An Intrusion Detection and Prevention Protocol for Internet of Things Based Wireless Sensor Networks

Rajkumar Krishnan1 · R. Santhana Krishnan2 · Y. Harold Robinson3 · E. Golden Julie4 · Hoang Viet Long5 · A. Sangeetha1 · M. Subramanian6 · Raghvendra Kumar7

Accepted: 6 January 2022 / Published online: 15 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Because of the heavy data and communication advances, the utilization of Internet of Things (IoT) gadgets has expanded dramatically. In the improvement of IoT, Wireless Sensor Network (WSN) plays out a crucial part and involves easy keen gadgets for data gathering. In any case, such savvy gadgets have requirements regarding calculation, preparing, memory, and energy assets. Alongside such requirements, the major difficulties for WSN are to accomplish dependability with the security of communicated information in a weak climate alongside pernicious nodes. This paper intends to build up an Anomalous Intrusion Detection Protocol and Intrusion Prevention Protocol for interruption evasion in IoT dependent on WSN to expand the network time frame and information reliability. The proposed framework makes dissimilar energy-efficient groups dependent on the natural characteristics of nodes. Also, in view of the (k, n) limit related Shamir mystery sharing plan, the unwavering quality also, the security of the tangible data within the Base Station and group head are accomplished. The proposed security conspires demonstrates a trivial answer to adapt to interruptions produced by malignant nodes. The trial results utilizing the network test system Network Simulator-2 show that the proposed directing convention accomplished improvement as far as network lifetime, end-to-end delay as 24%, packet delay ratio as 30%, when contrasted and the current work under unique network characteristics.

Keywords Wireless sensor network · Internet of Things · Anomalous intrusion detection protocol · Intrusion prevention protocol

1 Introduction

Internet of Things (IoT) is an overall transmission framework which comprises of various availability protests that give organizing, tactile, and data handling devices [1]. The essential topic of IoT is to give availability anyplace within the homogeneous articles. Radio-recurrence ID (RFID) [2] is an underlying innovation for IoT that permits electromagnetic
elements to move the distinguishing proof information naturally towards within the user through remote network gadgets. Radio sign transponder (tag) and label per users are the two fundamental pieces of the RFID framework. Normally, RFID labels envelop electronically put away data and individuals can order, track, and screen the articles. The RFID labels are connected to some object for data assembling and checking the objective area.

WSNs [3] are an additional primary innovation for IoT that contains savvy objects known as the sensor nodes. These nodes are conveyed in an amorphous way for data catching with restricted imperatives as far as various assets. Nonetheless, because of the intricate formation of WSN and limited limitations on sensor nodes, actualizing security for IoT frameworks is difficult to measure and transmission may bargain with an assortment of network assaults [4]. Additionally, WSNs dependent on IoT is utilized in both joined in and unattended conditions like air contamination, water quality observing, keen urban areas, and so forth, another basic issue is to improve energy proficiency [5] other than solid information sending. Previously, various scientists have been given a group-based answer for WSN to accomplish energy productivity [6]. In grouping plans, the nodes are isolated into various locales with single group leader alluded to as the pioneer node.

The point of the group leader is to gather the information through the part nodes, total delivered packets across the base station. The data communication from group leaders to BS might be cultivated neither exploiting distinct bounce nor several jump procedures. Probabilistic enabled techniques are mostly two sorts of grouping arrangements. In probabilistic procedures [7], groups are produced in haphazardly request, which brings about unequal burden conveyance and energy utilization. Then again, the non-probabilistic technique [8] have been utilized various variables for the choice of group leaders. Despite the fact that, the non-probabilistic strategies give an improved exhibition when contrasted with customary probabilistic techniques, notwithstanding, due to dynamic environment of sensor nodes [9], humanizing energy protection and directing strength are as yet untie difficulties for IoT dependent on WSN that centers on building up an energy-productivity and secure steering convention to accomplish solid network transmission against vindictive dangers.

When contrasted with previous energy-proficient IoT enabled WSN frameworks, our proposed intrusion detection protocol called as anomalous intrusion detection protocol and intrusion prevention protocol. Right off the bat, the ESR convention utilizes the inborn capacities of nodes and creates different energy-effective groups by thinking about the Quality of Service (QoS) prerequisites. The proposed approach is constructed for providing secure, extensible concerning the expansion in the network field and dynamic as far as modifying the keys. In view of the previously mentioned commitments, the IPP convention is suitable for an enormous scope IoT based WSN frameworks that require energy-mindfulness, reliability, and shortcoming bearableness.

Due to this headway, new registering and transmission conditions, for example, the Internet of Things came into the image. A great deal of examination work is in advancement in the IoT space which helps for the general improvement of society and makes lives simple and agreeable. It is practically incomprehensible to build up a completely secure framework with IoT and WSN. The innovation is getting increasingly more helpless against security dangers. Later on, the quantity of Internet-associated individuals will be not exactly the brilliant items so the set up is used a hearty framework for keeping the previously mentioned conditions protected and normalized for the smooth conduction of transmission among IoT objects. Today in the advancement of technology forces the people to use their smart phone, laptop and other smart devices. In addition with this smart devices are connected together in the form of Internet of Technology. In recent years researchers
and organization decided to develop more protocols, services and standards. These concepts of IoT with WSN consist of embedded system, Intelligent and sensing Technology. Due to large sensor nodes are used to monitor the environment. In addition with large sensor nodes are grouped into cluster for reducing network traffic as well as energy saving. Each CH collects the data from sensor node, aggregates them and forwarded to the sink node. The proposed system is made out of two sub-segments. Right off the bat, non-covering and self-sufficiently coordinated groups are created and kept up the group dependability dependent on the vulnerability standard.

The main contribution of the paper is.

- A new Intrusion Detection Protocol method is constructed to detect the intruder in IoT based wireless sensor network. It consists of three phases are learning phase, the training phase, and the refreshing phase.
- The learning phase formulates for finding the neighbor node in a group, the training phase shows its ability in carrying the selected node with information and the refreshing phase determine the intruder node.
- A new Intrusion Prevention Protocol method is utilized to avoid the attacker or intruder happening within an IoT-based wireless sensor network. Here, the group updation will avoid the intruder into the network.

2 Related Works

Because of the progression of data and transmission advancements, the utilization of IoT gadgets has expanded dramatically. In the advancement of WSNs play out a fundamental part and includes minimal effort savvy gadgets for data gathering. Notwithstanding, such savvy gadgets have imperatives as far as calculation, preparing, memory, and energy assets. Alongside such imperatives, main difficulties for WSN are to accomplish unwavering quality throughout the privacy of delivering information in a weak climate beside inductive nodes. It intends to build up an energy-proficient enabled secure routing protocol for interruption shirking in IoT dependent on WSN to expand the lifetime frame and information dependability. Right off the bat, the proposed convention makes dissimilar energy-proficient groups dependent on the inherent characteristics of nodes. Furthermore, in light of the (k,n) limit related Shamir mystery sharing plan, the dependability and security of the tangible data within the base station and group leader are accomplished [10].

The framework of wireless sensor networks is organized in an impromptu way and coordinated nodes announcing the occasions to the Base Station. A WSN is coordinated with savvy advances to grow quick Internet of Things interchanges among various applications. As of late, numerous scientists proposed their answers for streamline IoT information transmissions in an energy proficient way with financially savvy uphold. Notwithstanding, a large portion of the arrangements have been zeroed in on the plan and advancement of static geographies and ignored the dynamic structure of versatile sensor nodes [11]. Besides, because of restricted imperatives of sensor nodes with open availability of remote transmissions medium, information assurance against vindictive exercises should be upgraded with the least network overheads. Subsequently, the commitment of this article is to propose interruption anticipation structure for portable IoT gadgets with its coordination to WSN so that to furnish information security with improved packet delivery ratio. Besides, start to finish secure and multi-jump steering
ways are created dependent on the blockchain engineering. The reproduction results exhibit a huge improvement when contrasted with existing arrangements as far as various performance measurements [12].

The possibility of running a lightweight Intrusion Detection System inside an obliged sensor or IoT node, the mIDS technique is implemented which screens and recognizes assaults utilizing a measurable investigation device dependent on Binary Logistic Regression. The mIDS takes as info just neighborhood node boundaries for both kind and malevolent conduct and determines a typical conduct model that recognizes variations from the norm inside the obliged node. The verification of right activity is completed by testing mIDS in a setting where network-layer assaults are available. In such a framework, basic information from the directing layer is gotten and utilized as a reason for profiling sensor behavior. Our results show that, notwithstanding the lightweight execution, the proposed arrangement accomplishes assault recognition precision levels inside the scope of 96–100% [13].

The innovation is extended to be close to people very soon on the grounds of its comprehensive development. These days, a ton of utilizations that are making our carries on with agreeable, for example, keen vehicles, savvy homes, brilliant traffic the executives, shrewd workplaces, brilliant clinical interview, savvy urban areas, and so on All such offices are in the span of an everyday person due to the headway in Information and Communications Technology. The arising activities of WSNs incorporated into IoT are additionally informed. A scientific categorization of security and protection conservation conventions in WSN and IoT is additionally featured. At last, the technique has examined some exploration challenges which should be tended to in the coming future [14].

The neighborhood location is directed by the devoted sniffers where each DS utilizes a regulated learning approach dependent on choice trees to create effectively characterized examples. The worldwide stage gathers the CCIs sent from the devoted sniffers to the super node and applies an iterative straight relapse to produce a time-sensitive profile called the aggregated proportion of variance for malignant and typical nodes. A profile of a malignant and an ordinary node is gotten, and an abnormality is distinguished after three cycles [15].

IoT has arisen as a significant, adaptable, and interoperable organization of gadgets, articles, things, and hardware. Fuelled by late advances in systems administration, interchanges, calculation, programming, and equipment innovations, IoT has ventured out of its earliest stages and is considered as the following advancement innovation in changing the Internet into a completely coordinated Future Internet [22]. Wireless Sensor Networks are used by IoT to gather, trade, and convey information distantly utilizing the capability of IoT in pragmatic applications and administrations. Notwithstanding, conveying information distantly may be undermined by different and genuine security assaults that centers on building up a visual-helped device for uncovering security dangers in IP-empowered WSNs. The intrusion detection system increased major centrality in the field of the web as the conveying substances could arrive at a large number of nodes.

Security is one among the major challenge of IoT. In WSN contain much type of attacks that affect the integrity, authentication and malicious activity. Include intrusion detection and prevention. Two algorithms were proposed to solve the intrusion detection and prevention. This algorithm was compared with standard algorithms like S-LEACH [20], MSLEACH [21], TBIDS and MBIDS [18]. The link failure within the cluster heads has been invoked that the predecessor will deliver the data packets to the base station using the technique of H2B2H [16]. The improved intrusion detection system [17] has been implemented to protect the system from several attacks with end-to-end transmission. The cluster related transmission in WSN is developed for producing the secured communication [19].
The existing algorithms were used to solve the problem of memory network overhead and detect the intrusion by using dummy message. LEACH is one of the traditional clusters routing protocol specifically designed for WSN to make clustering. Each round CH selection is based on random in the first round; further selection is based on remaining energy of threshold value. S-LEACH is an Improvement of LEACH focus on security aspects. It used to protect inside and outside the intruder. In this SPIN algorithm is also used for symmetric keys for authentication purpose. CH authentications are done by using shared keys in the MAC. MS-LEACH is also an advancement of S-LEACH. In addition with S-LEACH confidentiality will be provided into the Cluster Head. It contain shared pair wise key for establish connection between CH and members. In this MS-LEACH assumed with two symmetric key shared with sink node and CH. MBIDS is assumed to update all the CH. In this AODV routing protocol were used for routing the CH data to sink. Based on received control message sink node find out the intrusion occurrences and forward to all CH to avoid compromised.

3 Proposed Solution

An IDS that utilizes a mixture of learning the methodology comprises of two phases of identification, nearby and worldwide. The information assortment for the characterization purposes at the neighborhood location stage is proposed to mirror the network’s conduct as opposed to node conduct and the capacity to surmise the condition of the node. A plan dependent on acquiring datasets identified with the bundle means ordinary and vindictive cases, gathered utilizing the wanton mode is received in the network. Figure 1 demonstrates the Anomalous Intrusion Detection and Prevention Protocol Architecture which describes the working hybrid model of Intrusion Detection Protocol and Intrusion Prevention Protocol, it evaluates the working in each step.

A convention that changes trust and notoriety in view of node conduct. Pernicious conduct is distinguished utilizing the Tiny Attack and Fault Detection system (TAFDS). The convention changes to trust and notoriety esteem to the conduct of nodes by registering experience esteem dependent on the cautions produced by ATMP. The experience esteems are traded between the nodes and are utilized to refresh the notoriety and trust. This implies that a noxious or broken node will have low trust. The trust esteems can be utilized in secure steering or secure accumulation instruments. AIDP works in three stages: Learning, Trading, what’s more refreshing stage. In the Learning stage, the experience values are changed dependent on cautions from TAFDS. In the exchanging stage, every node sends its experience esteems to its neighbors. In the refreshing stage, the standing is refreshed dependent on the experience esteems and trust is refreshed in light of the new standing.

The experience is registered dependent on the authentic experience (the worth processed in the past cycle) and the discovery experience esteems decided dependent on the cautions produced by TAFDS. Subsequent to accepting the new experience esteem from the neighbors, the nodes figure notoriety dependent on the chronicled notoriety esteem, the immediate experience (if the node is an indicator), and the roundabout experience. The trust depends on the authentic trust esteem and the new notoriety. The convention is versatile on the grounds that trust and notoriety values are changed on each cycle, as indicated by the alarms from the TAFDS, which runs on the neighborhood node. The convention is community since nodes trade experience esteems with their neighbors in each cycle all together to figure notoriety esteems. The trust esteems are utilized to decide if a certain node has the right to assist in the
network. While the trust in a node is over sure breaking point, that node can take an interest in detecting and transmission activities. At the point when trust drops underneath the breaking point, the node should be rejected from the network. The phases of the proposed technique are demonstrated in 3 steps.

(a) The Learning Phase:
Each alarm got from TAFDS is converted into a discovery experience (just if the nearby node is a finder).
For every node that caused a caution, the experience esteem is refreshed utilizing in Eq. (1)

\[ L_{\text{new}}(x) = \alpha L_{\text{old}}(x) + \sum_{j=1}^{m} \beta_j L_j(x) \]  

\[ \text{Eq. (1)} \]
\( L_{old} \) is the old evaluated value in old cycle, \( L_i \) detection process, \( m \) is the number of alarm based on \( x \alpha_i, \beta_i \) are the weight values. Every part has a related load in the equation. The chronicled insight worth ought to normally have the best worth, and recognition experience esteems ought to have weight as per the seriousness of the alarm. Each non indicator node keeps up the past estimation of the experience in Eq. (2).

\[
\sum_{j=1}^{m} \beta_j L_j(x) = 1
\]  

(2)

c) Each node produces a rundown of the relationship among nodes and experience esteems, called experience affiliations, that contains just the qualities altered in the current cycle.

(b) The Trading Phase:
Every node sends the experience related to its neighbors utilizing a transmission message.
Each node holds on to get the arrangements of relationship from its neighbors for a pre-defined timeframe.
(c) The Refreshing Phase:

After the timeframe has terminated, the standing worth is recomputed utilizing Eq. (3).

\[
U_{new}(x) = \gamma U_{old}(x) + \delta D_e(x) + \sum_{i=1}^{k} C_i L_i(x)
\]  

(3)

\( U_{old} \) is old repeated values, \( D_e \) is experienced value computed directly, \( k \) is experienced value computed indirectly. The chronicled notoriety ought to have the best weight, while the immediate and aberrant experience may have various loads relying upon the aptitude on the reviewed node in Eq. (4).

\[
\gamma + \delta \sum_{i=1}^{k} C_i L_i(x) = 1
\]  

(4)

After that, detection is registered utilizing Eq. (5).

\[
D_{new}(x) = \tau D_{old}(x) + \phi U_{new}(x)
\]  

(5)

\( D_{old} \) is the old value, \( D_{new} \) is current value, \( \tau + \phi = 1 \). The chronicled trust ought to have the best weight in the recipe. An indicator node, which remains in a steering way from the reviewed node to the base station, has more aptitude than a finder node not remaining on that directing way. In any case, contemplating the portability of nodes and the incessant difference in directing ways, consider the experience esteem dictated by other identifier nodes, as they may have past involvement in the examined node. A total trust the executive’s cycle comprises of a Learning, Exchanging, and Updating stage. Toward the finish of a cycle, every node has refreshed the trust in different nodes.

The utilization of residual energy through the Received signal strength indication (RSSI) within the BS and Queue Length (QL) factors, the competitive value has been calculated for every nodes and the node receives the adjacent node data. Initially, the node energy is the main factor in the network with highest residual energy of the node and utilizes the RSSI measurement to improve the performance of the wireless link which affords the highest reception rate along with the threshold values. Secondly,
IPP protocol generates the reception rate into the beacon packets within a specific time period which is computed in Eq. (6).

\[ \text{RSSI}_{\text{threshold}} = \frac{Y}{n} \]  

Thirdly, the BS reduces the energy consumption by providing the shortest path and prolonging the network lifetime. The QL maximizes the data packet delivery at the node level. The QL is computed in Eq. (7).

\[ QL = \frac{RR}{TBS} \]  

At last, all the elements are summed up dependent on weighted methods as appeared in Eq. (8) and the nodes are designated as beginning group heads dependent on the most noteworthy serious worth C. Accordingly, the proposed IPP convention chooses an advance group heads dependent on natural characteristics and created groups are more versatile. The figured estimation of C is standardized in the arrangement of [0,1].

\[ C = we_1 \ast s_i + we_2 \ast \text{RSSI} + we_3 \ast \left( \frac{1}{d_{\text{toBS}}} \right) + we_4 \ast QL \]  

where the weighting factors are meant by \( we_1, we_2, we_3, \text{and} we_4 \) for different determination viewpoints, to be specific the node’s lingering energy, RSSI, vicinity from BS, and line length. Throughout the choice measure, every weighting factors mean the specific effect in processing the serious estimation of nodes, though \( we_1 + we_2 + we_3 + we_4 = 1 \). The affectability examination of the weighting factors that the assessed serious worth is in the arrangement of [0,1] as all the lingering energy, RSSI, nearness from BS, and line length have values in a similar reach. Initially, the leftover energy metric makes the group choice instrument more versatile. Moreover, the RSSI aspect is brought together in the choice component of the group head, which shows the presentation of the remote connection. Besides, in light of the littlest good ways from BS, a proper node is considered for the choice of the group head.

Every node sends guide collection to its neighbors at a time frame fixed period. On getting signals bundles, the neighbor node assesses its RSSI esteem and delivers back through the source node. Eventually, the line length factor is fused in the determination system of the group leader, along these lines a node is given a higher need to be chosen as a group head if its travel line length is superior to a specific limit. Following the choice of essential group leaders, they publicized their status in an exact way. Every typical node joins their nearby group head for the development of groups, after accepting the status messages. Typical nodes may get status messages from the neighboring group head and partner themselves with those group leaders, containing the most grounded RSSI esteem. Toward the finish of groups arrangement measure, the IPP convention allocates an exceptional ID for all produced groups to determine their limits. The arrangement of nodes chose as group heads declare channel access plans dependent on time-division numerous entrances (TDMA). Algorithm 1 demonstrates the Intrusion Detection Protocol in the phases of learning and rephrasing. The entire process is demonstrated in Fig. 2.
Fig. 2 Flowchart of IDP
Algorithm 1 – Intrusion Detection Protocol

Begin Procedure

Node with BS
Discover the intruder
Start learning phase
    Formation of Group (G)
    Discover the adjacent node $N_0$
    Set alarm $a_1$
    if $N_0$ is found within $a_1$
       Compute $L_{\text{new}}(x)$ using Eq. (1).
    end if
End learning phase
Start Refreshing phase
    Compute $U_{\text{new}}(x)$ using Eq. (3).
Reviewed node $R_n$
Detect D

The proposed IPP convention separates the general usefulness into two fundamental parts that are talked about in the following segments. In the principal segment, the IPP convention arranges ideal progressive geography development based information steering. In light of various rules alongside QoS requirements, the advanced group heads are resolved in relationship with the appropriated groups in an energy-productive and adjusted way. Besides, the proposed grouping plan enhances network lifetime and force utilization proportion within the sensor nodes. In the subsequent segment, the safe and reliable directing way is developed within group leaders and BS to maintain a strategic distance from any interruptions brought about by pernicious nodes. To accomplish solid information sending, the BS produces a mystery key, which is shared among chosen group leaders. In information sending from group heads, the information bundles are encoded utilizing the system. Then again, BS remakes the inbound information bundles from group heads utilizing the proposed mystery sharing plan. Besides, the overall effect of each factor in an enhanced choice cycle of the group head is assessed dependent on an affectability examination, which is a numerical model that gives a comprehension of the association among info and
yield esteems being developed. Reproduction consequences IPP beat other applicable plans regarding parcel conveyance proportion, network lifetime; End-to-end delay, transmission cost, number of course disclosures and network overhead. Algorithm 2 demonstrates the Intrusion Prevention Protocol.

Algorithm 2 – Intrusion Prevention Protocol

Begin group formation
Discover the adjacent node in the network
For every hub
   compute the value of C using Eq. (8)
   if C is not null
      Frame the C as the group head
   end if
End for
Group head can form the group and maintain the channel with TDMA
End

In the group updation process as the WSNs have confined assets, hence ESR conventions re-figure the function of group heads in a unique way. The principal point behind refreshing of group heads part is to accomplish uniform burden adjusting and energy utilization. ESR convention notices the resulting to assess the network measure.

i. At the point when any node receives the data packet then initially it confirms if it previously got a similar information bundle. In the event that indeed, at that point group heads essentially drop the copy information bundle to diminish network blockage and energy utilization.

ii. It very well may be a case that the group head gets another information bundle, yet it has no enough energy asset, i.e., $er < \text{edge}$, at that point it stops from information sending and starts re-appointment the instrument inside a specific group limit. Besides, the IPP convention likewise processes the clog rate $CL$ of each group dependent on the capacity, which implies the standardized blockage esteem in the scope of $[0,1]$ as appeared in Eq. (9).

\[
CL = \frac{AvDR}{AvRR}
\]  

(9)

where $AvDR$ demonstrates the mean delay ratio within the data packets and $AvRR$ denotes the mean reception rate of data packets, the algorithm 3 demonstrates the Group Heads updating process.
Algorithm 3 – Group Heads updating

Begin group head updation
For a hub in the group head
do
   if energy < threshold
      Compute CL using Eq. (10).
      Compute C using Eq. (8)
      Update the Time Division Multiple Access
   end if
End for
End

Threshold based IDS is identified by the sink nodes, which saves energy. It does not affect the packet loss, in both cases sink node only detect intrusion based on the threshold value set by sink. This situation can identify the intrusion by comparing the message from each CH. These values were learned by the sink node in the learning phase.

4 Performance Analysis

In the experimental setup the performance of the proposed algorithm were compared with other algorithms. Experiments are conducted with different parameters like number of sensor node, sensor nodes position and different number occurrences of intrusion. In our experiment sensor nodes vary from 25 to 500 nodes in the random deployment. In this experiment Deployment area also vary from $50 \times 50$ m to $1000 \times 1000$ m for approximation. It contains 75 nodes dispersed on a $650 \times 650$-m level space. This space causes the most extreme jumps to be 3 bounces. The actual layer and 802.11 MAC layer are remembered for the remote augmentations of NS2. Table 1 shows the AIDP parameter setting and the other parameter setting. UDP traffic with a consistent bit rate (CBR) is utilized with a packet size of 512 bytes and an information pace of 4 packets per second. Every information point was acquired by running the reenactment multiple times with various seed numbers and taking the normal worth. The sensor nodes populace fluctuates from 0 to 35% with 15% additions. The shrewd aggressors’ number is set to a consistent level of 35% from the all outnumber of acting-up nodes.

Every node sends acknowledgement packets to its neighbors at a time frame fixed time period. On getting signals packages, the neighbor node assesses its RSSI regard and delivers back through the source node. Eventually, the line length factor is fused in the determination system of the group leader, along these lines a node is given a higher need to be chosen as a group head if its travel line length is superior to a specific limit. Following the choice of essential group leaders, they publicized their status in an exact way. Every typical node joins their nearby group head for the development of groups, after accepting
the status messages. Typical nodes may get status messages from the neighboring group head and partner themselves with those group leaders, containing the most grounded RSSI esteem. Toward the finish of the groups arrangement measure, the IPP convention allocates an exceptional ID for all produced groups to determine their limits. The arrangement of nodes chose as group heads declare channel access plans dependent on time-division numerous entrances (TDMA).

In the evaluation phase of any, machine learning model should contain one important step is measuring accuracy. In regression analysis method Mean Absolute Error (MAE), Mean Square Error (MSE), Root Mean Square Error (RMSE) is used to evaluate the performance of the proposed model. Mean Absolute Error is used to measure the average difference between actual and predicted value in the learning phase of the dataset. Mean Square Error is measured the average of square difference between original and predicted value, it is also called as variance. Root Mean Square Error is measured the square root of Mean Square Error. The lower value of MAE, MSE and RMSE implies higher accuracy. MAEs are more robust to data with outliers and the performance result is demonstrated in Fig. 3 shows that the proposed technique has the minimized error values than the related techniques.

Intrusion detection protocol has the monitoring functionality which discovers the attacks and produces the alerts while detecting the intrusion. According to the detection alert, a security mechanism may respond and takes the necessary actions for reducing the security threats in WSN. The detection accuracy can be limited with the network traffic and exact labeling parameter. The proposed technique has been integrated with the outputs for different scenarios and produces the alarm to demonstrate the malicious activities. The detection accuracy has been improved by reducing the total amount of false alarm while discovering

| Table 1 AIDP Parameters |
|-------------------------|
| AIDP Parameter         | Value                      |
| Snoop forwarder errors | ✔                          |
| Snoop source routs     | ✔                          |
| Cache                  | ✔                          |
| Tap mode               | ✔                          |
| Response from cache to | ✔                          |
| request               |
| Maximum time between   | 10(in sec)                |
| request & response     |                            |
| Packet life time       | 35 (in sec)               |
| # nodes               | 75                         |
| Simulation area        | 650*650                   |
| Simulation time        | 850 s                     |
| Model                  | Random waypoint            |
| Speed range from       | Similarity distribution    |
| Maximum speed          | (1–20)                    |
| Traffic variety        | Consistent Bit Rate       |
| Packet size            | 512 bytes                 |
| Packet rate            | 5/sec                     |
| Maximum connections    | 10                         |
| Communication range    | 100 m                     |
| Transmission power of  | 1000 mW                   |
| sensor node            |                            |
| Sink node placement    | Based on required position|
| Node deployment        | Random manner              |
the intrusion detection. The sensors are mainly utilized for generating the security related functionalities with the console has monitored the sensors that the system produces alters in intrusion detection. Figure 4 demonstrates that the detection accuracy for the proposed technique is compared with the other techniques and the produced result shows that the proposed AIDP is performed well (Fig. 5).

---

**Fig. 3** Comparison of MSE, MAE and RMSE

**Fig. 4** Detection Accuracy
The network lifetime is computed as the time period for runs out of energy for the specific sensor node as every node has configured for forwarding the gathered data to the sink node through the specific transmission process. The enhanced routing protocol has the enhanced network lifetime with specific routing management. The network lifetime is related with the network throughput that the failure time for the initial sensor node in the network transmission. The improved energy management should enhance the network lifetime as the huge amount of sensors with communication range which monitors the network through random deployment of the sensor nodes in the network. The proposed technique has the improved network lifetime than the relevant techniques which is demonstrated in Fig. 5.

The packet delivery ratio is the highest amount of packets delivered to the recipient node within the specified time period while transmitting huge amount of packets, the packet loss has been increased so the efficient routing process will eliminate the packet loss and enhances the packet delivery ratio. The proposed technique has the enhanced delivery ratio than other techniques which is illustrated in Fig. 6.

The sensor nodes with random deployment have directly delivered the data to the nearest sink node for minimizing the energy consumption. The residual energy has been used to augment the balance energy within the nodes in the cluster by reducing the energy consumption while active network transmission. The energy utilization has varied according to the techniques used in data transmission while several routing functions are involved for minimizing the energy utilization. The base stations are having the elements of nodes with several transmissions and energy related resources that will act as the bridge within the nodes and the sink node will deliver the data packets into the recipient node. The energy consumption for the proposed technique is minimized compared with the relevant techniques and it is demonstrated in Fig. 7.

The end-to-end delay is characterized between the times a packet is produced at the sensor to the time it is gotten by the sink node. Accordingly, the start to finish transmission deferral of a packet is equivalent to the nearby transmission delay and is from the
time it is created to the time it is gotten at the sink. The end-to-end delay defines the packet should be delivery within the end-to-end transition in a network and the process of nodes will reveal the method of the network process within the framework in Fig. 8.

Fig. 6 Packet delivery ratio

Fig. 7 Energy Consumption
Throughput is a proportion of absolute units of data a framework can process in a given measure of time. Related proportions of framework yield incorporate the speed with which some particular responsibility can be finished and reaction time, the measure of time between a solitary intelligent client solicitation and receipt of the reaction. Bundle communication per time presents a deferral, in the interim, a bigger packet will take more time to get and return than a little one in Fig. 9.
5 Conclusion

The paper is constructed to introduce the Anomalous Intrusion Detection Protocol and Intrusion prevention protocol convention for interruption safeguard in IoT dependent on WSN. In the current arrangement, the majority of them utilized an insatiable calculation for the development of the steering way, ignored interruptions in a complex climate. This outcomes in a highest amount of course disclosures, especially below the quantity of vindictive nodes and high network load situations. Essentially, AIDP streamlined the choice cycle of group heads and utilized a circulated methodology to create groups for consistent appropriation of energy utilization. Moreover, the higher estimations of RSSI and least network block improved the steering execution regarding QoS limitations and information dependability. Besides, to accomplish a protected network wide information steering against vindictive nodes, the AIDP convention embraced a light-weight mystery sharing plan within the group leaders and BS. This gave information security from nodes through the group heads to the BS against pernicious dangers. The proposed technique has maintained the QoS with the reduced end-to-end delay, improved energy consumption, increased network throughput, enhanced packet delivery ratio and more detection accuracy than the related techniques. For future work, the proposed convention will be reached out by allowing for multi-bounce network transmission alongside the versatility principles.

Acknowledgements This paper is funded in part by the Ministry of Science and Technology of Vietnam, under Grant No. ĐTDLCN.105/21-C.

Declarations

Conflict of interest The authors have no conflicts of interest to declare that are relevant to the content of this article. All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. The authors have no financial or proprietary interests in any material discussed in this article.

References

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29, 1645–1660.
2. Downie, J.D.; Nederlof, L.; Sutherland, J.S.; Wagner, R.E.; Webb, D.A.; Whiting, M.S. Radio Frequency Identification (RFID) Connected Tag Communications Protocol and Related Systems and Methods. U.S. Patent No. 9,652,707, 16 May 2017.
3. Hezaveh, M.; Shirmohammdi, Z.; Rohbani, N.; Miremadi, S.G. A fault-tolerant and energy-aware mechanism for cluster-based routing algorithm of WSNs. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, Canada, 11–15 May 2015; pp. 659–664.
4. Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. Computer, 46, 46–53.
5. Sharma, N., & Sharma, A. K. (2016). Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network. Sadhana, 41, 283–288.
6. Abo-Zahhad, M., Ahmed, S. M., Sabor, N., & Sasaki, S. (2015). Mobile sink-based adaptive immune energy-efficient clustering protocol for improving the lifetime and stability period of wireless sensor networks. IEEE Sensors Journal, 15, 4576–4586.
7. Heinzelman,W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 7 January 2000; pp. 1–10.
8. Abdulsalam, H.M.; Kamel, L.K. W-LEACH: Weighted Low Energy Adaptive Clustering Hierarchy aggregation algorithm for data streams in wireless sensor networks. In Proceedings of the 2010 IEEE International Conference on Data Mining Workshops (ICDMW), Sydney, Australia, 13 December 2010; pp. 1–8.

9. Mittal, N., Singh, U., & Sohi, B. S. (2017). A stable energy efficient clustering protocol for wireless sensor networks. *Wirel. Netw.*, 23, 1809–1821.

10. Haseeb, Khalid, Almogren, Ahmad, Islam, Naveed, Din, Ikram Ud, & Jan, Zahoor. (2019). An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. *Energies.*, 12(21), 4174.

11. Haseeb, Khalid, Islam, Naveed, Almogren, Ahmad, & Din, Ikram Ud. (2019). Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. *Ieee Access*, 7, 185496–185505.

12. Tsitsiroudi, Niki, Panagiotis Sarigiannidis, Eirini Karapistoli, and Anastasios A. Economides. "EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs." In 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC), pp. 103–109. IEEE, 2016.

13. Ioannou, Christiana, and Vasos Vassiliou. "An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression." In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pp. 259–263. 2018.

14. Pundir, Sumit, Wazid, Mohammad, Singh, Devesh Pratap, Das, Ashok Kumar, Rodrigues, Joel JPC., & Park, Youngho. (2019). Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. *IEEE Access.*, 8, 3343–3363.

15. Amouri, Amar, Vishwa T. Alaparthy, and Salvatore D. Morgera. "Cross layer-based intrusion detection based on network behavior for IoT." In 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON), pp. 1–4. IEEE, 2018.

16. Krishnan, R., & Perumal, G. (2019). H2B2H protocol for addressing link failure in WSN. *Cluster Computing*, 22, 9687–9696.

17. Granjal, Jorge, Silva, Joao M., & Nuno, Lourenco. (2018). Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection. *Sensors*, 18, 8.

18. Ramadan, Rabie A. (2020). Efficient intrusion detection algorithms for smart cities-based wireless sensing technologies. *Journal of Sensor and Actuator Networks*, 9, 3.

19. Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL attack detection and prevention in the internet of things networks using a gru based deep learning. *IEEE Access*, 8, 183678–183689.

20. El-Saadawy, M.; Shaaban, E. Enhancing S-LEACH security for wireless sensor networks. In Proceedings of the 2012 IEEE International Conference on Electro/Information Technology, Indianapolis, IN, USA, 6–8 May 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1–6.

21. Ferreira, A.C.; Vilaça, M.A.; Oliveira, L.B.; Habib, E.; Wong, H.C.; Loureiro, A.A. On the security of cluster-based communication protocols for wireless sensor networks. In Proceedings of the International Conference on Networking, Reunion Island, France, 17–21 April 2005; pp. 449–458

22. Haseeb, K., Din, Ikram Ud, Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors*, 20, 7.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Rajkumar Krishnan is working as Assistant professor in the department of Information Technology at PSNA College of Engineering and Technology. He has 16 years of teaching experience in the departments of CSE and IT. He is a life member of ISTE. He has published many Scopus and SCI indexed journals. His area of interest includes Computer Network, Wireless sensor network etc.

R. Santhana Krishnan is currently working as an Assistant Professor, Dept of ECE in SCAD College of engineering and Technology, Tirunelveli. He has published several papers in International Journals. He has presented many papers in National and International conferences in IOT, Mobile Computing and Network Security. He has the Total Teaching Experience of 10 Years.

Y. Harold Robinson is currently working in the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore. He has received Ph.D. degree in Information and Communication Engineering from Anna University, Chennai in the year 2016. He is having more than 15 years of experience in teaching. He has published more than 50 papers in various International Journals and presented more than 45 papers in both national and International Conferences. He has written 4 book chapters by Springer, IGI global Publication. He is acting as an editor for a book Title as “Successful Implementation and Deployment of IoT Projects in Smart Cities”. IGI Global in the The Advances in Environmental Engineering and Green Technologies (AEEGT) book series. He is one of the editor for the book “Handbook of Research on Blockchain Technology: Trend and Technologies” publish by Elsevier. He is acting as a Reviewer of many journals like Multimedia Tools and Applications, Wireless Personal Communication by Springer Publication. He has given many Guest Lecturer in various subjects such as pointer, operating system, compiler design in Premier Institutions. He has also given an invited talk in technical symposium He has acted as a Convenor, coordinator and jury in National level and international IEEE Conferences, project fair and Symposium. He has attended various Seminars Workshops, and Faculty Development Programmes to enhance the knowledge of student’s community. His research area includes Wireless Sensor Networks, Ad-hoc Networks, Soft computing, blockchain, IoT and Image Processing. He has published research papers in various SCIE journals like wireless personal communication, IEEE access, Ad-hoc networks, Mobile networks and application, Journal of Ambient Intelligence and Humanized Computing, Peer-to-Peer...
E. Golden Julie is currently working as a Senior Assistant Professor in the department of computer science and Engineering, Anna university, Regional campus, Tirunelveli. She has received Ph.D degree in Information and Communication Engineering from Anna University, Chennai in the year 2017. Completed M.E degree in Computer Science and Engineering in Nandha Engineering College, Tamilnadu in the year 2008 and did her B.E Computer Science and Engineering in Tamilnadu college of Engineering, Coimbatore, Tamilnadu. She is having more than 12 years of experience in teaching. She has published more than 34 papers in various International Journals and presented more than 20 papers in both national and International Conferences. She has written 6 book chapters by Springer, IGI global Publication. She is acting as an editor for a book Title as “Successful Implementation and Deployment of IoT Projects in Smart Cities”. IGI Global in the The Advances in Environmental Engineering and Green Technologies (AEEGT) book series. She is one of the editor for the book “Handbook of Research on Block chain Technology: Trend and Technologies” publish by Elsevier. She is acting as a Reviewer of many journals like computers and electrical Engineering Elsevier publisher & got best reviewer certificate, Wireless Personal Communication by Springer Publication. She has given many Guest Lecturer in various subjects such as multi-core Architecture, operating system, compiler design in Premier Institutions. She has acted as a jury in National level and international IEEE Conferences, project fair and Symposium. She has attended various Seminars Workshops and Faculty Development Programmes to enhance the knowledge of student’s community. Her research area includes Wireless Sensor, Ad-hoc Networks, Soft computing, block chain, IoT and Image Processing. She has published research papers in various SCI journals like wireless personal communication, IEEE access, Ad-hoc networks, Mobile networks and application, Journal of Ambient Intelligence and Humanized Computing, Peer-to-Peer Networking and Applications, Journal of Intelligent & Fuzzy Systems, Computer Standards & Interfaces and Earth Science Informatics. She is an active life time member in Indian Society of Technical Education.

Hoang Viet Long received Ph.D. diploma in Computer Science at Hanoi University of Science and Technology in 2011, specializing in fuzzy computing and soft computing techniques with applications to electronic engineering. He has been promoted to Associate Professor since 2018. Recently, he has been concerned about Machine Learning with applications to Cybersecurity.
A. Sangeetha is working as Assistant professor in department of Information Technology at PSNA College of Engineering and Technology. She has 13 years of teaching experience in the departments of CSE and IT. She has published many journals. His area of interest includes Computer Network, Wireless sensor network etc.

M. Subramanian is working as an Assistant Professor in the Department of Computer Science and Engineering, SCAD College of Engineering and Technology, Tirunelveli. He has 10 years of teaching experience and he has published several journals and conferences. His area of interest includes Wireless Sensor networks, Internet of Things and Image Processing.

Dr. Raghvendra Kumar is working as Associate Professor in Computer Science and Engineering Department at GIET University, India. He received B. Tech, M.Tech and Ph.D. in Computer Science and Engineering, India, and Postdoc Fellow from Institute of Information Technology, Virtual Reality and Multimedia, Vietnam. He serves as Series Editor Internet of Everything (IOE): Security and Privacy Paradigm, Green Engineering and Technology: Concepts and Applications, publishes by CRC press, Taylor & Francis Group, USA, and Bio-Medical Engineering: Techniques and Applications. Published by Apple Academic Press, CRC Press, Taylor & Francis Group, USA. He also serves as acquisition editor for Computer Science by Apple Academic Press, CRC Press, Taylor & Francis Group, USA. He has published number of research papers in international journal (SCI/SCIE/ESCI/Scopus) and conferences including IEEE and Springer as well as serve as organizing chair (RICE-2019, 2020), volume Editor (RICE-2018), Keynote speaker, session chair, Co-chair, publicity chair, publication chair, advisory board. Technical program Committee members in many international and national conferences and serve as guest editors in many special issues from reputed journals (Indexed By: Scopus, ESCI, SCI). He also published 13 chapters in edited book published by IGI Global, Springer and Elsevier. His researches areas are Computer Networks, Data Mining, cloud computing and Secure Multiparty Computations, Theory of Computer Science and Design of Algorithms. He authored and Edited 23 computer science books in field of Internet of Things, Data Mining, Biomedical Engineering, Big Data, Robotics, and IGI Global Publication, USA, IOS Press Netherland, Springer, Elsevier, CRC Press, USA.
Authors and Affiliations

Rajkumar Krishnan¹ · R. Santhana Krishnan² · Y. Harold Robinson³ · E. Golden Julie⁴ · Hoang Viet Long⁵ · A. Sangeetha¹ · M. Subramanian⁶ · Raghvendra Kumar⁷

Rajkumar Krishnan
rajkumar4research@gmail.com
R. Santhana Krishnan
santhanakrishnan86@gmail.com
Y. Harold Robinson
yhrobinphd@gmail.com
E. Golden Julie
goldenjuliephd@gmail.com
A. Sangeetha
sangeetha@psnacet.edu.in
M. Subramanian
m.subramanian86@gmail.com
Raghvendra Kumar
raghvendraagrawal7@gmail.com

¹ Department of IT, PSNA College of Engineering and Technology, Dindigul, India
² Department of Electronics and Communication Engineering, SCAD College of Engineering and Technology, Tirunelveli, India
³ School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India
⁴ Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, India
⁵ Faculty of Information Technology, University of Technology–Logistics of Public Security, Bac Ninh, Vietnam
⁶ Department of Computer Science and Engineering, SCAD College of Engineering and Technology, Tirunelveli, India
⁷ Department of Computer Science and Engineering, GIET University, Gunupur, India