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

Rajkumar Krishnan
PSNA College of Engineering and Technology
R. Santhana Krishnan
SCAD College of Engineering and Technology
Y. Harold Robinson
VIT University
E. Golden Julie
Anna University Regional Campus
Hoang Viet Long (hoangvietlong@tdtu.edu.vn)
Ton Duc Thang University https://orcid.org/0000-0001-9883-9506
A. Sangeetha
PSNA College of Technology
M. Subramanian
SCAC College of Engineering
Raghvendra Kumar
GIET Unviersity

Research Article

Keywords: Wireless Sensor Network (WSN), Internet of Things (IoT), Anomalous Intrusion Detection Protocol (AIDP), Intrusion Prevention Protocol (IPP).

Posted Date: June 15th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-554397/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on March 15th, 2022. See the published version at https://doi.org/10.1007/s11277-022-09521-4.

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

Rajkumar Krishnan[1], R. Santhana Krishnan[2], Y. Harold Robinson[3], E. Golden Julie[4], Hoang Viet Long[5,6,*], A. Sangeetha[1], M. Subramanian[7], Raghvendra Kumar[8]

[1]Department of IT, PSNA College of Engineering and Technology, Dindigul, India, rajkumar4research@gmail.com, sangeetha@psnacet.edu.in
[2]Department of Electronics and Communication Engineering, SCAD College of Engineering and Technology, Tirunelveli, India. santhanakrishnan86@gmail.com
[3]School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India. yhrobinphd@gmail.com
[4]Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, India. goldenjuliephd@gmail.com
[5]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam;
[6]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam. hoangvietlong@tdtu.edu.vn
[7]Department of Computer Science and Engineering, SCAD College of Engineering and Technology, Tirunelveli, India. m.subramanian86@gmail.com
[8]Department of Computer Science and Engineering, GIET University, India raghvendraagrawal7@gmail.com

Abstract: Because of the headway of data and correspondence advances, the utilization of Internet of Things (IoT) gadgets has expanded dramatically. In the improvement of IoT, 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 is to accomplish dependability with the security of communicated information in a weak climate alongside pernicious hubs. This paper intends to build up an Anomalous intrusion detection protocol (AIDP) and Intrusion Prevention Protocol (IPP) for interruption evasion in IoT dependent on WSN to expand the organization's time frame and information reliability. Right off the bat, the proposed convention makes dissimilar energy-efficient groups dependent on the natural characteristics of hubs. 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 (BS) and group head are accomplished. The proposed security conspires demonstrates a trivial answer to adapt to interruptions produced by malignant hubs. The trial results utilizing the organization test system (NS-2) show that the proposed directing convention accomplished improvement as far as organization lifetime, end to end delay as 24%, packet delay ratio as 30%, when contrasted and the current work under unique organization geographies.

Keywords: Wireless Sensor Network (WSN); Internet of Things (IoT); Anomalous Intrusion Detection Protocol (AIDP); Intrusion Prevention Protocol (IPP).

1. Introduction

Internet of Things (IoT) is an overall correspondence foundation that comprises of various availability protests that give organizing, tactile, and data handling devices [1–4]. The essential topic of IoT is to give availability anyplace within the homogeneous articles. Radio-recurrence ID (RFID) [5–7] 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.

Remote sensor organizations [8–11] are an additional primary innovation for IoT that contains savvy objects known as the sensor hubs. These hubs 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 hubs, actualizing security for IoT frameworks is difficult to measure and correspondence may bargain with an assortment of organization assaults [12,13]. 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 [14,15] other than solid information sending. Previously, various scientists have been given a bunch-based answer for WSN to accomplish energy productivity [16 – 20]. In bunching plans, the hubs are isolated into various locales with single group leader alluded to as the pioneer hub.

The point of the group leader is to gather the information through the part hubs, total delivered packets across the base station (BS). The data communication from bunch leaders to BS might be cultivated neither exploiting distinct bounce nor several jump procedures. Probabilistic enabled techniques are mostly two sorts of bunching arrangements. In probabilistic procedures [21–25], groups are produced in haphazardly request, which brings about unequal burden conveyance and energy utilization. Then again, the non-probabilistic technique [26–29] have been utilized various variables for the choice of bunch 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 hubs [30–34], 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 organization correspondence 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 hubs and creates different energy-effective bunches by thinking about the nature of administration (QoS) prerequisites. The proposed approach is constructed for providing secure, extensible concerning the expansion in the organization 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.

The rest of this paper deals with different types of sections such as description of IoT in section 2, the section 3 is about wireless sensor network and the section 4 is literature survey and the last and final section is proposed work of two protocols such as AIDP and IPP with performance analysis. The conclude section is initialized.

2. Related works

Because of the progression of data and correspondence 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 hubs. This paper intends to build up an energy-proficient enabled secure routing protocol (ESR) for interruption shirking in IoT dependent on WSN to expand the organization time frame and information dependability. Right off the bat, the proposed convention makes dissimilar energy-proficient bunches dependent on the inherent characteristics of hubs. 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 (BS) and bunch leader are accomplished **[35]**.

The framework of wireless sensor networks (WSN) is organized in an impromptu way and coordinated hubs announcing the occasions to the Base Station (BS). A WSN is coordinated with savvy advances to grow quick Internet of Things (IoT) 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 hubs. Besides, because of restricted imperatives of sensor hubs with open availability of remote correspondences medium, information assurance against vindictive exercises should be upgraded with the least organization 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 organization conveyance proportion. 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 bunches dependability dependent on the vulnerability standard. 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 organization measurements **[36]**.

Internet of Things (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. Remote Sensor Networks (WSNs) 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. This work centers on building up a visual-helped device for uncovering security dangers in IP-empowered WSNs. The proposed device, called EyeSim, is a human intuitive visual-based abnormality location framework that is able to check and speedily alarming for the presence of wormhole joins. Moreover, it is equipped for showing the malignant hubs that

structure the wormhole connect. EyeSim may uncover foes by directing psychological organization information investigation dependent on powerful steering data. The adequacy of EyeSim is evaluated in the wording of location precision. The reproduction results show that EyeSim has the capacity to precisely distinguish numerous wormhole assaults continuously **[37]**.

The possibility of running a lightweight Intrusion Detection System inside an obliged sensor or IoT hub, we propose mIDS, which screens and recognizes assaults utilizing a measurable investigation device dependent on Binary Logistic Regression (BLR). mIDS takes as info just neighborhood hub boundaries for both kind and malevolent conduct and determines a typical conduct model that recognizes variations from the norm inside the obliged hub. We offer verification of right activity 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% **[38].**

As we as a whole realize that innovation is extended to be close to people very soon on the grounds of its comprehensive development. These days, we see 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 (ICT). Due to this headway, new registering and correspondence conditions, for example, the Internet of Things (IoT) 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. Yet, in the asset obliged climate of Wireless Sensor Network (WSN) and IoT, it is practically incomprehensible to build up a completely secure framework. As we are pushing ahead quickly, 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 we have to set up a hearty framework for keeping the previously mentioned conditions protected and normalized for the smooth conduction of correspondence among IoT objects. In this overview paper, we give the subtleties of the danger model relevant to the security of WSN and IoT based interchanges. We additionally talk about the security prerequisites and

different assaults conceivable in WSN and IoT based correspondence conditions. The arising activities of WSNs incorporated into IoT are additionally informed. We at that point give the subtleties of various designs of WSN and IoT-based correspondence conditions. Next, we examine the current issues and difficulties identified with WSN and IoT. We likewise give a basic writing review of late interruption identification conventions for IoT and WSN conditions alongside their similar investigation. A scientific categorization of security and protection conservation conventions in WSN and IoT is additionally featured. At last, we examine some exploration challenges which should be tended to in the coming future **[39].**

The intrusion detection system increased major centrality in the field of the web of things (IoT) as the conveying substances could arrive at a large number of hubs. 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 organization's conduct as opposed to hub conduct and the capacity to surmise the condition of the hub. A plan dependent on acquiring datasets identified with the bundle means ordinary and vindictive cases, gathered utilizing the wanton mode is received in the organization. The neighborhood location is directed by the devoted sniffers (DS) where each DS utilizes a regulated learning approach dependent on choice trees to create effectively characterized examples (CCIs). The worldwide stage gathers the CCIs sent from the devoted sniffers (DS) to the supernode (SN) and applies an iterative straight relapse to produce a time-sensitive profile called the aggregated proportion of variance (AMoF) for malignant and typical hubs. A profile of a malignant and an ordinary hub is gotten, and an abnormality is distinguished after three cycles (prepared examples) **[40].**

3. Proposed Work

3.1 Anomalous Intrusion Detective Protocol (AIDP)

A convention that changes trust and notoriety in view of hub 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 hubs by registering experience esteem dependent on the cautions produced by ATMP. The experience esteems are traded between the hubs and are utilized to refresh the notoriety and trust. This implies that a noxious or broken hub 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 hub 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 hubs figure notoriety dependent on the chronicled notoriety esteem, the immediate experience (if the hub is an indicator), and the roundabout experience (the got values). 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 hub. The convention is community since hubs 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 hub has the right to partake in the organization. While the trust in a hub is over sure breaking point, that hub can take an interest in detecting and correspondence activities. At the point when trust drops underneath the breaking point, the hub should be rejected from the network.

Three Phases:

1. **Learning**
2. **Trading**
3. **Refreshing**

The Learning Phase:

a) Each alarm got from TAFDS is converted into a discovery experience (just if the nearby hub is a finder).

b) For every hub that caused a caution, the experience esteem is refreshed utilizing in Eq. (1)

$$L_{new}(x) = \alpha L_{old}(x) + \sum_{j=1}^{m} \beta_j \; L_j(x) \; . \qquad (1)$$

L_{old} is the old evaluated value in old cycle, L_i detection process, m is the number of alarm based on x α_i,β_i are weightage. 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 hub keeps up the past estimation of the experience in Eq. (2).

$$\sum_{j=1}^{m} \beta_j \; L_j(x) = 1 \qquad (2)$$

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

The Trading Phase:

a) Every hub sends the experience related to its neighbors utilizing a transmission message.

b) Each hub holds on to get the arrangements of relationship from its neighbors for a predefined timeframe.

The Refreshing Phase:

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

$$U_{new}(x) = \gamma U_{old}(x) + \delta \; D_e(x) + \sum_{i=1}^{k} C_i L_i(x) \qquad (3)$$

$U_{old}$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 hub in Eq. (4).

$$\gamma + \delta \sum_{i=1}^{k} C_i L_i(x) = 1 \qquad (4)$$

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

$$D_{new}(x) = \tau\, D_{old}(x) + \emptyset\, U_{new}(x) \quad (5)$$

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. We think about that as an indicator hub, which remains in a steering way from the reviewed hub to the base station, has more aptitude than a finder hub not remaining on that directing way. In any case, contemplating the portability of hubs and the incessant difference in directing ways, we additionally consider the experience esteem dictated by other identifier hubs, as they may have past involvement in the examined hub. A total trust the executive's cycle comprises of a Learning, Exchanging, and Updating stage. Toward the finish of a cycle, every hub has refreshed the trust in different hubs.

3.2 Intrusion Prevention Protocol (IPP)

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 bunches in an energy-productive and adjusted way. Besides, the proposed bunching plan enhances network lifetime and force utilization proportion within the sensor hubs. 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 hubs. To accomplish solid information sending, the BS produces a mystery key, which is shared among chosen bunch leaders. In information sending from bunch heads, the information bundles are encoded utilizing the SSS system. Then again, BS remakes the inbound information bundles from bunch 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, start to finish delay, correspondence cost, number of course disclosures and organization overhead.

The utilization of residual energy through the RSSI within the BS and 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).

$$RSSI_{threshold} = \frac{Y}{n} \qquad (6)$$

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 nodel level. The Queue Length (QL) is computed in Eq. (7).

$$QL = \frac{RR}{TBS} \qquad (7)$$

At last, all the elements are summed up dependent on weighted methods as appeared in Eq. (8), and the hubs are designated as beginning bunch 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].

$$C = we_1 * s_i + we_2 * RSSI + we_3 * \left(\frac{1}{d_i \, to \, BS}\right) + we_4 * QL \qquad (8)$$

where the weighting factors are meant by $we_1, we_2, we_3, and\, we_4$ for different determination viewpoints, to be specific the hub'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 hubs, 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 hub is considered for the choice of the bunch head.

Cluster Updation:

As 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 organization measure.

i. At the point when any bunch head j gets the information parcel 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 bunch head gets another information bundle, yet it has no enough energy asset, i.e., er < 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).

$$CL = \frac{AvDR}{AvRR} \qquad (9)$$

where $AvDR$ demonstrates the mean delay ratio within the data packets and $AvRR$ denotes the mean reception rate of data packets.

4. Performance Analysis

Every hub sends guide bundles to its neighbors at a time frame fixed period. On getting signals bundles, the neighbor hub assesses its RSSI esteem and delivers back through the source hub. Eventually, the line length factor is fused in the determination system of the group leader, along these lines a hub is given a higher need to be chosen as a bunch 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 hub joins their nearby bunch head for the development of groups, after accepting the status messages. Typical hubs may get status messages from the neighboring group head and partner themselves with those

bunch leaders, containing the most grounded RSSI esteem. Toward the finish of the bunches arrangement measure, the IPP convention allocates an exceptional ID for all produced bunches to determine their limits. The arrangement of hubs chose as bunch heads declare channel access plans dependent on time-division numerous entrances (TDMA).

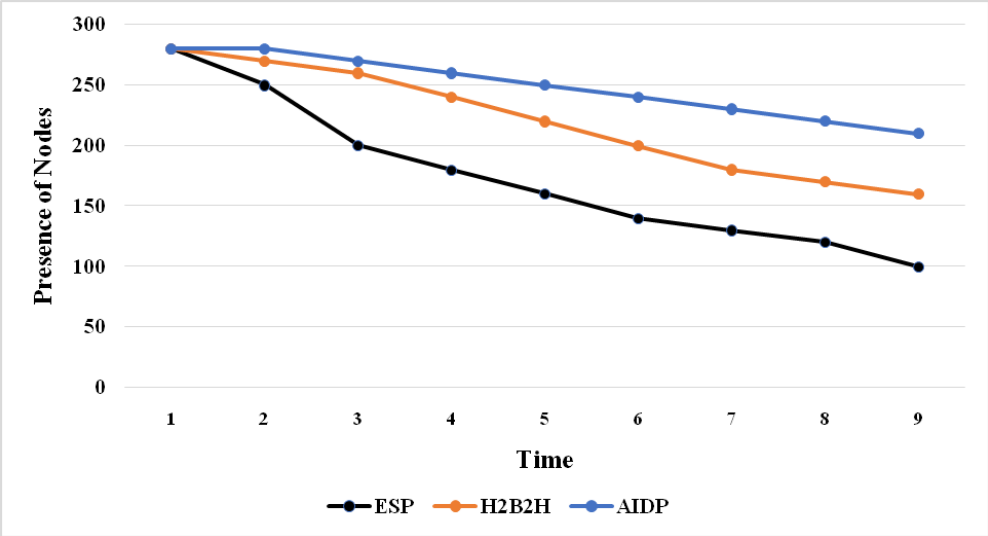

Figure 1: Network Life time

The development protocol is always concentrated on its network lifetime which plays an vital role of the wireless network to work with and the its depends on the presence of nodes within the network. Within minimum period of time the network should formed with maximum number of node in Fig. 1.

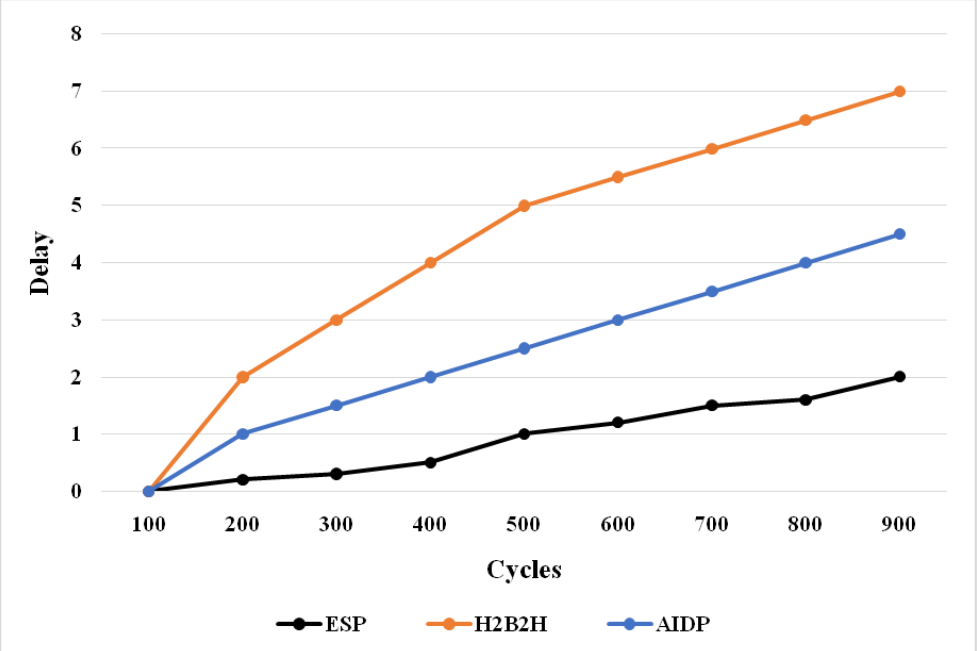

Figure 2: End-to-End delay

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. 2.

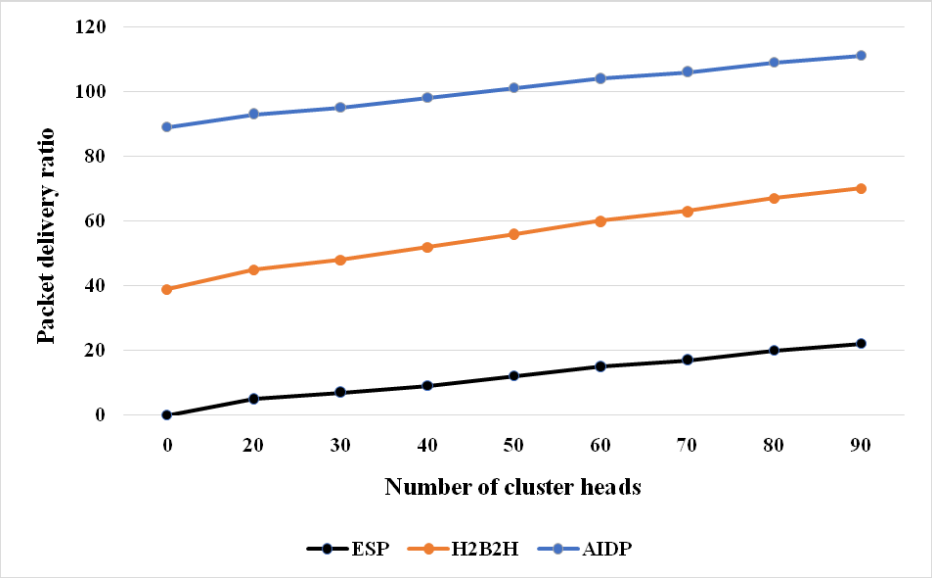

Figure 3: Packet delivery ratio

The packet delivery ratio of the network is the structure of network was the source of packet starts and the destination of the packet stops. Within this the nodes have the responsibility to achieve the maximum packet delivery ratio with maximum number of clusters which is demonstrated in Fig. 3.

5. Conclusion

The point of this paper was to introduce the Anomalous Intrusion Detection Protocol (AIDP) and Intrusion prevention protocol (IPP) convention for interruption safeguard in IoT dependent on remote sensor organizations. 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 hubs and high organization load situations. Essentially, AIDP streamlined the choice cycle of bunch heads and utilized a circulated methodology to create groups for consistent appropriation of energy utilization. Moreover, the higher estimations of RSSI and least organization clog improved the steering execution

regarding QoS limitations and information dependability. Besides, to accomplish a protected organization wide information steering against vindictive hubs, the AIDP convention embraced a light-weight mystery sharing plan within the group leaders and BS. This gave information security from hubs through the bunch heads to the BS against pernicious dangers. For future work, the proposed convention will be reached out by allowing for multi-bounce network correspondence alongside the versatility principles.

Declarations

The authors have no relevant financial or non-financial interests to disclose.

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. Internet of Things (IoT): A vision, architectural elements,and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660
2. Jing, Q.; Vasilakos, A.V.;Wan, J.; Lu, J.; Qiu, D. Security of the internet of things: Perspectives and challenges. Wirel. Netw. 2014, 20, 2481–2501.
3. Uckelmann, D.; Harrison, M.; Michahelles, F. An architectural approach towards the future internet of things.In Architecting the Internet of Things; Springer: Heidelberg, Germany, 2011; pp. 1–24.
4. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. J. Netw. Comput.Appl. 2014, 42, 120–134.
5. 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.

6. Koch, M.J.; Swope, C.B.; Bekritsky, B.J. System for, and Method of, Accurately and Rapidly Determining,in Real-Time, True Bearings of Radio Frequency Identification (RFID) Tags Associated with Items in a Controlled area. U.S. Patent 9,773,136, 26 September 2017.
7. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. Ad Hoc Netw. 2012, 10, 1497–1516.
8. 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.
9. Mahajan, S.; Malhotra, J.; Sharma, S. An energy balanced QoS based cluster head selection strategy for WSN.Egypt. Inf. J. 2014, 15, 189–199.
10. Mehrani, M.; Shanbehzadeh, J.; Sarrafzadeh, A.; Mirabedini, S.J.; Manford, C. FEED: Fault tolerant, energy efficient, distributed clustering for WSN. In Proceedings of the 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 7–10 February 2010; pp. 580–585.
11. Tarigh, H.D.; Sabaei, M. A new clustering method to prolong the lifetime of WSN. In Proceedings of the 2011 3rd International Conference on Computer Research and Development (ICCRD), Shanghai, China, 11–13March 2011; pp. 143–148.
12. Ning, H.; Liu, H.; Yang, L.T. Cyberentity security in the internet of things. Computer 2013, 46, 46–53.
13. Pirbhulal, S.; Zhang, H.; Alahi, M.E.E.; Ghayvat, H.; Mukhopadhyay, S.C.; Zhang, Y.-T.; Wu, W. A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors 2017, 17, 69.
14. Sharma, N.; Sharma, A.K. Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network. Sadhana 2016, 41, 283–288.
15. Wang, K.;Wang, Y.; Sun, Y.; Guo, S.;Wu, J. Green industrial Internet of things architecture: An energy-efficient perspective. IEEE Commun. Mag. 2016, 54, 48–54.
16. Abo-Zahhad, M.; Ahmed, S.M.; Sabor, N.; Sasaki, S. Mobile sink-based adaptive immune energy-efficientclustering protocol for improving the lifetime and stability period of wireless sensor networks. IEEE Sens. J.2015, 15, 4576–4586.

17. Batra, P.K.; Kant, K. LEACH-MAC: A new cluster head selection algorithm for wireless sensor networks. Wirel. Netw. 2016, 22, 49–60.
18. Chen, G.; Li, C.; Ye, M.; Wu, J. An unequal cluster-based routing protocol in wireless sensor networks. Wirel.Netw. 2009, 15, 193–207.
19. Hassanabadi, B.; Shea, C.; Zhang, L.; Valaee, S. Clustering in vehicular ad hoc networks using anity propagation. Ad Hoc Netw. 2014, 13, 535–548.
20. Xiong, Z.; Guo, T.; Xue, Z.; Cai, W.; Cai, L.; Luo, N. Online energy-efficient deployment based on equivalent continuous DFS for large-scale web cluster. Clust. Comput. 2018, 22, 583–596.
21. 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.
22. Irkhede, T.; Jaini, P. Cluster and trac distribution protocol for energy consumption in wireless sensor network. In Proceedings of the 2013 Students Conference on Engineering and Systems (SCES), Allahabad,India, 12–14 April 2013; pp. 1–5.
23. Khalil, E.A.; Ozdemir, S. Reliable and energy efficient topology control in probabilistic wireless sensor networks via multi-objective optimization. J. Supercomput. 2017, 73, 2632–2656.
24. Tarachand, A.; Kumar, V.; Raj, A.; Kumar, A.; Jana, P.K. An Energy efficient Load Balancing Algorithm for cluster-based wireless sensor networks. In Proceedings of the 2012 Annual IEEE India Conference(INDICON), Kochi, India, 7–9 December 2012; pp. 1250–1254.
25. Younis, O.; Fahmy, S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. Mob. Comput. IEEE Trans. 2004, 3, 366–379.
26. 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.
27. Bednarczyk, W.; Gajewski, P. An enhanced algorithm for MANET clustering based on weighted parameters.Univers. J. Commun. Netw. 2013, 1, 88–94.

28. Chauhan, N.; Awasthi, L.K.; Chand, N.; Chugh, A. A Distributed Weighted Cluster Based Routing Protocol for MANETs. In Computer Networks and Information Technologies; Springer: Heidelberg, Germany, 2011;pp. 147–151.
29. Muthuramalingam, S.; RajaRam, R.; Pethaperumal, K.; Devi, V.K. A dynamic clustering algorithm for MANETs by modifying weighted clustering algorithm with mobility prediction. Int. J. Comput. Electr. Eng.2010, 2, 709–714.
30. Mittal, N.; Singh, U.; Sohi, B.S. A stable energy efficient clustering protocol for wireless sensor networks.Wirel. Netw. 2017, 23, 1809–1821.
31. Wang, Feng, and Jiangchuan Liu. "Networked wireless sensor data collection: issues, challenges, and approaches." IEEE Communications Surveys & Tutorials 13, no. 4 (2010): 673-687.
32. Luong, Nguyen Cong, Dinh Thai Hoang, Ping Wang, Dusit Niyato, Dong In Kim, and Zhu Han. "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey." IEEE Communications Surveys & Tutorials 18, no. 4 (2016): 2546-2590.
33. S. Ehsan and B. Hamdaoui, ``A survey on energy-efcient routing techniques with QoS assurances for wireless multimedia sensor networks,"IEEECommun. Surveys Tuts., vol. 14, no. 2, pp. 265278, May 2012.
34. M. A. Mehaseb, Y. Gadallah, A. Elhamy, and H. Elhennawy, ``Classification of LTE uplink scheduling techniques: An M2M perspective," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 13101335, 2nd Quart., 2016.
35. Haseeb, Khalid, Ahmad Almogren, Naveed Islam, Ikram Ud Din, and Zahoor Jan. "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN." Energies 12, no. 21 (2019): 4174.
36. Haseeb, Khalid, Naveed Islam, Ahmad Almogren, and Ikram Ud Din. "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things." Ieee Access 7 (2019): 185496-185505.
37. 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.
38. 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.

39. Pundir, Sumit, Mohammad Wazid, Devesh Pratap Singh, Ashok Kumar Das, Joel JPC Rodrigues, and Youngho Park. "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges." IEEE Access 8 (2019): 3343-3363.
40. 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.