets which be lost, changed, discarded, or disrupted until they are forwarded to the target. This causes a significant deterioration in communication efficiency. This could also decrease throughput and packet delivery ratio and increase end-to-end delay [25]. Thus, developing an effective intrusion detection strategy is necessary for WSN and IoT communication.

IDS can be categorized into two groups based on its deployment: Host and Network-based IDS. By scanning log and audit documents, host-based IDS detects intrusion actions. This kind of IDS is typically used on important hosts to secure the host protection from all directions. The benefit of the host-based IDS is that it offers more accurate details, lower error rates, and less difficulty. However, it decreases the quality of the system application and depends extensively on log files and host monitoring capabilities.

Network-based IDSs need consideration because of the features of the IoT and because many IoT devices can be linked to the network. To discover possible intrusions, network-based IDS may detect suspicious activity and data flow in the network. It does not alter the configuration of the host and does not affect the business system's performance. Even if the IDS network fails, regular business activities will not be affected. An issue is that without looking at the network segments, network-based IDS only tests the direct relation to the network segment. Encrypted sessions with network-based IDS are also difficult to process.

Intrusion detection strategies are divided into four main groups based on different intrusion attacks: [26] signature, specification, anomaly and hybrid methods. Signature-based approaches initially check the network data and compare it with a database of features. If it is found that the scanned data matches the characteristics in the database of signatures, the data will be viewed as an intrusion. The benefit is that it can assess the form of attack accurately. It is relatively easy to use, and there is comparatively little demand for services.

Specification-based approaches enable rules and thresholds to be set in advance by system managers. As per the administrators' requirements and parameters, IDS detects the current device and network status. The IDS can recognize an unstable condition and respond appropriately if the threshold is exceeded or the rules are broken.

Anomaly-based approaches rely on abnormal patterns to be detected, and traffic patterns to be compared. The benefit of using this process is that it allows new and unknown intrusions to be identified. The primary drawback is that high false-positive rates appear to result from the process. Machine learning methods are used for anomaly detection, which improves effectiveness. Anomaly-based intrusion detection approaches can track the ongoing intrusion footprints by using machine learning algorithms and comparing them with existing datasets to be alert to possible future attacks.

Hybrid methods refer to any variation of the detection methods listed above being used in the same IDS. By improving the efficiency of the entire IoT system, this approach will help resolve the limitations of a single process. The obvious downside is that the whole of IDS is going to become very big and complex. This will make it harder to run the entire system, which will make more money. The intrusion detection method will have tremendous resources and time requirements, mainly when many protocols are involved in the IoT framework.

4. Methodology

This section explains the proposed trust knowledge-based outlier, and intrusion detection (TK-OID) method for IoT enabled WSN, including Network Assumption, Outlier Detection and Intruder Detection.

A. Network Assumption

A wireless sensor network usually comprises a group of sensor nodes spread over an area of interest to track specific physical processes. Sensor nodes can be organized to different kinds of topologies for various purposes. The proposed network consists of n number of sensor nodes (SN=sn_1, sn_2,…, sn_n) distributed randomly in a grid area. There is m number of small gateway node (SGN=sgn_1, sgn_2, …, sgn_m) deployed in randomly shown in Figure 1.

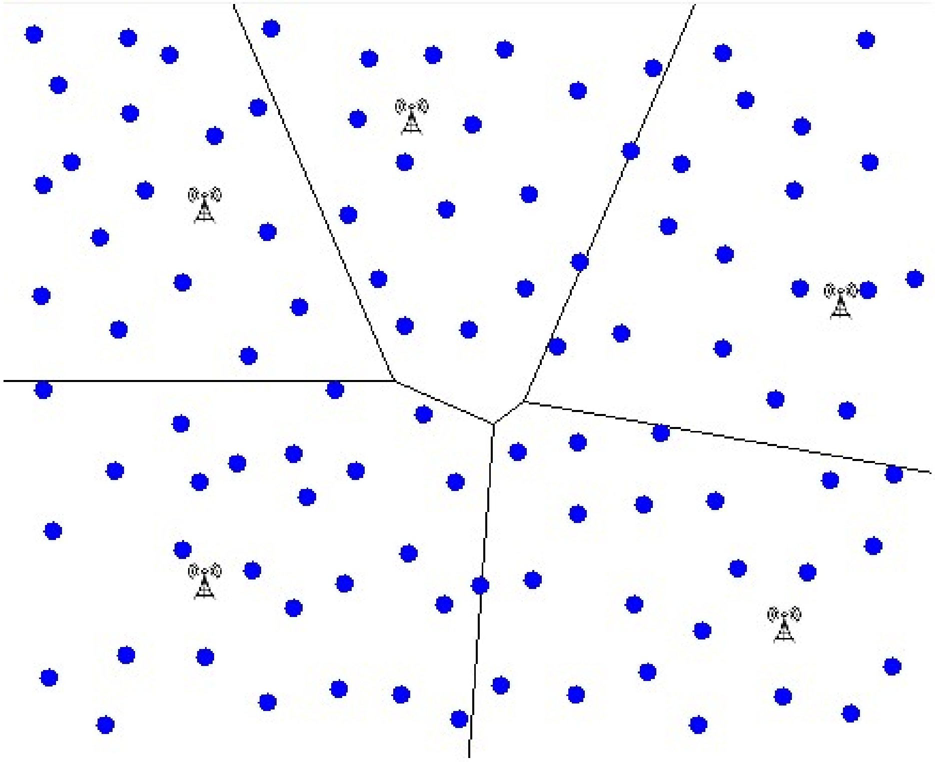

Figure 1 Sample network

The following assumption is used to form a network

- Randomly deploy sensor nodes (SN=sn_1, sn_2,…, sn_n) and SGN (SGN=sgn_1, sgn_2, …, sgn_m)
- Build the Voronoi tessellation relating to the SGN locations $sgn_i(x,y)$ to form a cluster.
- An empty trust knowledge base is deployed on each cluster nearer to the SGN, used to detect the outliers.

- One sink node or base station is located at the network centre with a trust knowledge base used to detect the intruders.
- A node in a cluster is only communicated with SGN.
- The sensors are uniform and synchronized with time.
- In the cluster, each sensor node generates an information vector comprised of various attributes.

B. Outlier Detection

The method of defining certain data instances that differ from the remaining data patterns based on a particular factor is the Outlier detection technique. Each measurement whose characteristics vary significantly from standard behaviours is therefore considered to be outliers. The following steps are used to detect outliers.

```
Algorithm-1 Outlier Detection

For i = 1 to |SGN|
    For j = 1 to |SN| ∈ SGN
        $X_{jt}$ = Sample Data Collected by $j^{th}$ Sensor Node at time t
    End For
    Remove Data in X that contains Null Values
    For k = 1 to t
        CC=Compute correlation coefficient for sequences
        init_Out = CC ≤ 0.4
    EndFor
    OF = ∅
    For j = 1 to |init_Out|
        $\eta_{nx}$= Find n- nearest neighbours
        Assign weight w based on Euclidean distance
        Compute $gf = \frac{cc * \sum_{i=1}^{n} w_i}{n}$
        If gf ≥ 1 then
            out = out ∪ $init\_Out_j$
        EndIf
```

```
18. EndFor
```

C. Intruder Detection

In general, IDS is installed in each node of a WSN for gathering essential data, and the cluster head can find the trust values of other nodes. In this work, trust knowledge-based IDS is deployed in Base Station to find the intruders. The intruders are detected based on the outlier data. The following steps are used to detect intruders.

1. The sensor nodes are randomly deployed and clustered based on the small gateway nodes.
2. For a particular time interval, each sensor node, sense information and send it to the small gateway.
3. The small gateway collects the sensed information and analyzes the data to find the outliers and report base station
4. The base station receives the outlier records and compute trust value based on the correlation.
5. Base station reports intruder node to small gateway node about the threats. Small gateway node takes further action.

5. Experimental Result

This section explains the simulation result analysis of the TK-OID approach against iForest [27], LOF [29] and iNNE [12]. Two types of the dataset are used for experiments. The first one is realtime temperature and humidity sensor data collected from [28]. Another one is a randomly generated data set, which contains 36 attributes. A labelled wireless sensor network data is collected using TelosB motes from a simple single-hop and multi-hop wireless sensor network deployment [28]. This dataset has outliers that are monitored, and all the information in the dataset is labelled. Four sensor nodes are completely available: two indoor and two outdoor sensor nodes. The dataset includes measurements of temperature and humidity gathered at an interval of 5s throughout six hours. Label '0' denotes regular data and label '1' indicates an occurrence that has been added, i.e. the outlier. In this event, to raise the humidity and temperature, steam from hot water is added. Outliers are a series of mistakes or incorrect readings in the dataset triggered by an incident. The dataset description is shown in Table 1.

Table 1 Dataset Description

Setting	ID	Samples		
		Total	Normal	Outlier
Indoor	1	4417	4300	117
	2	4417	4417	0
Outdoor	3	5039	5039	0
	4	5041	5009	32
Random	-	351	225	126

The following metrics are used to evaluate the performance of the proposed work: accuracy, detection rate, false alarm rate.

These metrics can be calculated as,

$$ACC = \frac{TN + TP}{TN + FP + TP + FN} \times 100\%$$

$$DR = \frac{TP}{FN + TP} \times 100\%$$

$$FAR = \frac{FP}{TN + FP} \times 100\%$$

Where TP, FP, TN, and FN denote the number of outliers correctly detected, the number of usual measurements wrongly detected as outliers, the number of regular measures correctly detected, and the number of outliers incorrectly detected as usual, respectively.

Table 2 shows the accuracy comparison of different methods. The proposed method achieves higher accuracy for the indoor and outdoor data set. For the random dataset, the iNNE has maximum accuracy.

Table 2 Accuracy Comparison

Dataset	iForest	LOF	iNNE	Proposed
Indoor-1	88.16	97.42	93.8	99.98
Outdoor-4	70.82	99.48	98.7	99.94
Random	77.78	67.81	92.4	90.59

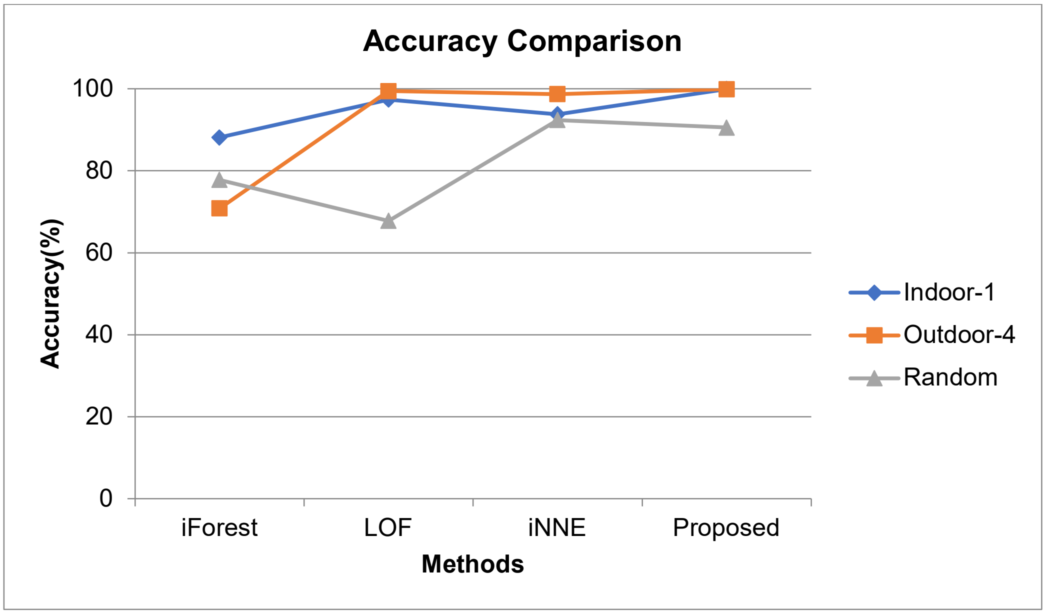

Figure 2 Accuracy Comparison

Table 3 shows the detection rate comparison. The proposed has a high detection rate for indoor and random data set. For the outdoor dataset, the iForest and iNNE provide high detection rate.

Table 3 DR Comparison

Dataset	iForest	LOF	iNNE	Proposed
Indoor-1	97.43	25.64	48.7	99.14
Outdoor-4	96.87	18.75	96.8	90.62
Random	61.11	10.31	65.7	77.77

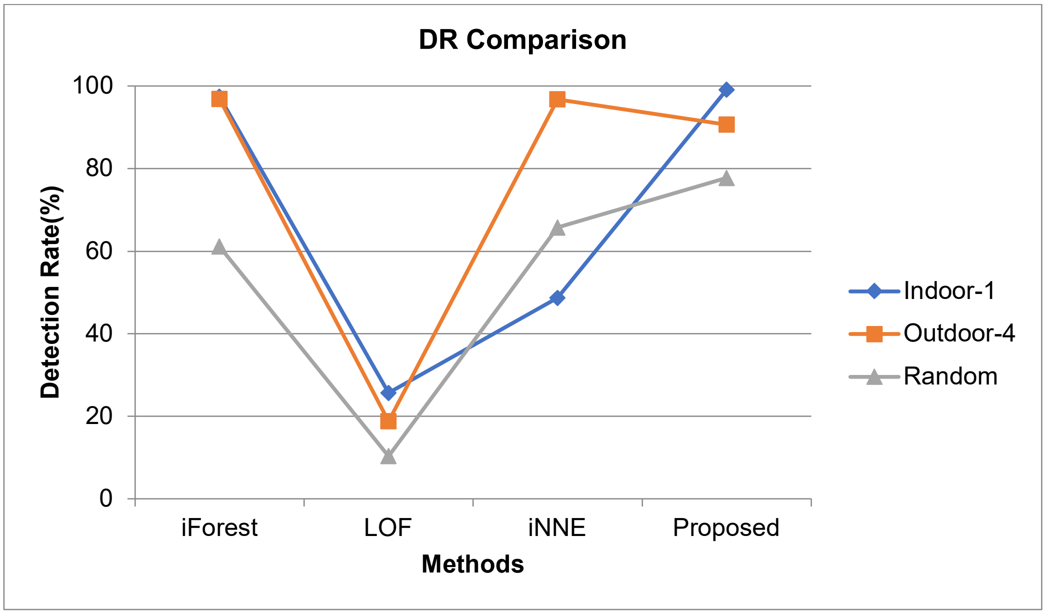

Figure 3 DR Comparison

Table 4 shows the false alarm rate comparison.

Table 4 FAR Comparison

Dataset	iForest	LOF	iNNE	Proposed
Indoor-1	12.16	0	4.9	0
Outdoor-4	29.34	0	1.3	0
Random	12.88	0	3.6	2.2

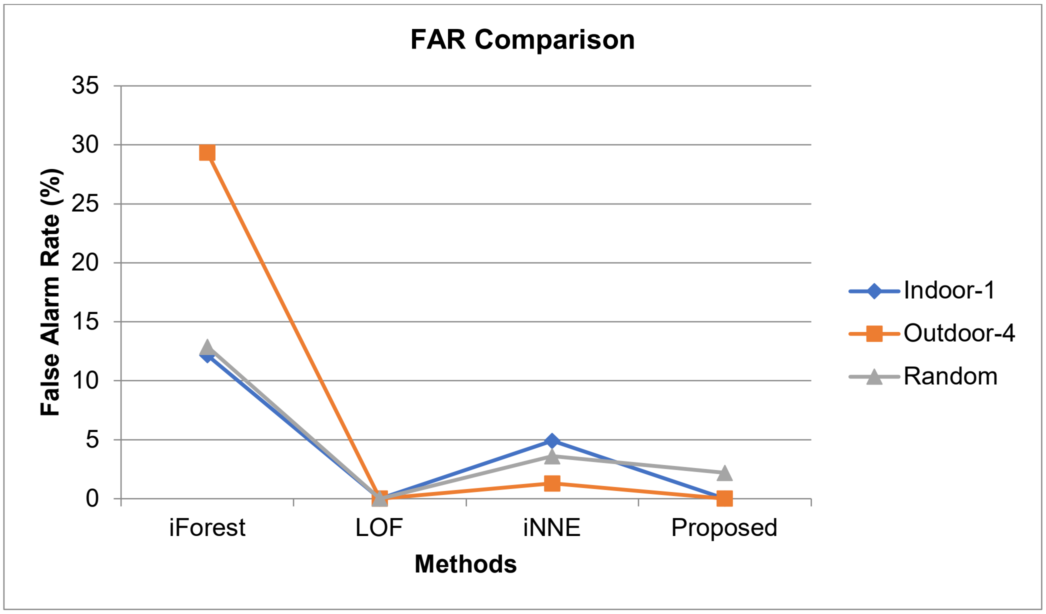

Figure 4 FAR Comparison

6. Conclusion

WSN is a significant IoT application that enables the sensing and controlling interconnected devices, i.e., direct integration of the physical world and computational systems. This kind of network is susceptible to numerous threats, particularly insider threat. Many algorithms have been proposed to detect insider attack; all of them has heavy computation. This paper presents an efficient trust knowledge-based outlier, and intrusion detection (TK-OID) for IoT enabled WSN. The proposed work efficiently identifies the outliers and intruders in the network. The work performs well in terms of accuracy, detection rate and false alarm rate compared to existing methods.

Reference

[1] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," in IEEE Access, vol. 8, pp. 3343-3363, 2020

[2] J.E. barra-Esquer, F.F. González-Navarro, B.L. Flores-Rios, L. Burtseva, M.A. Astorga-Vargas, "Tracking the evolution of the internet of things concept across different application domains", Sensors, vol. 17, 2017.

[3] H.N. Dai, H. Wang, G. Xu, J. Wan, M. Imran, "Big data analytics for manufacturing internet of things:Opportunities, challenges and enabling technologies", Enterp. Inf. Syst, pp. 1–25, 2019

[4] M. A. Bhatti, R. Riaz, S. S. Rizvi, S. Shokat, F. Riaz and S. J. Kwon, "Outlier detection in indoor localization and Internet of Things (IoT) using machine learning," in Journal of Communications and Networks, vol. 22, no. 3, pp. 236-243, June 2020

[5] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Application, vol. 60, pp. 19–31, 2016.

[6] I. Crameret al., "Detecting anomalies in device event data in the IoT," inProc. IoTBDS, pp. 52–62, 2018

[7] I. Lee, K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons, vol. 58, no. 4, pp. 431-440, 2015

[8] B.L. Risteska Stojkoska, K.V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions", Journal of Cleaner Production, vol. 140, no. 3, pp. 1454-1464, 2017

[9] V. Adat, B.B Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture" Telecommunication System, vol. 67, pp. 423–441, 2018

[10] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks", Ad Hoc Netw., vol. 55, pp. 97-106, Feb. 2017.

[11] K. Zhang, K. Yang, S. Li, D. Jing and H. Chen, "ANN-Based Outlier Detection for Wireless Sensor Networks in Smart Buildings," in IEEE Access, vol. 7, pp. 95987-95997, 2019.

[12] Z. Wang, G. Song and C. Gao, "An Isolation-Based Distributed Outlier Detection Framework Using Nearest Neighbor Ensembles for Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 96319-96333, 2019.

[13] R. Zhu et al., "KNN-Based Approximate Outlier Detection Algorithm Over IoT Streaming Data," in IEEE Access, vol. 8, pp. 42749-42759, 2020

[14] K. Selvakumar, M. Karuppiah, L. Sairamesh, S. H. Islam, M. M. Hassan,G. Fortino, and K.-K.-R. Choo, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," Inf. Sci., vol. 497, pp. 77–90, Sep. 2019.

[15] 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.

[16] Z. Sun, Y. Xu, G. Liang, and Z. Zhou, "An intrusion detection model for wireless sensor networks with an improved V–detector algorithm," IEEE Sensors J., vol. 18, no. 5, pp. 1971–1984, Mar. 2018.

[17] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," IEEE Access,vol. 7, pp. 42450–42471, 2019.

[18] V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "BRIoT: Behavior rule specification–based misbehavior detection for IoT–embedded cyber–physical systems," IEEE Access, vol. 7, pp. 118556–118580, 2019.

[19] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," Future Gener. Comput. Syst., vol. 96, pp. 481–489, Jul. 2019.

[20] A. Thierer, A. Castillo, "Projecting the Growth and Economic Impact of the Internet of Things", George MasonUniversity: Arlington, VA, USA, 2015.

[21] G. Pachauri, S. Sharma, "Anomaly Detection in Medical Wireless Sensor Networks using Machine Learning Algorithms", Procedia Comput. Science, 2015.

[22] V.M. Van Zoest, A. Stein, G. Hoek, "Outlier Detection in Urban Air Quality Sensor Networks", Water AirSoil Pollut, 2018

[23] M. Wazid and A. K. Das, "A secure group–based blackhole node detection scheme for hierarchical wireless sensor networks," Wireless Pers.Commun., vol. 94, no. 3, pp. 1165–1191, Jun. 2017

[24] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, N. Kumar, andJ. J. P. C. Rodrigues, "RAD–EI: A routing attack detection scheme foredge-based Internet of Things environment," Int. J. Commun. Syst.,vol. 32, no. 15, Oct. 2019
[25] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkholenode detection mechanism for hierarchical wireless sensor networks," Secur. Commun. Netw., vol. 9, no. 17, pp. 4596–4614, Nov. 2016.
[26] C. Liang, B. Shanmugam, S. Azam, A. Karim, A. Islam, M. Zamani, S. Kavianpour, and N. B. Idris, "Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems," Electronics, vol. 9, no. 7, Jul. 2020.
[27] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest", in Proc. 8th IEEE Int. Conf. Data Mining, pp. 413-422, 2008
[28] S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, and M. Palaniswami, "Labelled data collection for anomaly detection in wireless sensor networks," in Proc. 6th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP), pp. 269-274, 2010
[29] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers", ACM SIGMOD Rec., vol. 29, no. 2, pp. 93-104, 2000.