International Journal of Advanced Science and Technology
Vol. 28, No. 13, (2019), pp. 961-971

# Multi-Level Authentication (MLA) For Wireless Sensor Networks Using Artificial Intelligence

1Dr. B. Raja Rao, 2Dr. B. B. M. Krishna Kanth

*1Associate professor &HOD, Department of ECE, Dadi institute of engineering and technology, Anakapalle, Visakhapatnam District, A.P, India*

*2Professor, Department of ECE , Anurag Engineering College, Kodada, Telangana, India*

## Abstract

Wireless sensor applications deployed in different types of domains due to its vast applications such as the medical field, metering system, research and development area, industrial machinery monitoring, etc. One of the big problem and challenge with this network is intrusion detection .whenever sensor nodes are communicating with each other they don`t know either its conjugative node is authorized node or not if node authorized node there is no problem in the exchange of sensitive data if it is not then the problem will arise. In this case, it is essential to find out the type of intruder; in this Manuscript, the proposed algorithm can quickly solve this problem by using the multilevel authentication using Artificial Intelligence. If any sensor node wants to join in the network, it must authenticate itself with the nearest server with the multilevel authentication mechanism; once the authentication is successful, then only it can get the permissions to exchange the sensitive data with its conjugative node.

***Keywords:*** *Artificial intelligence, wireless sensor network, sensor nodes,authentication, unauthorized node, encryption, decryption, sensitive data.*

## 1. Introduction

In the current era the applications of wireless sensor network has increased day-by-day rapidly in the human lives due to their vast applications in the different types of domains like energy metering system, medical applications-commercial applications, industrial machinery monitoring, SCADA applications, etc, In the olden days traditional message exchanged methods are consuming much more time and manual power, Whenever wireless sensor network has came in the human life these two problems quickly solve because these sensor networks can easily carry the information from one place to another place[1]. But one of the most significant issues in this network is, whenever nodes are exchanging sensitive data, there is a chance to hack this information by the hackers. Hence the consumer or the organization can lose their privacy. Thus It is challenging thing to maintain the confidentiality in the communication, by finding out the intruder in the communication network [2], many authors proposed their algorithms to find out these intruders but in this manuscript, the proposed algorithm was a sophisticated algorithm which is called Multi-Level Authentication (MLA) by Using Artificial Intelligence. The basic block diagram of the wireless sensor network has given below Fig1.

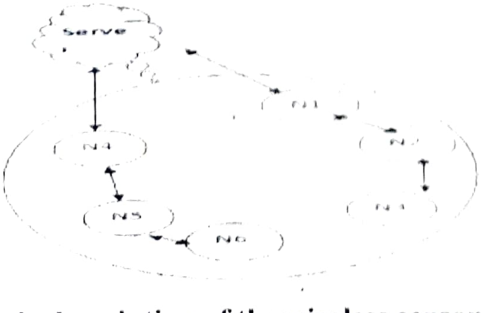


**Fig. 1: Basic description of the wireless sensor network.**

The wireless sensor network node exists with two major parts, and one is server next one is a sensor node. Again each sensor node consist of three different parts

1).Sensors.

2).RF-Modules.

3).Processing unit.

Sensors: The use of the sensors is to sense the data for the particular applications, the sensors are weak intelligent devices means simply they can detect the data, and they will give the data to the processing unit .whatever the data ranges maybe they can take any decision even the sensing data limits are below or over threshold values [3].

RF-Modules: RF modules are also poor, intelligent devices; they don't have self intelligence: they don't know what they are carrying and what they are receiving in the sensor network. They transmit the data which was given by the Processing unit and provide the data to the processing unit, which was received externally [3].

Processing Unit: Processing unit is the heart of the sensor node they are excellent, intelligent devices they can collect the data from the sensors and they can make the decisions based on the threshold values, and also they can send the information from one place to another place with the help of RF-Modules. Here the processing unit may be microcontroller or microprocessors. In the current era, many wearable devices and wireless sensor networks are using microcontrollers for the application execution because they are portable devices and limited to hardware and consumes less power [3]. The basic block diagram of the sensor node has given in Fig2.

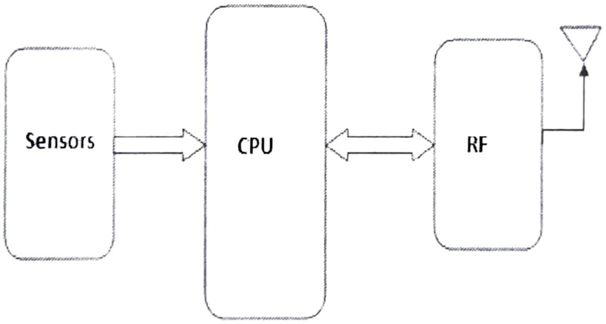


**Fig. 2: Basic Block diagram model of the sensor node.**

## 2. ARTIFICIAL INTELLIGENCE

Artificial Intelligence is a new approach in information technology, which is useful to solve problems like the human brain. It is an investigation to solve many issues and values to provide excellent solutions. The things which are not possible to settle by the human resources, such type of challenges easily, can be solved by the AI, Some of the examples for the AI is robotic applications, neural network applications, network security applications, etc. For example, let us take one of the applications is robotic applications. The robotic applications are vastly using in the different domains like health care applications, SCADA applications. In the case of health care applications, the robotic applications are using in the radiology to spoil the Cancer cells. The cancer cell size is around 19.9 microns.

Hence it is challenging to project the X-Rays at this point, to get such type point of projection that should be possible by the robotic applications which are trained by the AI. A second application is SCADA applications. The SCADA applications aim to monitor the data continuously. If anyone wants to watch the environment in the hazardous area, it is not possible to send any person to that location, in this critical situation the AI can quickly solve this problem by using robots which were trained by the AI. Due to its intelligence, the usage of these AI applications is becoming a part of human life and different types of areas. Hence the revenue was also increasing in this AI field, which was depicted in Fig3.

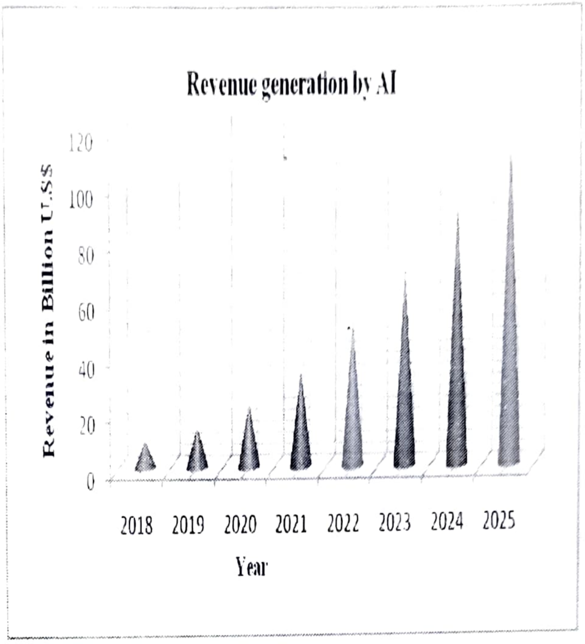


**Fig. 3: Expected Revenue generation by the AI software market [4].**

## 3. SECURITY ISSUES IN WSN

Because of the way that WSNs utilize remote methods for data exchange, security inside WSNs is significant and must be tended to. A malicious client can undoubtedly do assaults to capture the information. Many authors proposed different types of solutions to solve the issues in the WSNs, for example, handling and correspondence impediments, to the failure to execute safety efforts [5-7]. Essential security necessities in WSNs have been distinguished as information validation, information privacy, information trustworthiness, and accessibility, and excess [8-9]. To accomplish major security objectives, the dangers to WSNs should initially be distinguished. Assaults on WSNs are classified into objective orientated, entertainer orientated, and layer arranged assaults [10]. The Goal related network security attacks exist with passive, active attacks [6]. Passive attacks are made when malevolent client screens delicate system data without upsetting system activities, so it might be utilized in different attacks. These attacks bring about the revelation of delicate or information documents unbeknown to the system client.

Dynamic attacks are the point at which the assailant utilizes this data to expect command over the system or upset system activity. Instances of dynamic attacks incorporate DoS, wormhole, hi flood, Sybil, dark opening/sinkhole, information adjustment and mocking [9-12]. Entertainer orientated assaults comprise of outside and inside assaults. Outside assaults take into account observing information transmissions just as infusing false information into the system to devour assets bringing about DoS Attacks. Inside assaults are when pernicious hubs march as real hubs to harm the system. When trusted by the system, the pernicious hub would then be able to dispatch various attacks [6], the wellspring of which is hard to situate because of the way that the harmful hub can smother significant data from arriving at the base station. There may be many more hackers to hack our data by retrieving from the cloud or to collect the data by joining between the communication to spoil the organization's reputation or which spoils the organization's financial strategies. So it is always better to provide the security for that sensitive data to protect from the network security attacks. As per Revision Legal report, the confidential affected data of the peoples have given in Table.1 [13], and the Pie graph analysis is shown in Fig.4.

Table.1: Hacking Information [13].

| Year | Type of information | Info in millions |
|---|---|---|
| Jan:2018 | Patient information | 2.9 |
| Apr:2018 | A ride-sharing app | 14 |
| June:2018 | Customer Email-database | 92 |
| July:2018 | Bit-humb Cryptocurrency | 31.5 |

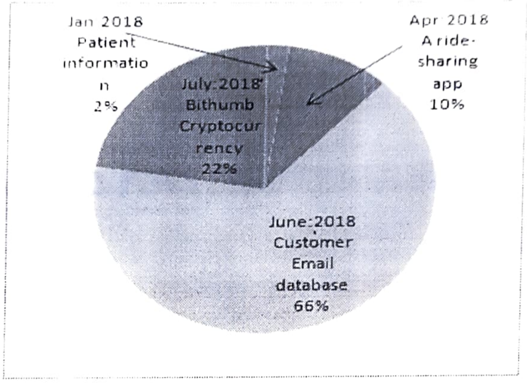


Fig. 4: Customers hacking information in 2018 [4].

## 4. SECURITY REQUIREMENTS

Whenever WSN is carrying sensitive data then it has to take care to protect the data from the intruders, The basic security models have given in the [14-15], and also these can also discuss the data integrity, confidentiality, etc. The secondary solutions are also given in the [16-18], which can talk node localization and the self-organization. The security solutions are described in the [19] when the data is transmitting over the network.

**Data Confidentiality**: The Applications of a wireless sensor network is to carry the data from one node to another node. Whenever nodes are transporting data from one end to another end, it is necessary to maintain the data confidentiality by the encryption technique; otherwise, it should be a chance for the data leakage in the network [20].

**Data Integrity**: Data integrity is one of the important in the WSN. The sender always sends the data, and the receiver receives these data, but the intruder can join in between the communication, and it can change the data as per its requirements[21-22].

**Data Authentication**: one of the best methods in the WSN to establish the data communication between the nodes is node authentication to overcome the data leakage.

**.Data Availability**: WSN always carries valuable data; hence, it is essential to establish excellent communication between nodes to reach the data to the customer at any time.

**Data Freshness**: Data Freshness is vital in the WSN; the node always must send the recently updated data only for the quality of services; hence, once the data was transmitted from the node, the node must flush the data for the updated data[19].

## 5. PREVIOUS WORK

This section discusses the previous work handled by the many scholars which protect the data confidentiality in the Wireless sensor network.

SAaaS was introduced by Doelitzscher et al. in [23]. They presented a cloud event recognition framework Security Audit as a Service. Their framework depends on smart, independent operators who know about hidden business streams of sent cloud examples, along these lines giving adaptability and bolstered cross-client occasion checking of a cloud foundation [23].

Shosha et al. in [21] proposed a disseminated IDS dependent on a joint network effort between different specialists for recognizing digital interruptions in Supervisory Control and Data Acquisition (SCADA) systems. The proposed engineering additionally consolidates the SCADA organize topology and network requirements.

Mabu et al. depicted a novel fluffy system interruption discovery technique dependent on class-affiliation rule mining in hereditary system programming. The proposed strategy is adaptable and capable of both abuse and irregularity recognition in systems, and it is equipped for managing the blended databases which contain both discrete and consistent credits to mine significant class-affiliation rules required for improved interruption location. The investigations and assessment of the proposed strategy exhibited that this methodology gives aggressively high recognition rates in examination with other AI procedures [25].

Ojugo et al. exhibited GAIDS – a Genetic Algorithm Rule-Based Intrusion Detection System for improving framework security, secrecy, honesty, and asset accessibility in arranged settings. The proposed framework utilizes a lot of arrangement rules acquired from organizing review information and the help certainty system, used as wellness capacity to assess the quality of each standard [26].

Hassan structured an IDS dependent on hereditary calculation and fluffy rationale for proficient identification of different meddling exercises inside a system. The framework is versatile and savvy as it can refresh manages once new nosy activities become known. The investigations and assessments result demonstrated that the proposed framework accomplished a sensible interruption location rate [27].

Jongsuebsuk et al. proposed a system IDS dependent on a fluffy hereditary calculation. Fuzzy principles are utilized to group organize assault information, while hereditary calculation upgrades finding suitable fluffy standard to acquire the ideal arrangement. The assessment results indicated that the proposed IDS could distinguish arrange assaults progressively (or inside 2-3 seconds) upon the appearance of information lands to the recognition framework with the discovery pace of over 97.5% [28].

Chaudhary et al. built up an irregularity based fluffy interruption identification framework to identify the bundle dropping assaults in portable, specially appointed systems. The reenactment results showed that the proposed framework could identify the parcel dropping assaults with high favorable and low bogus positive rates under all speed levels of versatile hubs [29].

Benicia et al. introduced a system interruption recognition model dependent on Genetic Algorithm approach with an improved beginning populace and choice administrator used to enhance the pursuit of assault situations in review documents and give the subset of potential assaults inside reasonable preparing time. They utilized a hereditary calculation approach since it supports the exhibition and diminishes the bogus positive rate [30].

Padmadas et al. displayed a layered hereditary calculation based interruption recognition framework for observing exercises in an offered domain to decide if they are real or pernicious dependent on the accessible data assets, framework uprightness, and classification. The exploratory outcomes indicated that the proposed framework effectively identify R2L assaults with 90% precision [31].

The analysis between coverage and connectivity for WSNs is examined in [32]. In this article, they classified these protocols into three categories one is Coverage sending methodologies, the second one is the mechanism by the sleep schedule, and the third one is auto-adjusted and radius protocols. They survey entirely focusing on the coverage protocols only.

The authors provide a survey about Barrier coverage for WSNs is given in [33]. The audited boundary inclusion conventions are, for the most part, characterized into two classifications: Barrier inclusion for static sensor hubs and hindrance inclusion for portable sensor hubs. The agreements are additionally ordered dependent on the accompanying criteria: the detecting range bearing, the detecting model, and the inclusion prerequisite. Also, a few advancement issues in obstruction inclusion are contemplated.

Another survey of boundary inclusion is given in [34]. Be that as it may, the focal point of this audit is hindrance inclusion for directional sensor hubs as it were. The inspected conventions are arranged, in light of the inclusion prerequisite, into four classifications: Strong boundary and powerless hindrance, 1-obstruction and k-obstruction, most exceedingly terrible and best-case inclusion, and introduction way inclusion, and any-see inclusion and full-see inclusion.

In [35], the inclusion issue is examined as a topology control method in WSNs. The considered inclusion conventions are ordered into three classifications separately: Area inclusion conventions, boundary inclusion conventions, and clear inclusion conventions. Region inclusion conventions are additionally grouped dependent on the sorts of sensors accessible in the WSNs and the inclusion necessity. Besides, boundary inclusion conventions are read for both deterministic and probabilistic detecting models.

The creator of [36] presents a short review of k-inclusion issues and conventions. The conventions were primarily arranged into two classifications: k-inclusion confirmation conventions and rest booking conventions for k-inclusion items.

Kumar and Goyal [37] have clarified they actualize hereditary calculations in dataset preparing to group the marks that are smurf assaulted and accomplishes low bogus definite proportion of 0.2%. Further work done by Abdullah [38] and colleagues explained interruption identification arrangement rules utilizing hereditary calculations. Interruption identification rules using genetic calculations was additionally the investigation made by Ojugo et al. [39]. This technique utilizes wellness work for evaluating the principles.

AI methods are likewise actualized to distinguish the interruption. Existing AI procedures for interruption location was portrayed by Roshani group [40].

Gaikwad et al. [41] presented a system dependent on fluffy bunching and ANN approach. This strategy could be appropriate to defeat the issues of feeble soundness location just as low exactness identification. The reestablish point in this strategy was utilized for vault keys, framework records move back, venture database, and introduced programs. Fluffy grouping will create various subsets for preparing to decrease the measure of subset size and multifaceted nature. At that point, every subgroup is ready with multiple kinds of artificial neural systems, lastly handled to get tremendous outcomes.

## 6. RESULT & DISCUSSION

The Importance of the wireless sensor network is widely increasing day by day in human life in different areas like healthcare applications, energy metering systems, industrial monitoring, etc. The sensor nodes are transmitting and receiving the data in the different mechanisms like clustering mechanism, polling mechanism, priority-based mechanism, scheduling based mechanism, etc. Whenever nodes are transmitting and receiving sensitive data, it is necessary to find out the neighbor node, either it is a trustable node or not, and if it is intruder, then the problem came into the picture. Hence it is necessary to authenticate the neighborhood with its adjacent nodes beforė join in between the communication. Here the proposed Manuscript is overcoming this problem by an authentication technique. In between the communication, any node wants to join, and it is necessary to authenticate with the neighborhood node in multilevel states; once the authentication was completed, then only it can get the permissions in the network.

### a. Algorithm:

Every node its self trained with multilevel authentication steps; any node wants to join in the network; the node can follow the 4-level authentication mechanism, which is well trained. If any intruder participates in the communication, it is difficult to pass with the 4-level authentication mechanism, because it is nọt prepared before installation in the communication. The artificial intelligence stages for the authentication have listed below.

**Password Generation Stage (PGS):** In this stage, each can generate itself n-bytes of Authentication String Randomly (ASR), which are ready to exchange; the generation of random number has given below.

By using the Whichman_Hill, the random string (ASR) was generated, which combines the three linear congruential generators. Now let us say the state space is

$$\{0,1,2,.....r_1-1\}X\{0,1,2,.....r_2-1\}X\{0,1,2,.....r_3-1\} \rightarrow (1).$$

And say is sate at the step of the nth stage.

Now the Random generator is

$$X_n = 171X_{n-1} \bmod r_1 \rightarrow (2).$$

$$Y_n = 171Y_{n-1} \bmod r_2 \rightarrow (3).$$

$$Z_n = 171Z_{n-1} \bmod r_3 \rightarrow (4).$$

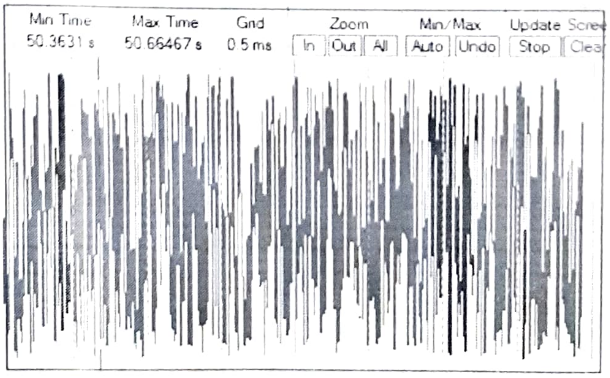
Where $r_1 = 30296, r_2 = 30307, r_3 = 30323$ Where $r_1 = r_2$

Now the output function is

From the equations (2),(3),(4), the final generated random number is which was given in the equation (5).

$$R_n = \frac{X_n}{r_1} + \frac{Y_n}{r_2} + \frac{Z_n}{r_3} \bmod 1 \rightarrow (5).$$

By using the above equation (5), n-bytes of random string was generated in each node. And where they are the authenticate random messages generated by the nodes.



Min Time 50.3631 s
Max Time 50.66467 s
Gnd 0.5 ms

Fig5: Typical random number generation.

The typical graphical representation of random number generation has given in Fig5.

**Password Exchange Stage (PES):** Once the password was generated, the nodes which are joined in the communication, they have to exchange the password both itself. For understanding convention, node-1 is represented as , and node-2 is represented as . For example, let us say are the and message which are generated in the PGS stage. The was sending to the node2 by the node1 and was send by the node2 to the node1, Which was given in the Fig6.

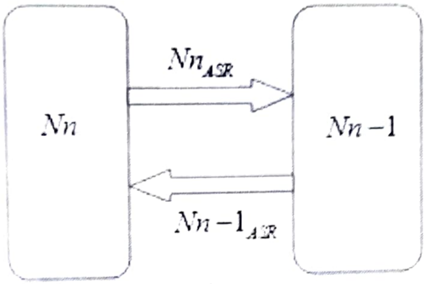


**Fig. 6**: Message exchange of nodes.

**Message Encryption Stage (MES):** In This stage, each node can encrypt the message using X-OR encryption with the predefined n-bytes of a key, which means the encrypts the message of which can be sent by the in the PES and encrypt the message of in the same stage. In this, each can encrypt the received message using XOR-operation with n-bytes of a predefined key, which was explained below.

For example, $Nn_{ASR}$ is the nth node message received by the $Nn-1_{ASR}$ node, and the n-bytes of encrypted key is .
Now the resultant encrypted message is $f(R_{encrypted}) = f(K \oplus Nn_{ASR}) \rightarrow (6)$.

Once the message was encrypted by the $Nn-1$ node, the $f(R_{encrypted})$ which was resultant encrypted message was sent back to the .

**Node Authentication Stage (NAS):** After the success of MES again, both nodes will exchange this encrypted message in this stage. Now the nodes will decrypt these $N_{1m}$, $N_{2m}$, with their n-bytes of a key.

Now
$R_{decrypted} = f(K \oplus R_{encrypted}) \rightarrow (7)$.

From the equation, it $R_{decrypted}$ is equal to $Nn_{ASR}$ means the $Nn-1$ node was authenticated successfully, which exchanged in the PGS mode means they are artificially trained nodes; now, they are ready to transfer the messages.

For example, if nodes are not well-known nodes, they don't know the trained encrypted and decrypted keys. Hence the encryption will go in the wrong direction with the unknown key in the MES stage. Once the message was encrypted with the incorrect key automatically, the NAS stage will fail with the improper authentication. Due to this authentication fail, the node will be recognized as the introducer because of the intruder not trained with the known keys.

## 7. CONCLUSION

The Manuscript is mainly concentrating on the security issues in the WSN, and providing the solution using Artificial Intelligence. Security is a big problem in data communication; whenever sensitive data is sending in receiving in the network, there is a much more change to hack these data by the introducers. Hence it is a necessity to take care of these hackers. The developed algorithm successfully applied for the wireless sensor network, and the MLA algorithm artificially trained to each node. When the communication was going the node which was trained by the MLA algorithm, it was successfully exchanged the message, and the node which was not by the MLA it was not got permission to join in the network. The complete algorithm was tested by the ARM-CORTEX, which can support the high-speed execution, which was vastly used in artificial intelligence applications.

## References

1. Abu-Mahfouż, A. M., Hamam, Y., Page, P. R., Djouani, K., & Kurien, A. (2016). Real-time dynamic hydraulic model for potable water loss reduction. Procedia Engineering, 154, 99-106.
2. Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015). Security in software-defined networks: A survey. IEEE Communications Surveys & Tutorials, 17(4), 2317-2346.
3. Rao, V. M., Ram, M. S. S., & Giriprasad, M. N. Power Saving Scheduling For Iot Based Garbage Monitoring System.
4. https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/.
5. J.Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.
6. K.Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in Proc. World Congr. Eng., vol. 1, 2015.
7. A.M. Abu-Mahfouz and G. P. Hancke, "Evaluating ALWadHA for providing secure localization for wireless sensor networks," in Proc. IEEE AFRICAN 2013 conf., Mauritius, Sep. 2013, pp. 501–505.
8. D.Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless sensor networks and the internet of things: Selected challenges," Struct. Heal. Monit., vol. 5970, pp. 31–33, 2009.
9. H.Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in 2011 Third Int. Conf. Comput. Intell. Model. Simul., 2011, pp. 308–311.
10. .A.S. K. Pathan, H. W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in 2006 8th Int. Conf. Adv. Comm. Tech., vol. 2, 2006, p. 1048.
11. H.I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," IEEE Access, vol. 5, pp. 1872–1899, Feb. 2017.
12. T.Zia and A. Zomaya, "Security issues in wireless sensor networks," in 2006 International Conference on Systems and Networks Communications (ICSNC06), 2006, p. 40.
13. https://revisionlegal.com/data-breach/2018-statistics/
14. Eirini Karapistoli, Anastasios A. Economides, "Wireless sensor network security visualization," 2012 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 850-856, 2012.
15. Virendra Pal Singh, Sweta Jain, and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks," International Journal of Computer Science Issues (IJCSI), Volume 7, Issue 3, No 11, pp. 23-27, May 2010.

16. Pankaj Pardesi and Jitender Grover, "Improved Multiple Sink Placement Strategy in Wireless Sensor Networks," 2015 IEEE International Conference on Futuristic Trends on Computational Analysis and Knowledge Management ,Amity University, Greater Noida, Uttar Pradesh, India, DOI: 10.1109/ABLAZE.2015.7155032, pp. 418-424, 25-27 Feb, 2015.
17. Jitender Grover, Shikha Sharma and Mohit Sharma, "Reliable SPIN in Wireless Sensor Network: A Review," IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-0661, Vol. 16, Issue 6(III), DOI: 10.9790/0661-16637983, pp. 79-83, Nov.-Dec. 2014.
18. G.Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms, and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security (IJCSIS), Volume 4, Issue 1 & 2, pp. 1-9, August 2009.
19. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah, and Kashif Naseer Qureshi, "Security Issues and Attacks in Wireless Sensor Network," World Applied Sciences Journal, Volume 30, Issue 10, pp. 1224-1227, November 2014.
20. Chinyang Henry Tseng, Shiau-Huey Wang, Woei-Jiunn Tsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection," IEEE Transactions on Reliability, Vol. 64, Issue: 3, pp. 1078 - 1085, 2015.
21. Sneha Ghormare, Vaishali Sahare, "Implementation of data confidentiality for providing high security in Wireless Sensor Network," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, pp. 1-5, 2015.
22. Singh, Ajay Vikram, and Moushumi Chattopadhyaya. "Mitigation of DoS attacks by using multiple encryptions in MANETs." In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on, pp. 1-6. IEEE, 2015.
23. F.Doelitzscher, C. Reich, M. Knahl, N. Clarke, (2011) "An Autonomous Agent-Based Incident Detection System for Cloud Environments," IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), pp.197-204.
24. A.F. Shosha, P. Gladyshev, W. Shinn-Shyan, L. Chen-Ching, (2011) "Detecting cyber intrusions in SCADA networks using multi-agent collaboration," 16th International Conference on Intelligent System Application to Power Systems (ISAP), pp.1-7.
25. S.Mabu, C. Chen, L. Nannan, K. Shimada, K. Hirasawa, (2011) "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.1, pp.130-139.
26. A.A.Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro (Mrs), F.O. Aghware, (2012) "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 8, pp. 1182 – 1194. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015
27. M.Md. M. Hassan, (2013) "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, No. 7.
28. P.Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, (2013) "Real-time intrusion detection with a fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp.1-6.
29. A.Chaudhary, V. N. Tiwari, A. Kumar, (2014) "Design an anomaly-based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," IEEE International Conference on Advanced Computing (IACC), pp. 256-261.

30. S.E. Benaicha, L. Saoudi, S. E. Bouhouita Guermeche, O. Lounis, (2014) "Intrusion detection system using genetic algorithm," Science and Information Conference (SAI), pp. 564-568.
31. M.Padmadas, N. Krishnan, J. Kanchana, M. Karthikeyan, (2013) "Layered approach for intrusion detection systems based genetic algorithm," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1-4.
32. C.Zhu, C. Zheng, L. Shu, and G. Han, "A survey on coverage and connectivity issues in wireless sensor networks," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 619 – 632, 2012, simulation and Testbeds. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804511002323
33. F.Wu, Y. Gui, Z. Wang, X. Gao, and G. Chen, "A survey on barrier coverage with sensors," Frontiers of Computer Science, vol. 10, no. 6, pp. 968–984, 2016. [Online]. Available: http://dx.doi.org/10.1007/s11704- 016-5532-4
34. D.Tao, and T. Y.Wu, "A survey on barrier coverage problem in directional sensor networks," IEEE Sensors Journal, vol. 15, no. 2, pp. 876–885, Feb 2015.
35. M.Li, Z. Li and A. V. Vasilakos, "A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues," Proceedings of the IEEE, vol. 101, no. 12, pp. 2538–2557, Dec 2013.
36. N.Yeasmin, "k-coverage problems and solutions in wireless sensor networks: A survey," International Journal of Computer Applications, vol. 100, no. 17, 2014.
37. Goyal,A.and Kumar, C.GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System, Electrical Engineering and Computer Science, Northwest University, Technical Report;2008.
38. Abdullah, B., Abd-algafar I., Salama G. I. and Abd-alhafez A. Performance Evaluation of a Genetic Algorithm Based Approach to Network Intrusion Detection System, Proceedings of 13th International Conference on Aerospace Sciences and Aviation Technology (ASAT-13), Military Technical College, Cairo, Egypt, 2009;1-5.
39. Ojugo,A. A., Eboka, A. O., Okanta, O. E., Yòra, R. E. and Aghware, F. O.Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS), Journal of Emerging Trends in Computing and Information Sciences, 3(8);2012; 1182 – 1194.
40. Roshani Gaidhane, Vaidya, C. and Raghuwanshi, M. Survey.Learning Techniques for Intrusion Detection System (IDS), International Journal of Advance Foundation, and Research in Computer (IJAFRC) Feb 2014. ISSN 2348 – 4853, 2014;1(2).
41. Gaikwad, Sonali Jagtap, D.P. Kunal Thakare, and Vaishali Budhawant. Anomaly Based Intrusion Detection System Using Artificial Neural Network and fuzzy clustering., International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, N.