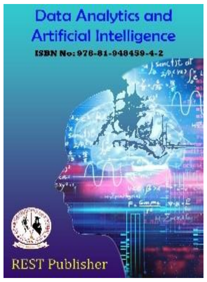
Data Analytics and Artificial Intelligence
Vol: 3(7), 2023
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/daai/


Data Analytics and Artificial Intelligence
ISBN No: 978-81-948459-4-2
REST Publisher

Hierarchical Model with Hash Based Intruder Algorithm Using IntrusionDetection System in Wireless Sensor Network

*G. P. Logesh
MGR College, Hosur, Tamil Nadu, India.
*Corresponding Author Email: lokeshpuk@gmail.com

Abstract: *Wireless Sensor Network is one of the most significant parts in the field of Communication Technology since it costs fewer establishment charges and has a straightforward network operation. In the present day, WSN is utilized broadly in every one of the significant segments which requires classification and security; subsequently, WSN requires an extremely advanced security system. Wireless Sensor Networks (WSNs) comprises of little sensor hubs sent in different geographic conditions to accumulate the data about the earth. The Intrusion Detection System (IDS) in Wireless Sensor Network is utilized to identify different assaults happening on sensor hubs of WSNs that are put in different threatening situations. This paper proposed to Rule-based hierarchical model and Hash-based intruder algorithm utilizing the Intrusion Detection System process. The presentation of the proposed plan is assessed utilizing different measurements, for example, Throughput, Traffic Ratio, Detection Ratio and Accuracy Ratio.*

Keywords: *Hierarchical Model, Intruder Algorithm, Throughput, Detection Ratio, IDS.*

1. INTRODUCTION

One of the most definitely developing, sensor hub based wireless networks is Wireless Sensor Network (WSN). The sensor hubs sent in WSN can speak with each other. The Wireless Sensors Nodes may speak with different hubs by confirming the predefined properties, for example, hub ID, conduct, Security component, and so forth. So now the very first moment of the rising examination territories is a wireless sensor network. The applications under WSN are developing quickly consistently. The wireless sensor network is independent sensors appropriated spatially. It is utilized something like recognize the ecological conditions in both physical and natural conditions. It finds a significant application in all situations, particularly in combat zone observation, modern applications, and so forth. Information is passed from source hub to goal hub with the assistance of middle hubs in the course. Besides in this network, there are various sensorswhere the sensors speak with the little hubs utilizing radio connections. The network contains various sensor hubs with a base station. As of late, the circulated sensor networks have comparable gathering hubs having the capacity of self-sorting out. These networks can be connected to open networks too with requirement hubs. Because of this property, the network is inclined to numerous assaults. This hardship is made for the security of the networks. Numerous kinds of research are at stake to ponder on the security of WSNs. The dangers by which the majority of the networks are enduring like interferences or approaching of infused pernicious packets to the hubs. The objective is set to the sensor hubs to gather the data by checking and recording the procedure and conduct of the hubs to improve the advancement in WSNs. Intrusion detection systems for PCs give exhaustive safeguards against wholesale fraud, data mining, and network hacking. Enormous organizations and government offices utilize such programming to protect data and records just as screen the network exercises of workers to guarantee nearby offices are not being abused. In any case, for every one of the favorable circumstances, intrusion detection systems are hampered bythe powerlessness to tell pernicious movement from unplanned or legal action and may secure a network causing loss of work and income. The intrusion detection system (IDS) way to deal with security is based on the supposition that a system won't be secure, yet that infringement of security arrangement (intrusions) can be distinguished by checking and breaking down system behavior.

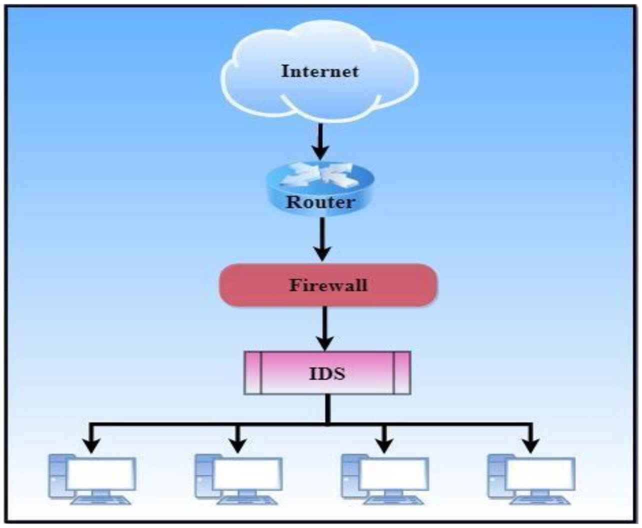


FIGURE 1. Overview of Intrusion Detection System

IDS systems guarantee to identify enemies whenthey are in the demonstration of assault Monitor operation, Trigger relief method on detection, Monitor: Network, Host, or Application occasions. IDS systems truly allude to two sorts of detection innovations Anomaly Detection, Misuse Detection. The multi- bounce dispersed systems include greater intricacy in a security assault. In this sort of condition, there is significant trouble in finding assailants or the malevolent hubs. To dealwith numerous assaults it is a need to plan another system. Probably the best answer for giving protection from a few assaults is an Intrusion Detection System (IDS). Wireless sensor hubs gather the data from nature and send it to the base station. Data needs security from the assailants. Cryptographic security isn't sufficient as it can shield the network from untouchable assaults as it were. So The need a second line of guard like an intrusion detection system (IDS). IDS screen the traffic of the network and on the off chance that any pernicious movement found by any hub, at that point sends an alarm message to the base station with the hub data. The IDS is conveyed on every hub which can get to the data of the hub and neighbor table. At the point when a parcel is transmitted by the hub, the IDS screen the packet. The assailant can assault on a hub and can transmit counterfeit packet into the network to lessen the battery life of the hubs. IDS screen every hub and check is if every one of the hubs is transmitting packet inside the fixed timeframe.

2. LITERATURE SURVEY

Lyes Bayou, Nora Cuppens-Boulahia, David Espes and Frédéric Cuppens(2015) Proposed towards a based intrusion detection organization conspire for verifying modern wireless sensor networks. proposed a proficient IDS sending plan exceptionally custom fitted to fit WISN qualities. It manufactures a virtual wireless spine that adds security purposes to the WISN. an organization conspires for the situation of the IDS- specialist of a decentralized IDS in a Wireless Industrial Sensor Network. To approve the organization conspires, correspondence with regards to WSN was modeled and afterwardit was demonstrated that this plan satisfies the characterized security necessities. It very well may be utilized either in decentralized, bunched or hierarchical models. It makes a virtual spine that adds security purposes to a current sensor network. It can adjust the sending plan to be utilized in heterogeneous networks in which gadgets don't have similarcapacities as far as transmission range, stockpiling and computational resources.

Merits

- To guarantee the modern procedure progression in a safe condition, it is significant that information sent by these sensors is adequately gotten by the fundamental station and in a suitable time.
- End-to-end correspondence.
- It is improved to transmission range, stockpiling and computational assets.

Demerits

- IDS items that point of confinement its viability as a security arrangement Performance Barriers Detection Accuracy, Product Complexity, Growing IDS Evasion, Passive Device and Enterprise Scalability.

Jian Li, Yun Liu, Zhenjiang Zhang, Bin Li, Hui Liu, Junjun Cheng (2018) Proposed an Efficient ID-based message verification with improved security in wireless impromptu networks. the proposed plan can accomplish improved protection which can guard against full key introduction assault. Additionally officially demonstrate that the proposed IMAEP plan can accomplish unlimited security and enforceability. Open key cryptosystems have the less difficult key the board and are simpler to scale, in this manner are increasingly reasonable for message validation. Among a wide range of open key cryptosystems, a personality-based cryptosystem is the most alluring since people in general keys can be determined locally.

Merits

- The plot has a lot of lower computational overhead.
- The plan can hold unqualified security.

Demerits

- Requires a unified server: IBE's brought together approach infers that a few keys must be made and held retained and are accordingly at more serious danger of divulgence.
- Requires a protected channel between a sender or beneficiary and the IBE server for transmitting the private key.

Mert Melih OZCELIK, Erdal IRMAK, Suat OZDEMIR (2017) Proposeda half and half trust-based intrusion detection system for wireless sensor networks. The proposed IDS is based on practical notoriety and abuse detection rules. The primary thought is that every sensor hub figures utilitarian notoriety esteems for its neighbors by watching their exercises. Base Station (BS) recognizes malignant hubs by joining utilitarian notoriety esteems and abuse detection rules. half breed trust-based IDS for WSNs is proposed and a starter assessment of the plan is displayed. Practical notoriety based trust assessment is utilized with the abuse detection approach in the proposed system. Every hub ascertains trust estimations of its neighbors by considering theirpractices utilizing pre-characterized useful notoriety measurements. This immediate perception esteems are traded among hubs and combined trust esteems are registered.

Merits

- The approach builds the network's lifetime.
- It improves detected information freshness by recognizing noxious hubs ina concentrated manner without flooding vitality utilization.

Demerits

- Weaknesses of abuse based detection are to have high detection rates toknown assaults and low bogus positive rates.

Geethapriya Thamilarasu, Zhiyuan Ma (2015) Proposed the self-governingversatile operator based intrusion detection structure in wireless body region networks. A self-governing versatile operator based intrusion detection engineering to address securityin wireless body territory networks. numerous portable operators based intrusion detection system is created for wireless body region networks, where learning and basic leadership is appropriated among various hubs in the network. Body sensor hubs are equipped for performing nearby detection utilizing the assault highlights accessible. in the restricted detecting locale, while portal hubs and servers are equipped for performing worldwide assault detection. The assault detection methods must be intended to adapt to network portability, computational power and memory requirements.

Merits

- Reduced Network Load through code and information scattering.
- Fault Tolerance.
- Reduced Power Consumption.
- Improved Scalability.
- Reduced Complexity.
- Higher Accuracy

Demerits

- Wireless body territory networks contain an absence of an honesty sensor.
- Interference of multi gadgets that offer the channel.

Mohamed Guerroumi, Abdelouahid Derhab, Kashif Saleem (2015) Proposed an Intrusion detection system against SinkHole assault in wireless sensor networks with portable sink. The proposed IDS think about two sorts of sink portability: intermittent and arbitrary. So as to distinguish the sinkhole assault, to utilize a mark basedstrategy. The decision is because of the portability of the sink that can be misused by the sinkhole assault. The proposed plan is based on a hierarchical topology to verify any bunch based directing conventions. Utilizing marks procedure that speaks to the detectioninformation pace of a cell, conveying a recreated bogus versatile sink. Cell pioneers enacttheir IDS just when the sinkhole occasion happens. This licenses to diminish the number of hubs running their IDS and limit vitality utilization.

Merits

- The productivity of the proposed IDS as far as detection rate, proficiency,and vitality utilization.

Demerits

- The significant disadvantage of this plan is that it presents extra deferral bypassing those hubs that have low vitality levels. Thus, looking for high remaining vitality sensor hubs expend a lot of time and furthermore increment the voyaging cost of the portable sink.

3. PROPOSED WORK

Rule Based Hierarchical Model Using Intrusion Detection System We propose a model for sparing the power devoured by the hubs while executing an intrusion detection system in wireless sensor networks. As appeared in figure 2, this model pursues hierarchical engineering. The entire system is partitioned into littler parts (called cells). Every phone demonstrates the sensory furthest reaches of a hub and the hub is called bunch head hub. It must be underlined that, dissimilar to the customary IDS models like our proposed algorithm doesn't really require orchestrating the sensors in the system altogether. This implies the quantity of the sensors in the cells can be adaptable. The system topology might be changed. In the proposed algorithm, the fixed hubs in the network are restricted to the local and group head hubs as it were. These hubs ought to bechosen at the beginning of planning the network by the base station.

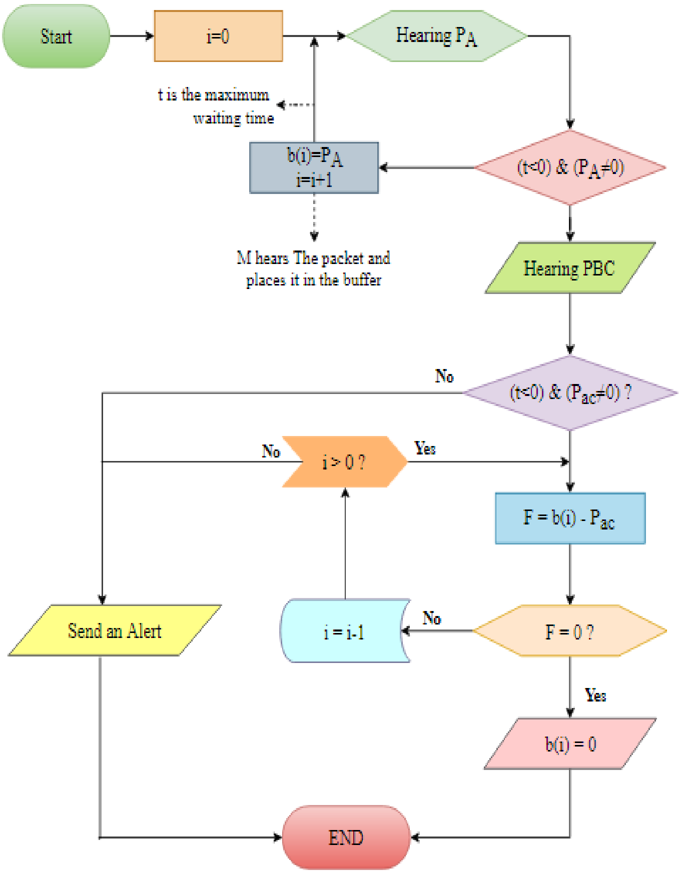


FIGURE 2. Proposed Work OverflowAlgorithm 1: Hash Based Intruder Algorithm

1. BS distributes key KEY to all the cluster heads and cluster heads distribute thekey to member nodes of the cluster
2. All the associated nodes of cluster, announce their encrypted hashed valueconsisting of ID and location to cluster head as under

SNci <- ID " (Ni (u , v))

H(Ni] <- KEY(M [IV(SNci)])
{ IV is the Initial Vector
{ M is message Digest Function, H stands for Hash}
{ H(Ni) is the message to be sent to cluster head}

3. Hsum(CNi] <- H(L (H(Ni)) for i=1 to n in cluster, H is the hashing function, node Ni are the member nodes, CNi is the cluster head
4. TH8S <- L Hsum[CNi] for i=1 to m , m is the cluster number {TH8S is computed hash total at BS}

In the foundation stage while laying off the decentralized group network each sensor hub Ni is recognized by its topographical area (ui,vi). As a matter of first importance, BS will appropriate (KEY) to all the bunch heads. The bunch head will understudy disperse the way into all the sensor hubs appended 106 ~ 1 to it. The sensor hubs intern will report their position (ui,vi) and area-id by encoding it with the encryptionwork KEY. The group head subsequent to getting the message will unscramble it and willhash the message with a reasonable introduction vector. The qualities from every one of the hubs will be decoded with unscrambling capacity DKEY, and hashed up. The hash anincentive from all related hubs will be scrambled and summarized at the group hub. At long last, the total is likewise hashed. So there is a net added keyed hash an incentive at the bunch hub. Toward the end-all, group head will answer to the 8S and all the keyed hashed values from the bunch heads will be summarized at the BS.

Algorithm 2: Detecting Malicious Nodes

1) A sends a packet to C via B. meanwhile, M (the cluster head node) eavesdrops the packet saves a copy in its counterpart section in buffer b.
2) The node M eavesdrops to the communication between B and C for t second (this time depends on the nodes processing and sending speed as well as the sensors type)and refers to the step 5 in the case of not receiving any packet.
3) The F_i value is calculated if M hears the P_{BC}.
If F_i=0, the message in cell bi (where its counterpart message has been savedin buffer b) will be deleted and the algorithm moves to the step 6. If $F_i \neq 0$, the message remains in the buffer and moves to step 5.
4) The warning message, signaling the maliciousness of the node B, is sent to the upper layer by the cluster head node.
5) The end of the algorithm

4. EXPERIMENTAL RESULTSTHROUGHPUT

TABLE 1. Comparison table of Throughput Ratio

EEACK Algorithm	**Watchdog Algorithm**	**Proposed Hash Based Intruder Algorithm**
0.09	0.04	**0.13**
0.14	0.08	**0.2**
0.19	0.13	**0.28**
0.25	0.19	**0.39**
0.3	**0.22**	**0.45**

The comparison table of Throughput Ratio shows the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. While comparing the EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm, the Proposed Hash Based Intruder Algorithm values provide the better results. The EEACK Algorithm value starts from 0.09 to 0.3, the Watchdog Algorithm values starts from 0.04 to 0.22 and the Proposed Hash Based Intruder Algorithm values starts from 0.13 to 0.45. The Proposed Hash Based Intruder Algorithm provides the great results compared to other algorithms.

The comparison chart of Throughput Ratio demonstrates the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. The above chart shows the no of nodes in X axis and throughput ratio in Y axis. The EEACK Algorithm value starts from 0.09 to 0.3, the Watchdog Algorithm values starts from 0.04 to 0.22 and the Proposed Hash Based Intruder Algorithm values starts from 0.13 to 0.45. The Proposed Hash Based Intruder Algorithm provides the great results compared to other algorithms.

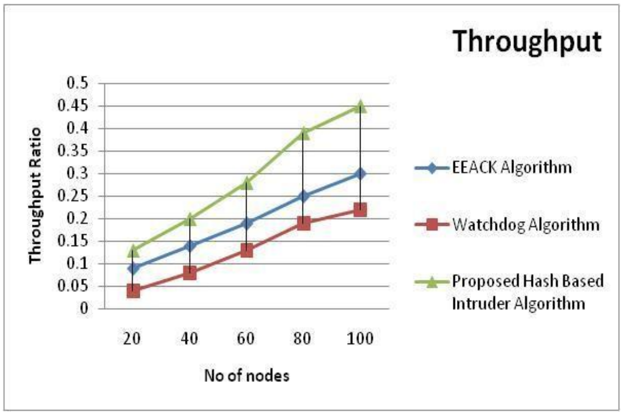


FIGURE 3. Comparison Chart of Throughput Ratio

Traffic Ratio

TABLE 2. Comparison table of Traffic Ratio

EEACK Algorithm	Watchdog Algorithm	Proposed Hash Based Intruder Algorithm
31.9	39	26.77
37.7	45	31.98
42.6	49	34.56
50.4	55	38.92
55.23	58	44.56

The comparison table of Traffic Ratio shows the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. While comparing the EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm, the Proposed Hash Based Intruder Algorithm values provide the better results. The EEACK Algorithm value starts from 31.9 to 55.23, the Watchdog Algorithm values starts from 39 to 58 and the Proposed Hash Based Intruder Algorithm values starts from 26.77 to 44.56. The Proposed Hash Based Intruder Algorithm provides the low traffic ratio compared to other algorithms.

The comparison chart of Traffic Ratio demonstrates the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. The above chart shows the no of nodes in X axis and traffic ratio in Y axis. The EEACK Algorithm value starts from 31.9 to 55.23, the Watchdog Algorithm values starts from 39 to 58 and the Proposed Hash Based Intruder Algorithm values starts from 26.77 to 44.56. The Proposed Hash Based Intruder Algorithm provides the better results compared to other algorithms.

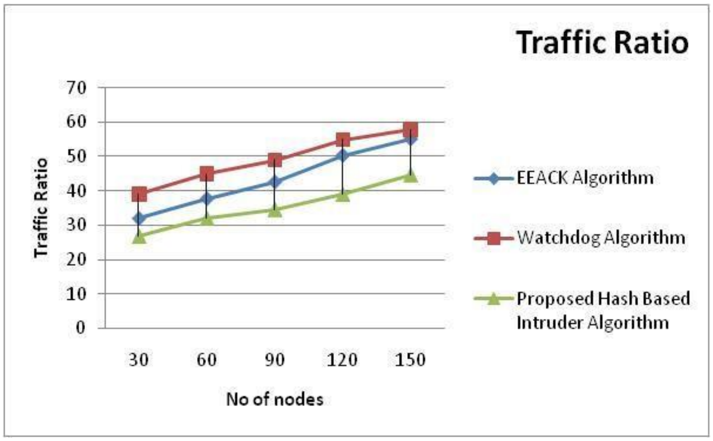


FIGURE 4. Comparison Chart of Traffic Ratio

Detection Ratio

TABLE 3. Comparison table of Detection Ratio

EEACK Algorithm	Watchdog Algorithm	Proposed Hash Based Intruder Algorithm
33	55	75
39	58.6	78.9
42	62.3	83.86
48.6	68.9	88.21
50.76	72	92.06

The comparison table of Detection Ratio shows the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. While comparing the EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm, the Proposed Hash Based Intruder Algorithm values provide the better results. The EEACK Algorithm value starts from 33 to 50.76, the Watchdog Algorithm values starts from 55 to 72 and the Proposed Hash Based Intruder Algorithm values starts from 75 to 92.06. The Proposed Hash Based Intruder Algorithm provides great results compared to other algorithms.

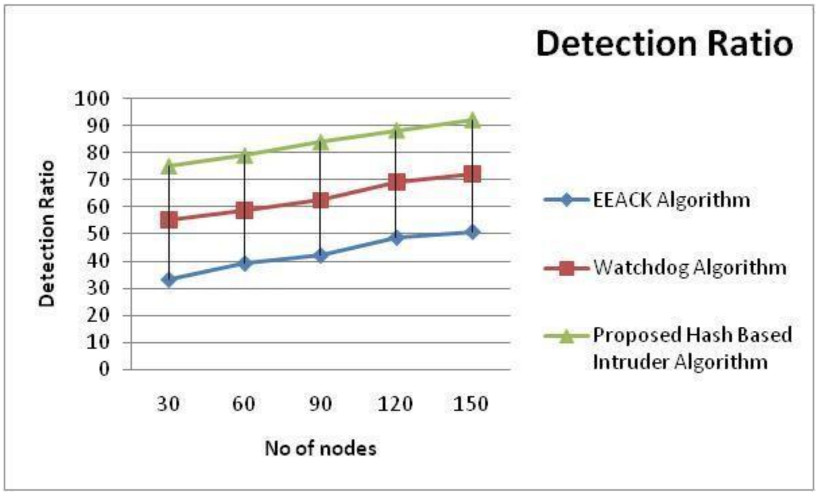


FIGURE 5. Comparison Chart of Detection Ratio

The comparison chart of Detection Ratio demonstrates the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. The above chart shows the no of nodes in X axis and detection ratio in Y axis.The EEACK Algorithm value starts from 33 to 50.76, the Watchdog Algorithm values starts from 55 to 72 and the Proposed Hash Based Intruder Algorithm values starts from 75 to 92.06. The Proposed Hash Based Intruder Algorithm provides great results compared to other algorithms.

Accuracy Ratio

TABLE 4. Comparison table of Accuracy Ratio

EEACK Algorithm	Watchdog Algorithm	Proposed Hash Based Intruder Algorithm
22	7	35
27	15	39
35	20	44
44	22	56
51	26	60

The comparison table of Accuracy Ratio shows the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. While comparing the EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm, the Proposed Hash Based Intruder Algorithm values provide the better results. The EEACK Algorithm value starts from 22 to 51, the Watchdog Algorithm values starts from 7 to 26 and the

Proposed Hash Based Intruder Algorithm values starts from 35 to 60. The Proposed Hash Based Intruder Algorithm provides great results compared to other algorithms.

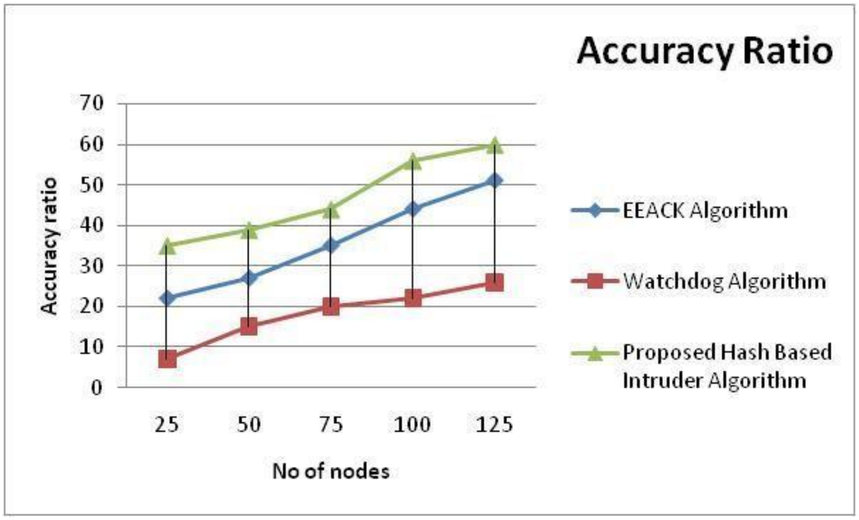


FIGURE 6. Comparison Chart of Accuracy Ratio

The comparison chart of Accuracy Ratio demonstrates the different values of EEACK Algorithm, Watchdog Algorithm and the Proposed Hash Based Intruder Algorithm. The above chart shows the no of nodes in X axis and accuracy ratio in Y axis.The EEACK Algorithm value starts from 22 to 51, the Watchdog Algorithm values starts from 7 to 26 and the Proposed Hash Based Intruder Algorithm values starts from 35 to 60. The Proposed Hash Based Intruder Algorithm provides great results compared to other algorithms.

5. CONCLUSION

Wireless sensor Networks are broadly utilized in numerous applications traversing from industry to look into zones. One of the significant restrictions in the WSNis the constrained power hotspots for the hubs. The life of the network, as a rule, is legitimately related to the life of its capacity sources. There are different assaults on the WSN focusing on the power utilization of the network with sham undertakings and enactments to lighten life and usefulness. In this paper, another Hash-Based Intruder algorithm is proposed to drag out the sensor hubs (and the network) Lifetime. Theproposed algorithm is another hierarchical engineering over the traditional confinements on the fixed situations for network hubs. The fixed hubs in the network are constrained tothe local and cluster heads as they were.

REFERENCES

[1]. Lyes Bayou, Nora Cuppens-Boulahia, David Espes and Frédéric Cuppens,” Towards a CDS-Based Intrusion Detection Deployment Scheme for SecuringIndustrial Wireless Sensor Networks”, © 2016 IEEE.

[2]. Jian Li, Yun Liu, Zhenjiang Zhang, Bin Li, Hui Liu, Junjun Cheng,” Efficient ID-based Message Authentication with Enhanced Privacy in Wireless Ad-hoc Networks”, ©2018 IEEE.

[3]. Mert Melih OZCELIK, Erdal IRMAK, Suat OZDEMIR,” A Hybrid Trust Based Intrusion Detection System for Wireless Sensor Networks”, ©2017 IEEE.

[4]. Geethapriya Thamilarasu, Zhiyuan Ma,” Autonomous Mobile Agent based Intrusion Detection Framework in Wireless Body Area Networks”, 2015 IEEE.

[5]. Mohamed Guerroumi, Abdelouahid Derhab, Kashif Saleem,” Intrusion detection system against SinkHole attack in wireless sensor networks with mobile sink”, © 2015 IEEE.

[6]. Imad Jawhar, Farhan Mohammed, Jameela Al Jarood , and Nader Mohamed,” TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks”, 2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance.

[7]. Alexander Basan, Elena Basan, Oleg Makarevich,” A Trust Evaluation Methodfor Active Attack Counteraction in Wireless Sensor Network”, © 2017 IEEE

[8]. Chen Chenl, Xiaomin Liu,Hualin Qi,Liqiang Zhao , Zhiyuan Ren,” A Security Enhancement and Energy Saving Clustering Scheme In Smart Grid Sensor Network”, ©2015 IEEE.

[9]. Christiana Ioannou, Vasos Vassiliou and Charalampos Sergiou,” An Intrusion Detection System for Wireless Sensor Networks”, ©2017 IEEE.

[10]. Qing Tang, Jian Wang,” A Secure Positioning Algorithm against Sybil Attack in Wireless Sensor Networks Based on Number Allocating”, 2017 17th IEEE International Conference on Communication Technology.

[11]. Alex Ramos, Marcella Lazar, Raimir Holanda Filho, Joel J. P. C. Rodrigues,” A Security Metric for the Evaluation of Collaborative Intrusion Detection Systems in Wireless Sensor Networks”, IEEE ICC 2017 SAC Symposium Internet ofThings Track.

[12]. Jessye Dos Santos, Christine Hennebert, Cedric Lauradoux,” Preserving Privacyin secured ZigBee Wireless Sensor Networks”, ©2015 IEEE.

[13]. Umashankar Ghugar, Jayaram Pradhan,” NL-IDS: Trust Based IntrusionDetection System for Network layer in Wireless Sensor Networks”, ©2018 IEEE.

[14]. Ting Bao, Zhangqin Huang, Da Li, “Data Loss and Reconstruction for WirelessEnvironmental Sensor Networks”, © 2017 IEEE.

[15]. Hui Li, Xiaoyu Du, Zhijie Han,” A Coverage Algorithm in Circular Area Based onPolar Coordinates for WSNs”, ©2018 IEEE.