IJRSET AUGUST 2021 Volume 8, Issue 8 Pages: 1-12

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

REVIEW ON CRYPTOGRAPHY TECHNIQUES IN WSN FOR ATTACK PREVENTION

[1] G. BANUPRIYA, [2] DR. P. LOGESWARI
[1] Research Scholar, [2] Assistant Professor,
[2] Department of Computer Science,
[1, 2] Sri Krishna Arts & Science College,
[1, 2] Coimbatore, Tamilnadu, India.

ABSTRACT - Scalability of routing protocols used in wireless sensor networks (WSNs) is a critical issue due to the extremely high node numbers and relatively high node density. The analysis of scalability of wireless sensor networks is a challenging performance issue. Complexity is caused by several issues. First, the large number of nodes heavily impacts simulation performance and scalability. Second, credible results demand an accurate characterization of the sensor radio channel. New aspects, inherent in WSN, must be included in simulators, e.g. a physical environment and an energy model, leading to different degrees of accuracy versus performance. A good routing protocol has to be scalable and adaptive to the changes in the network topology. Thus protocols must perform well as the network grows larger or as the workload increases. In this paper, we compare the algorithms in WSN to improve the scalability of the network. This computation showed the limitation and capability of the WSN scalability and specifically for Flooding. In this work, Supervised learning and Unsupervised learning algorithms like k-nn, Fuzzy Logic based has been compared successfully to analyze the efficiency of scalability in WSN.

Keyword: [Wireless Sensor Network, NS2, Fuzzy logic, Cluster Head, Routing, Machine Learning, Neuroscience, LEACH protocol.]

1. INTRODUCTION

Uses of remote sensor organizations (WSNs) have been developing at a quick rate over the recent many years. Since the subject has gotten consideration, the going with innovation additionally quickly upgraded, prompting the plan of little sensors that are equipped for detecting, preparing and imparting information. Sensor networks are normally conveyed at distant destinations. They are accused of the duty of detecting and moving information to the base station for handling and capacity. These tasks require continuous force source, which establishes a test given the areas of the sensors. One approach to take out this issue is to guarantee proficient force utilization. Notwithstanding the force utilization, there are a few different issues that require thought when the constraints of sensors are concerned. Given that the remote sensors are little gadgets with restricted abilities, they are restricted in preparing, force, memory, and correspondence. The sensors are normally

positioned on far off locales notwithstanding their force limits. Thusly, the WSN business centers around expanding the detecting capacity with the base force utilization. Extraordinary conventions are needed to make these sensors work with ideal force utilization. Furthermore, applying standard organization security strategies to WSNs isn't viewed as a feasible arrangement because of their restricted capacities. Besides, use of ordinary organization security methodology would likewise prompt expanded force utilization requiring extra preparing assets. A remote sensor network is a gathering of particular transducers with an interchanges framework for checking and recording conditions at assorted areas. Normally checked boundaries are temperature, moistness, pressure, wind course and speed, brightening force, vibration force, sound force, power-line voltage, substance fixations, toxin levels and crucial body capacities. Remote sensor organizations (WSNs) offer extraordinary guarantee for data catch and handling in both business and military applications. Effective framework plan and arrangement incorporates understanding RF channel attributes, and the decision of adjustment conspires on power utilization. Such factors eventually decide the accessible reach and information pace of a WSN, just as cost and battery lifetime. Remote sensor organizations (WSNs) have acquired overall consideration as of late, especially with the multiplication in Micro-Electro-Mechanical Systems (MEMS) innovation which has worked with the improvement of shrewd sensors. These sensors are little, with restricted preparing and processing assets, and they are economical contrasted with customary sensors. These sensor hubs can detect, measure, and accumulate data from the climate and, in light of some nearby choice cycle, they can send the detected information to the client.

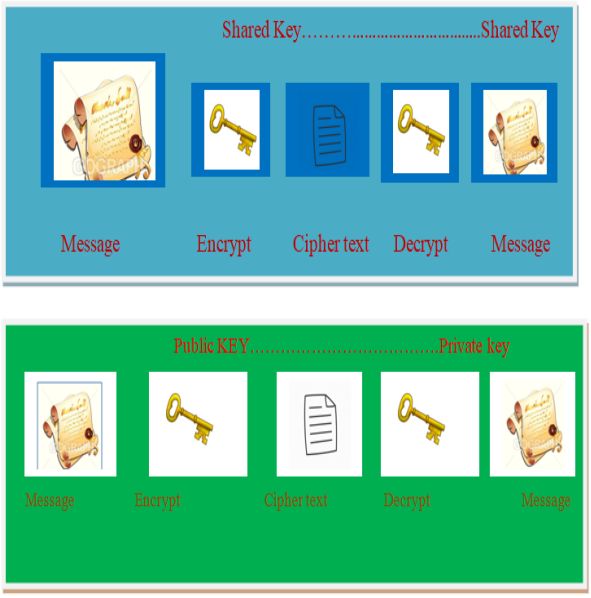

Figure1. Encryption and Decryption process

2. LITERATURE SURVEY

1. Cong Gao, Zhongmin Wang and Yanping Chen (2019), et.al proposed On the connectivity of highly dynamic wireless sensor networks in smart factory. With the advancement of brilliant assembling in Industry 4.0, huge measure of heterogeneous information is created from numerous sources. Different information handling procedures can be applied to these information to separate expected data about the situation with the assembling organization. In this manner, information is significant to the investigation and change of the assembling measures. Because of the variety of items, mechanical production systems and assembling measures are exceptionally powerful. Considering the adaptable sending of remote sensor organizations, they have been generally conveyed to lead information assortment. Notwithstanding, because of the restricted radio scope of a remote sensor hub, the availability of an exceptionally powerful remote sensor network is a central question. Broke down the availability in a remote sensor organization and agreed three sorts of network. At that point, we created two organization availability models from the

viewpoint of one measurement and two measurements. The levels of availability for both two hubs and the organization are expounded. At long last, the connection between the quantity of sink hubs and the normal level of availability of the organization is dissected dependent on exploratory outcomes.

2. Waltenegus Dargie (2020), et.al proposed A Clustering Strategy for Wireless Sensor Networks. The bat algorithm (BA) is a novel metaheuristic search algorithm which simulates the behavior of the bat species for searching prey. Preliminary studies show that it is very promising and could outperform existing algorithms. The BA utilizes a population of bats to represent candidate solutions in a search space and optimizes the problem by iteration to move these agents to the best solutions about a given measure of quality. Cluster Head Selection algorithm is used to put together hubs into productive groups in remote sensor networks works with information accumulation and order dispersal. In any case, grouping is a perplexing and expensive interaction, since it must be done in a dispersed and occasional way. In this paper we propose a basic grouping system utilizing a nearness lattice which encodes hubs' area and availability in an organization. Our methodology empowers the task of bunch sets out toward numerous rounds in a solitary advance consequently restricting the expense of group head political decision and kid hub affiliation.

3. Ahmed Nader al-Dulaimy, and Hannes Frey (2019), et.al proposed Subnet Addressing in Software Defined Wireless Sensor Networks. Software defined networking provides manageability and scalability to networks by decoupling network control and forwarding functions into separate layers. Though the concept is typically a subject for wired networks, recent research activities have also considered software defined networking in the context of wireless networking and especially in wireless sensor networking. Software defined networking in that context is, however, a very challenging task due to limited resources of the sensors. In particular, the number of entries in the flow table and the control message overhead is a limiting factor. This paper introduces a new approach to efficiently manage a software defined wireless sensor networks by means of a hierarchical addressing scheme. It is based on a tree of address masks which are used to split the network into subnets. Each subnet has a range of host addresses and a subnet head which acts as a gateway to its children. With that hierarchical structure, nodes need only to recognize the subnet where a packet is destined to and forward that packet to the subnet head. We evaluated the proposed approach using the Cooja simulation environment of Contiki. Compared to the state of the art our scheme reduces the amount of control messages, the size of path packets, the number of rules needed to be stored in the flow table and hence the processing time for these rules.

4. Babatunde S. Awoyemi, S. Alfa, and Bodhaswar T. Maharaj (2019), et.al proposed Network Restoration in Wireless Sensor Networks for Next-Generation Applications. Profoundly proficient organization reclamation models for remote sensor organizations (WSNs) to be conveyed for future (xG) applications. The created network rebuilding models are planned in view of two principle objectives. The principal objective is to enhance network asset use, and the second is to ensure the organization against disappointments. In understanding the objective of advancing asset utilization, a particular component of WSNs is misused, specifically, their capacity to stay in dynamic assistance in any event, when at least one of their dynamic components (sensor hubs and additionally associating joins) come up short. To accomplish the second objective of organization insurance, we influence the benefit of p-cycle-based rebuilding arrangements - the way that they can furnish ring-like recuperation speeds with network like limit efficiencies - in creating ideal p-

cycle reclamation models that give adequate security to the organization against both connection and hub disappointments. In the reclamation models created, we utilize a choice interaction that together thinks about the briefest lengths, best geographies, and limit necessities of the accessible p-cycles in accomplishing new limit ideal p-cycle-based rebuilding answers for the organization. Near outcomes acquired show that our created choice based limit effective p-cycle rebuilding answers for WSNs beat other comparable methodologies for both organization acknowledgment and assurance, making them especially ideal for xG applications.

5. Nazli Siasi, Adel Aldalbahi, Mohammed A. Jasim (2019), et.al proposed Reliable Transmission Scheme against Security Attacks in Wireless Sensor Networks. Routing protocols in wireless sensor network are vulnerable to various malicious security attacks that can degrade network performance and lifetime. This becomes more important in cluster routing protocols that is composed of multiple node and cluster head, such as low energy adaptive clustering hierarchy (LEACH) protocol. Namely, if an attack succeeds in failing the cluster head, then the entire set of nodes fail. Therefore, it is necessary to develop robust recovery schemes to overcome security attacks and recover packets at short times. Hence this paper proposes a detection and recovery scheme for selective forwarding attacks in wireless sensor networks using LEACH protocol. In general, wireless sensor nodes transmit and receive packets to a centralized base station via a wireless channel. The nodes here often operate with multiple limitations and constraints, in particular limited battery lifetime and hence requirement for low power consumption levels, i.e., resource-constraint nodes. In addition, the wireless channel is also vulnerable to various malicious attacks in the environment, such as selective forwarding and Sinkhole attacks. Hence sensor nodes can suffer from packet loss and also yield network failure when such attacks are present, i.e., yields nodes to selectively drop packets, which also reduces transmission reliability and security. Also, the multicast transmission nature in wireless sensor networks (WSN) further increases susceptibility to security attacks.

6. Runfa Zhou and Roger S. Cheng (2019) proposed Optimal charge planning for energy-compelled wireless-powered network. As an applicant power supply answer for the Internet of Things, radio frequency (RF) energy gathering has pulled in extraordinary consideration as of late. In this paper, they consider an RF wireless-powered network, which comprises of a committed power beacon (PB) and numerous client hubs. The PB is accepted to have constrained energy and moves its power to client hubs wirelessly. The client hubs work just dependent on energy reaped from the PB, and are thought to be in either energy collecting mode, energy utilization mode, or inactive mode. To amplify all out collected energy, they organize the practices of the PB and client hub. They consider a static wireless-powered network whichcomprises of a devoted power beacon (PB) and different wireless powered client hubs. For this energy-compelled wireless powered network, they proposed an ideal charge planning to expand the all-out gathered energy of all client hubs.

7. Craig B. Schindler, Daniel S. Drew, Brian G. Kilberg, Felipe M. R. Campos, Soichiro Yanase, Kristofer S. J. Pister (2019) proposed a bit equipped for 9-hub inertial measurement and low power wireless work networking with the littlest structure factor conceivable; the Micro Inertial Measurement System (MIMSY). Our exhibited stage is planned as a broadly useful wireless sensor bit with a structure factor and value point that makes it manageable to huge scale arrangements over an assortment of segments. The system is completely perfect with the Open WSN wireless sensor networking stack, which empowers the direct usage of principles consistent with 6TiSCH work networks utilizing MIMSY bits. While

the application space of MIMSY is very huge, they present three example usage displaying the open doors managed by a little and moderately ease bit with work networking and inertial measurement abilities. Bits consequently joined the wireless work network once turned on, wiping out the requirement for manual blending and availability support.

8. Basma Mostafa (2019) proposed Binary Integer Programming problem definition. One of the fundamental difficulties for network checking is figuring out where to install (place) the observing hubs. These components ought to have the likelihood for effectively/inactively running observing tests or potentially breaking down the checking results. The tests' arrangement must be upgraded so as to limit the energy cost and observing burden. Additionally, the observing computational cost, battery and memory necessities ought to be insignificant so as to fulfill the ease and energy requirements of IoT devices. Network checking models show that the related advancement is often NP-hard. The authors start by building up a model that focuses on the ideal position of screens while guaranteeing network coverage and computational tractability. The proposed models should work couple with RPL, the graph they use is the Destination Oriented Directed Acyclic Graph (DODAG) built by RPL. The ideal screen position is discovering the base number of observing hubs set on the graph to monitor every one of the connections in the network. The problem can be demonstrated as the great Vertex Cover Problem (VCP). VCP is NP-hard for general graphs. Then again, it is polynomial when comprehended on trees and Fixed-Parameter Tractable (FPT) when illuminated on "tree-like" graphs, likewise called pleasant tree disintegrations, and the jumping parameter here is the treewidth. Considering this information, they proposed calculations, that convert the DODAG speaking to the network topology into decent tree disintegration with solidarity treewidth.

9. Lina Xu and Nuno Pombo (2019) proposed a way to deal with use the sensor organization design and the high privacy saw detecting data to anticipate human conduct. As the supporting advancements for Ambient Assistant Living (AAL) in the Internet of Things (IoT) space have become all the more powerful and increasingly appealing, the related systems will be broadly conveyed and placed without hesitation. With all related implanted IoT detecting devices, how to keep up clients' privacy and data security is an exceptionally concerned issue. There are commonly two ways to deal with secure privacy. One is to actualize complex security protocols to ensure the safety of detecting, storage and data transmission. Another is to forestall the privacy issues and worries from the source. This proposed research will give an idea of a structure that can bolster conduct checking through noninvasive and privacy-protecting detecting. The data gathered, transmitted and utilized for breaking down in this system is detecting information with low extravagance. This structure expects to expand the clients'

10. Paul R. Berger, Miao Li, Ryan M. Mattei, Maimouna A. Niang, Noah Talisa, Michael Tripepi, Brandon Harris, Sagar R. Bhalerao, Enam A. Chowdhury, Charles H. Winter and Donald Lupo (2019) proposed progressions in arrangement process able devices utilizing metal oxides for printed internet-of-things objects. Putting a room light or an indoor regulator on the internet for remote control is viewed as dynamic. In any case, whenever printed gadgets can accomplish execution expands, at that point, IoT articles could be affixed to nearly anything, for example, coffee half and half containers, grain boxes, or that missing sock. Every one of these IoT articles could be driving a sensor, maybe position, temperature or weight, basically a huge number of applications. All together for IoT items to imitate a straightforward postage stamp, with self-powering from energy rummaging and

neighborhood energy storage, all housed in a non-harmful adaptable structure factor.

11. Roshmi Sarmah, Manasjyoti Bhuyan and Monowar H. Bhuyan (2019) proposed SURE-H: A Secure IoT Enabled Smart Home System. The proposed system that empowers to shield homes from robbery or bizarre exercises and parallelly spares power. Our system is created by abusing the highlights of IoT that encourages us to screen an IoT empowered home from anyplace anytime over the Internet when data are put away in the cloud. This system utilizes a movement locator to distinguish a moving article from the environment where the system is sent. The proposed system is assessed utilizing continuous arrangement at KU grounds thinking about 30 spaces for 60 days. It utilizes an Android application that gives exchanging functionalities, where the electrical or electronic devices are observed and controlled remotely. This system includes advantage by taking out the utilization of conventional personal computers (PC) and it is fringe devices during execution. The SURE-H system works dependent on the put-away cloud server data. They store the subtleties of home apparatuses for each room into the server. At first, it sends a solicitation to the server and hangs tight for the endorsement. When it watches any moving object it sends an alert with a detail report against the occurrence. This alert will trigger just when the new article watches.

12. Jernej Hribar, and Luiz DaSilva (2019) proposed a refreshing system fit for gaining from the substance of information gathered to diminish the frequency with which devices transmit their updates, hence improving their energy efficiency. Billions of low-power devices gathering information will be sent in the Internet of Things (IoT) networks. By exploiting the connection displayed in information gathered, it is conceivable to improve sensors' energy efficiency. The proposed instrument gains from the substance of information gathered to improve the energy efficiency of low-power devices, subsequently making IoT organizations increasingly feasible, both financially and environmentally. In our work, the timeliness of information, i.e., the time slipped by since the last transmitted update, has a critical job in the basic leadership process. Evaluate the timeliness of information utilizing the idea of the Age of Information (AoI). Also, they show that depending on information from one connected device can expand the exactness of gathered information on another device.

13. John Fox, Dr. Andrew Donnellan and Liam Doumen (2019), et.al proposed the planned engineering and strategy of a completely working LoRaWan based IoT system. Such a system can be given as a support of a given nearby area, by using an End Device related to a LoRa handset, a LoRaWan Gateway, and a characterized cloud stage. From a system point of view, a total IoT arrangement can be isolated into three classifications, the data gatherer, the communication strategy and the cloud stage administration. The data authority identifies with the inserted system device (or the 'things' component) at the wellspring of the application, the communication strategy identifies with the network protocol used to send or get the data and the cloud stage administration identifies with the office used to store and process the data gathered. LoRaWan and LoRa are 'Long Range' advances, which characterize the communication strategy for such IoT applied systems. LoRa characterizes the tweak technique, that takes into consideration long-range communication, while LoRaWan characterizes the communication and system engineering. The displayed IoT system currently serves the locale of Tallaght (Dublin, Ireland) and its more extensive region.

14. Mustafa A. Al Sibahee, Songfeng LU (2017), et.al proposed The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN. Wireless Sensor Networks (WSNs), applications are growing rapidly, so the needs to protect such applications are increased.

Cryptography plays a main role in information system security where encryption algorithm is the essential component of the security. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This phase provides evaluation of four of the most common encryption algorithms namely: RC4, DES, and AES as a symmetric cipher and RSA for asymmetric cipher. A comparison has been conducted for those encryption algorithms at different settings such as different sizes of data blocks, different key size and finally encryption/decryption speed. Simulation results are given to demonstrate the effectiveness of each algorithm on power consuming. Wireless sensor networks (WSN) are used to monitor environmental and physical changes by means of sensor nodes. Which is becoming a popular ubiquitous computing. They are used in different applications such as health care monitoring, environmental/earth sensing, air pollution monitoring, forest fire detection, industrial monitoring and many more. Since there are only limited resources, WSNs are exposed to many vulnerable attacks such as false message injection, eavesdropping etc., hence more security measures are needed. In recent times many techniques such as random key pre-distribution and random pairwise key distribution has been used. The security in WSN has been enhanced by using a symmetric key encryption technique. The pros and cons of the issues related to WSN have been put forth discussed, compared and evaluated in this research. Cryptographic is a set of algorithms operate in a way to encrypt and decrypt data. Encryption is transform plaintext to cipher text to serve security purposes.

15. Yildirim, G., & Tatar, Y. (2018), et.al proposed Simplified Agent-Based Resource Sharing Approach for WSN-WSN Interaction in IoT/CPS Projects. This phase focuses on the problem of interoperability and resource sharing in wireless sensor networks (WSNs) running under the Internet of Things (IoT) and cyber-physical systems (CPSs). Considering the scale of IoT/CPS projects, conventional WSN virtualization techniques remain incapable because of the hardware/software constraints and heterogeneity. To this end, in this paper, an agent-based server system approach, which improves the resource sharing between heterogeneous WSNs in IoT/ CPS providers, is proposed. In line with this approach, a software agent framework is introduced. With the help of the framework, called Firat Virtual WSN framework (FVWSN), the clients can move the commands/ queries and data fusion/ aggregation algorithms, which use on their local networks, to the provider side and run them remotely or automatically. This process is carried out by logical agent entities, called virtual nodes, which are created with the help of FVWSN. In this way, since the client evaluation mechanism is performed at a closer point to the shared resources, a shorter response time can be achieved in time-critical applications. The most important features that differentiate the developed agent framework from other agent-based technologies are that it is semi-autonomous and uses a specific resource selection/allocation algorithm. With the improvement that FVWSN provides for IoT/CPS WSN providers, it is possible to achieve a shorter response time and allow more client applications to share the same limited WSN resources. In this paper, first, the analysis and the necessity of the proposed system are discussed. Then, the system is simulated in the OPNET Modeler platform to make comparisons with well-known conventional WSN resource sharing mechanisms. Finally, the physical comparison tests of the system are carried out on an OpenStack-based cloud system, and the success of the system is shown.

3. PROPOSED METHODS, MERITS AND DEMERITS

Author Name& year	Proposed Method	Merits	Demerits
Cong Gao, Zhongmin Wang and Yanping Chen (2019),	On the connectivity of highly dynamic wireless sensor networks in smart factory	1. Straightforward and reduced network model.	1. Connectivity scheme for routing cannot be done.
Waltenegus Dargie (2020)	A Clustering Strategy for Wireless Sensor Networks	1. Simple clustering Algorithm has been used.	1.Low scalability
Ahmed Nader al-Dulaimy, and Hannes Frey (2019)	Subnet Addressing in Software Defined Wireless Sensor Networks	1. Compact ability of the system	1. Scalability is less.
Babatunde S. Awoyemi, S. Alfa, and Bodhaswar T. Maharaj(2019)	Network Restoration in Wireless Sensor Networks for Next-Generation Applications	1.The exceptional component of WSNs, which is its capacity to stay in dynamic assistance regardless of whether at least one of its components have fizzled.	1. Span a wide territory, implying that there are numerous sensor hubs that could fill in as a passage to the organization for a vindictive aggressor.
Nazli Siasi, Adel Aldalbahi, Mohammed A. Jasim(2019)	Reliable Transmission Scheme against Security Attacks in Wireless Sensor Networks	1. Vulnerability to attacks is less	1. Cost for the set up is high.
6.Runfa Zhou and Roger S. Cheng (2019)	Optimal charge planning for energy-compelled wireless-powered network	1. Optimal charge planning that can accomplish the system greatest energy gathering efficiency. 2. The complete collected energy is high.	1. It has a bigger bit of inertial measurement and low power wireless work networking.
Craig B. Schindler, Daniel S. Drew, Brian G. Kilberg, Felipe M. R. Campos, Soichiro Yanase, Kristofer S. J. Pister (2019)	A bit equipped for 9-hub inertial measurement and low power wireless work networking with the littlest structure factor conceivable; the Micro Inertial Measurement	High unwavering quality, low inertness communication for modern procedure computerization and control; Long lifetime physical occasion location and movement observing with negligible	1. It has a bigger bit of inertial measurement and low power wireless work networking.

	System (MIMSY)	arrangement time.	
Basma Mostafa (2019)	Binary Integer Programming problem definition	The BIP detailing was compelling in limiting energy utilization. The streamlining guaranteed full network coverage and negligible energy utilization. 3.The lingering battery never fell beneath 74% in all occasions	It very well may be time expending for huge measured or thick networks.
Jernej Hribar, and Luiz DaSilva (2019)	A refreshing system fit for gaining from the substance of information gathered to diminish the frequency	The proposed strategy improving energy efficiency by decreasing the frequency with which the detecting devices transmit their updates. The proposed component exploits connection, removed from information gathered, to improve the energy efficiency without bringing down the exactness of accessible information.	1. The refreshing component should adjust to consistently changing energy levels on devices.
Lina Xu and Nuno Pombo (2019)	A way to deal with use the sensor organization design and the high privacy saw detecting data to anticipate human conduct	It will stay away from data over-assortment and over introduction issues. Sensing data with uninformed wealth to ensure high apparent privacy.	1. Constrained information can be unique from the data.
Paul R. Berger, Miao Li, Ryan M. Mattei, Maimouna A. Niang, Noah Talisa, Michael Tripepi, Brandon Harris, Sagar R. Bhalerao, Enam A. Chowdhury, Charles H. Winter and	Progressions in arrangement process able devices utilizing metal oxides for printed internet-of-things objects	It watches varieties in the optical dielectric capacities and basic properties of the lighted oxide tests. Metal-oxide-based dynamic devices that are incorporated by arrangement handling and low-temperature	1.All housed in a non-harmful adaptable structure factor progresses in arrangement process able devices need to happen.

Donald Lupo (2019)		preparing to understand the up-and-comer discrete devices that will go into a total printed IoT system.	
Roshmi Sarmah, Manasjyoti Bhuyan and Monowar H. Bhuyan (2019)	SURE-H: A Secure IoT Enabled Smart Home System.	IoT-empowered smart home system that expands safeness from robbery and parallelly spares gigantic power cost. Automated switches for every home machine It can be proficient to recognize moving object and produce a secret phrase by joining a client secret phrases and fingerprints. It has ease, least time, exceptionally adaptable, oppose against man-in-the-center and online word reference assaults, and needs least infrastructures.	1.SURE-H can't support the huge scale environment, for example, offices and organizations.
John Fox, Dr. Andrew Donnellan and Liam Doumen (2019),	The planned engineering and strategy of a completely working LoRaWan based IoT system	As assistance, the system has been demonstrated to be fit for supporting a wide scope of IoT based applications. The same execution can be applied to different application necessities of the district.	1. Constraints of the End Device, for example, battery life span.
Mustafa A. Al Sibahee, Songfeng LU(2017)	The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in	1. It is scalable and hence can accommodate any new nodes or devices at any time.	1. It is expensive to build such network and hence can not be affordable by all.

	WSN		
Yildirim, G., & Tatar, Y. (2018)	Simplified Agent-Based Resource Sharing Approach for WSN-WSN Interaction in IoT/CPS Projects	1. Protection against data from theft and Protects the computer from being hacked.	1. The way it distracts can deviate our thoughts and activities towards unproductive activities.

CONCLUSION

In this work, various machine learning techniques which detect outliers WSN have been described. In WSN frameworks, sensors form the crux of generating raw data and are also responsible for detecting environmental changes. Thus, detecting outliers is much needed to analyze error free data generated from sensors. Some works have also been tabulated which are useful in detecting various kinds of outliers in sensor data. It can be easily concluded from the discussion that classification methods are the most extensively used learning methods for detecting outliers in WSN. The existing shortcomings in both WSN require developing more suitable outlier detection techniques for both univariate and multivariate data. Also, while developing new machine learning methods mobility of node and network topology change should also be seriously considered. To make asmall scale usage the examination has been actualized in NS2 using the for the most part accessible conventions.

REFERENCES

[1]. C. Gao, Z. Wang and Y. Chen, "On the Connectivity of Highly Dynamic Wireless Sensor Networks in Smart Factory," 2019 International Conference on Networking and Network Applications (NaNA), 2019, pp. 208-212, doi: 10.1109/NaNA.2019.00045.

[2]. W. Dargie and J. Wen, "A Simple Clustering Strategy for Wireless Sensor Networks," in IEEE Sensors Letters, vol. 4, no. 6, pp. 1-4, June 2020, Art no. 7500804, doi: 10.1109/LSENS.2020.2991221.

[3]. A. N. al-Dulaimy and H. Frey, "Subnet Addressing in Software Defined Wireless Sensor Networks," 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), 2019, pp. 32-38, doi: 10.23919/WMNC.2019.8881822.

[4]. B. S. Awoyemi, A. S. Alfa and B. T. Maharaj, "Network Restoration in Wireless Sensor Networks for Next-Generation Applications," in IEEE Sensors Journal, vol. 19, no. 18, pp. 8352-8363, 15 Sept.15, 2019, doi: 10.1109/JSEN.2019.2917998.

[5]. N. Siasi, A. Aldalbahi and M. A. Jasim, "Reliable Transmission Scheme Against Security Attacks in Wireless Sensor Networks," 2019 International Symposium on Networks, Computers and Communications (ISNCC), 2019, pp. 1-6, doi: 10.1109/ISNCC.2019.8909123.

[6]. C. B. Schindler, D. S. Drew, B. G. Kilberg, F. M. R. Campos, S. Yanase and K. S. J. Pister, "MIMSY: The Micro Inertial Measurement System for the Internet of Things," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 329-334, doi: 10.1109/WF-IoT.2019.8767232.

[7]. J. A. Cannataci, "Squaring the Circle of Smart Surveillance and Privacy," 2010 Fourth International Conference on Digital Society, 2010, pp. 323-328, doi: 10.1109/ICDS.2010.55.

[8]. H. Shastri and E. Frachtenberg, "Locality Bounds for Nonredundant Binary-Integer Representations," 2020 IEEE Symposium Series on Computational Intelligence (SSCI), 2020, pp. 2423-2430, doi: 10.1109/SSCI47803.2020.9308438.

[9]. R. Sarmah, M. Bhuyan and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019,

pp. 59-63, doi: 10.1109/WF-IoT.2019.8767229.
[10]. H. Jia, "Research on WSN Communication Data Fusion and Transmission Optimization Based on BPNN and ACO," 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE), 2019, pp. 1926-1929, doi: 10.1109/EITCE47263.2019.9095109.
[11]. H. Jia, "Research on WSN Communication Data Fusion and Transmission Optimization Based on BPNN and ACO," 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE), 2019, pp. 1926-1929, doi: 10.1109/EITCE47263.2019.9095109.
[12]. M. A. Al Sibahee, S. Lu, Z. A. Hussien, M. A. Hussain, K. A. Mutlaq and Z. A. Abduljabbar, "The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN," 2017 International Conference on Computing Intelligence and Information System (CIIS), 2017, pp. 308-312, doi: 10.1109/CIIS.2017.50.
[13]. V. Mathane and P. V. Lakshmi, "Deterministic Real Time Kernel for Dependable WSN," 2018 4th International Conference for Convergence in Technology (I2CT), 2018, pp. 1-4, doi: 10.1109/I2CT42659.2018.9057825.
[14]. M. Sharawi and E. Emary, "Impact of grey wolf optimization on WSN cluster formation and lifetime expansion," 2017 Ninth International Conference on Advanced Computational Intelligence (ICACI), 2017, pp. 157-162, doi: 10.1109/ICACI.2017.7974501.
[15]. V. Mathane and P. V. Lakshmi, "Deterministic Real Time Kernel for Dependable WSN," 2018 4th International Conference for Convergence in Technology (I2CT), 2018, pp. 1-4, doi: 10.1109/I2CT42659.2018.9057825.