March-April 2020
ISSN: 0193-4120 Page No. 1582 - 1586

An Analysis of Security Issues and Nature-Inspired Algorithms on Wireless Sensor Networks Integrated with IOT Environment

M. S. Vinmathi[1], Dr. M. S. Josephine[2], Dr. V. Jeyabalaraja[3]

[1]Research Scholar, [2]Addl. HOD & Prof, [3]Professor
[1&2]Dr. M.G.R. Educational and Research Institute
[3]Vellamal Engineering College
[1]vinmathis@gmail.com,[2]josejbr@yahoo.com

Article Info
Volume 83
Page Number: 1582 - 1586
Publication Issue:
March - April 2020

Abstract

WSN has the ability of detecting impelling the natural information the real time and positive data can be gathered utilizing sensor frameworks. These WSNs can be joined with internet of things to enable affiliation and broad access to sensor information. Wireless sensor networks are very inclined to security issues. The significant utilizations of sensor systems affect some of the areas such as in military, business, social insurance, retail, and transportations. These frameworks utilize wired or Adhoc systems. Wireless sensor systems, actuator systems, and vehicular systems have been considered incredibly in the industry level. Perhaps, the Internet of Things (IOT) has extensive research consideration recent years. The cutting edge innovation and the expanding figuring intensity of processors, the utilization of remote sensor systems have turned out to be to a great extent dispersed over wide regions. As of late the remote sensor systems is utilized in Agriculture, keen structures, ecological wellbeing and numerous different applications. In this paper ,an audit about joining of WSN with IOT, challenges looked by WSNs when coordinating with IOT have been discussed in a review manner and also showcased how they can be clarified from the parts of security and protection. In addition to the challenges, characteristics of nature-inspired algorithms are also analyzed for clustering the nodes in wireless sensor networks.

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 15 March 2020*

Keywords: *Challenges, Internet of Things, Nature-Inspired Algorithms, Wireless Sensor Networks, Security issues.*

1. Introduction

In recent technological development, with the high utilization of IoT numerous electronic gadgets are associated with web, this gadgets prompts numerous data security threats. The four layers of IOT Application layer, Perception layer, Network layer and Physical layer assumes a most significant job in making IOT progressively secure and dependable. So we have to ensure that these four essential layers are verified. Figure 1 demonstrates the overview of security issues in different Layers intended for IOT.

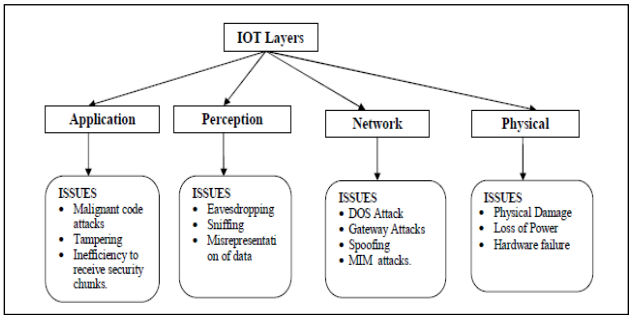

Figure 1: IOT Layers

March-April 2020
ISSN: 0193-4120 Page No. 1582 - 1586

2. Challenges

This section discusses various challenges faced in IoT environment. The first one is data security and privacy. Some of the developers have a keen focus on data transmission security during the development of the gadgets. The second is lack of standards and insurance deployment. Finally, security attacks and system vulnerabilities are focused. Here, the network, application and system security vulnerabilities are analyzed for finding out the issues.

3. Literature Survey

A portion of the safety efforts have been proposed by different researchers, here are a couple of recorded proposed safety efforts on account of the high utilization of IoT in numerous electronic are associated with web, this gadgets prompts numerous data security threats. Since web assumes a significant job here the fundamental spotlight is on system layer.

Abdulatif Alabdulatif et al. 2019 discussed on the security aspects to provide an efficient framework for healthcare surveillance through IoT. The framework have been designed completely in homomorphic encryption jam information security and prepared inside an EoT system. A dispersed methodology for grouping based procedures is produced for the proposed EoT structure with the versatility to total and investigate the huge scale and heterogeneous information in the disseminated EoT gadgets freely before it is sent to the cloud.

Youyang Qu et al. 2018 reviewed on the emerging challenges in wireless IoT. The authors also discussed on the various privacy policies and its oriented attacks in Wireless based IoT. The reviews are focused based on the trade-off optimization between privacy and the information utility over the WSN.

Partha Pratim Ray et al. 2018 focused on the reviews of existing ways to deal with experience the pertinent issues with calamities, for example, early cautioning, warning, information investigation, knowledge collection, remote observing, real-time analytics, and injured individual restriction. Concurrent mediations with IoT are likewise given most extreme significance while showing these facts.

A.Sardana and S. Horrow 2012 proposed personality the board Framework, it delivers issues identified with confirmation of information between the cloud and gadget utilizing character trough and administration chief, where the personality administrator verifies the information and sends data to support director to approve the guidelines of the administration to be performed.

Zhao, Walker and Wang 2012 proposed smart transportation framework security strategies, it tends to issues with respect to chance examination where an open key framework is utilized in that endorsement specialist is utilized for checking and overseeing security approval for the system hubs on ITS to gadgets to maintain a strategic distance from information from being ceased.

Lui, Xiao, Chen 2011 proposed confirmation and access control, it addresses on fixing escape clauses in gadget security and information honesty, where the client demands verification to get to a gadget and asks consent from an enrollment specialist (RA), RA thusly send client an inquiry, if reaction is OK, the client is confirmed to get to the device.

Li You-guo, Jiang and Ming-fu 2012 proposed security middleware, it delivers on giving security to shrewd home frameworks and specialized gadgets, where it utilizes element recognizable proof, security stockpiling, security review, information encryption what's more, unscrambling, computerized mark to verify correspondence between gadgets.

Survey on various Security Issues

Layer/Network	Issues	Technology	Solution	Limitation
WSN	Limitation of power,computing ability, Attacks in routing Protocol	Secure Routing Protocols such as AODV,DSDV,DSR	IDS	Network partition may occur due to infringement of packet loss
Network Layer	DoS/DDoS attacks	Encryption and access control technologies	Anti-collision algorithm	Increased complexityand cost due to additional control area implementation.
Adaptation Layer	DDoS attack	Management enhancing technology	Data disclosure and secure protection, control and recovery	Non-Distributed
Application Layer	Man-in-the – middle attacks, DDoS, Eavesdroping	IDS	Anticipated relay technology	High overhead during processing of data

Figure 2: Security issues

Figure 2 shows the security issues in WSN that are constrained of intensity, load and capacity limit. Since WSN is gathering of nodes henceforth there probability of attack towards directing protocols. The predominant solution for these issues is secure routing convention. There are some security issues in Adaptation layer. One of the issues is DoS attack; the answer for this is data disclosure, control and recuperation. The DoS attack is one of the issues in application layer and one of the solutions implemented for this is Guard Dog.

4. Nature-Inspired Algorithms

Nature-inspired algorithms in WSN can be classified namely Genetic bee colony algorithm(GBC), Fish swarm algorithm (FSA),Cat swarm optimization (CSO), WOA Whale optimization algorithm (WOA), Artificial algae algorithm (AAA), Elephant Search Algorithm (ESA), Chicken Swarm Optimization Algorithm (CSOA), Moth flame optimization (MFO) algorithm, and Grey Wolf Optimization (GWO) algorithms have been discussed below. [4].

a.Genetic bee colony algorithm (GBC)

GBC is another streamlining approach which is planned by incorporating the upsides of the Genetic Algorithms (GA) and Artificial Bee Colony (ABC) for enhancing the

numerical issues. The accompanying steps are followed in ABC optimizing algorithm.
i. Setting ABC parameters
ii. Initialization of the population of bee solutions
iii. Evaluation of the population of bee solutions
iv. Identification of employee bee
v. Identification of onlooker bee
vi. Identification of scout bee
vii. Genetic operators

b. Fish swarm algorithm (FSA)

The FSA, which has points of interest of profound and proficient search, fast intermingling speed, is one of the significant, savvy streamlining algorithms. FSA emulate the conduct of fish, where each fish can identify for its food of nourishment dependent on various ways. Likewise, each fish can permit data interchanges with others fish until to get a global optimization. The conduct of the FSA incorporates various practices, for example, swarming, rummaging, following and arbitrary behavior.

c. Cat swarm optimization (CSO)

CSO algorithm is an ongoing calculation of advancement that can mirror the cat's conduct. In the most recent years, CSO has been connected to locate the ideal answer for certain applications. The mode looking for is connected during the resting time frame for cats, yet they are alert; while the following mode is comparing to the neighborhood search strategy to get the optimal arrangement of the given issue.

d. Whale optimization algorithm (WOA)

Whales are the greatest mammals among all creatures and they are excessive creatures. There are some significant principle parts of this creature, for example, humpback, executioner, blue, and finback. Whales never rest on the grounds as they have to inhale more often than not from the oceans and seas. Besides, half of the minds can just rest. Whales live alone or in gatherings. A portion of their part, for example, the executioner whales can live in a family a large portion of their life. The humpback whales are considered as the greatest whales, and their preferred prey is little fish and krill species. The exceptional chasing method for humpback whales is considered as the primary intriguing purpose of these whales which can be characterized as bubble-net feeding strategy.

e. Artificial algae algorithm (AAA)

AAA is an ongoing nature-inspired algorithm, and it is mirror the living ways of life and conduct of microalgae. This algorithm has been put together reenacted based with respect to microalgae ways of life, for example, the algal propensity, proliferation, and adjustment to the encompassing condition to change the predominant species. In this manner green growth have three principle fundamental procedures called, transformative procedure, helical development, and adjustment. The populace in this algorithm is made out of algal provinces. The algal cells in algal settlements will develop in the event that it gets enough light and, at that point the algal state will develop to a greater size. However, in the developing procedure, the algal province may not develop enough because of they experience the ill effects of deficient light. In helical development, each algal settlement will almost certainly move towards the best algal state.

f. Elephant Search Algorithm (ESA)

ESA has a place with the gathering of contemporary met heuristic inquiry improvement algorithms. This imitates the conduct and attributes of an elephant, and its system depends on double inquiry instrument, or the pursuit operators can be separated into two gatherings. In this situation, ESA has three fundamental qualities as powerful inquiry streamlining algorithm;(i) the hunt procedure iteratively refines the answer to get the ideal arrangement; (ii) boss female elephants lead concentrated neighborhood look at spots, where higher likelihood of finding the best arrangement is normal' (iii) The male elephants have obligations of investigations out of the nearby optima.

g. Chicken Swarm Optimization Algorithm (CSOA)

CSOA is an ongoing optimization algorithm that copies the practices of the chicken swarm and their hierarchical request. The swarm of chicken can be depicted by various gatherings; each gathering comprises of just a single chicken and numerous chicks and hens. There is a challenge in this warm between various chickens with a particular hierarchical request. The hierarchical request in this swarm is significant in the public activities of chickens, for example, group structure, the hens, the chicks and the mother hens. The conduct of the chicken swarm differs with male or female. The head chicken will decidedly scan for the food, and battle with chickens that are around the hunt region of the gathering. The chicken that rummages for nourishment will be reliable with the head chickens, and the agreeable chicken will remain in a similar area of the gathering to scan for their sustenance. For the most part talking in this swarm, there is a challenge between chickens; be that as it may, chicks look for the sustenance around their mom.

h. Moth flame optimization (MFO) algorithm

Moths in their practices are like the butterflies, and the principle highlights of moths are their method for route by night to fly toward evening glow. Moths as a rule utilize a strategy which is called transverse direction to explore in the night.

i. Grey Wolf Optimization (GWO) algorithm

The fundamental motivation methods in GWO algorithm depend on chasing and social initiative of dark wolves (Canis Lupus) which have a place with the Canidae family. Dark wolves typically live in gatherings, and the

pioneer of the gathering is called alpha and is in charge of certain exercises, for example, settling on choices about dozing spot and chasing. Their second wolf is called beta, and he helps the wolf alpha in deciding. The third grey wolf is called omega and is in charge of giving the data to the various wolves. The all other staying dim wolves are called delta and are in charge of overwhelming the omega.

The main phases of the GWO algorithm of gray wolves are based on the following steps:

(i) Track, chase and approach the prey;
(ii) Pursue, encircle and harass the prey;
(iii) Attack toward the prey.

5. Conclusion and Future Work

The principle objective of this paper is to focus on major security issues of IoT especially, centering the security attacks and their countermeasures. Because of absence of security system in IoT gadgets, numerous IoT gadgets become vulnerable objectives and indeed, even the information being transferred is lost. Also, various nature – inspired algorithms are discussed for clustering of nodes in WSN. In this paper, the security necessities are classified such as secrecy, uprightness, and confirmation, and so on. In this overview, in future, distinct kinds of attacks can be classified as low-level, medium-level, abnormal state, and incredibly abnormal state attacks alongside their temperament/conduct just as recommended answers for experience these attacks examined.

References

[1] Abdulatif Alabdulatif, Ibrahim Khalil, Xun Yi , and Mohsen Guizani, “Secure Edge of Things for Smart Healthcare Surveillance Framework”, Special Section on Smart Caching, Communications, Computing And Cyber security for Information-Centric Internet of Things, IEEE Access, Vol 7,(2019),pp 31010-31021.

[2] Youyang Qu, Shui Yu, Wanlei Zhou, Sancheng Peng, Guojun Wang, and Ke Xiao, “Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things”, IEEE Wireless Communications, (2018), pp 91-97.

[3] Jagruthi H, Dr.Kavitha C, “Integration of WSN with IOT: A Review on Security Issues”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 7, No. 5, (2018), pp 6217-6221.

[4] Ashraf Darwish. “Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications”, Future Computing and Informatics Journal Vol.3,(2018), pp. 231-246

[5] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah, “Security Issues in the Internet of Things (IoT): A Comprehensive Study”, International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, (2017),pp 383-388.

[6] Suchitra.C and Vandana C, “Internet of Things and Security Issues”, International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, (2016), pp 383-388.

[7] Partha Pratim Ray, Mithun Mukherjee, And Lei Shu, “Internet of Things for Disaster Management: State-of-the-Art and Prospects”, IEEE Access, Vol 5, (2017), pp 18818-18835.

[8] A. Sardana and S. Horrow, “Identity management framework for cloud based internet of things”, Proceedings of the First International Conference on Security of Internet of Things, (2012), pp. 200-203.

[9] Zhao, Walker and Wang, “Security Challenges for the Intelligent Transportation System”, Proceedings of the First International Conference on Security of Internet of Things, (2012), pp. 107-115.

[10] Lui, Xiao, Chen, “Authentication and Access Control in the Internet of things” 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), (2012), pp.588 – 592.

[11] Manikanthan, S.V., Padmapriya, T., An efficient cluster head selection and routing in mobile WSN, International Journal of Interactive Mobile Technologies, 2019.

[12] Li You-guo, Jiang Ming-fu, “ The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home Through the Use Of Middleware”, Fourth International Symposium on Knowledge Acquisition and Modeling (KAM), (2011), pp. 254 - 257.

Authors

M.S.Vinmathi has 22 years of teaching Experience and has published papers in various journals and conferences, and has membership in various professional bodies. Currently working as Associate Professor in Panimalar Engineering College.

Dr.M.S Josephine has experience of 20 years in teaching subjects for UG and PG students .She acted as Member in Board of Examination of MCA / M.Sc (CS) / M.Sc (IT), University of Madras, Committee member in Scrutini organizing MCA/M.Sc Examination – Bharathiar University, and Committee Member in Scrutinizing MCA Examinations – Loyola College. Guided Guided many Ph.D candidates in Dr.MGR University and other Universities. Acted as Doctoral Committee Member for Bharat and Anna University.

Dr.V.Jeyabalaraja has more than twenty four years for teaching experience. He has more than fifty paper publications in various reputed journals. He has addressed many conferences as a key note speaker, won many special awards in the field of his profession oriented activities. Presently he is working as a Professor, CSE department at Vellammal Engineering College, Chennai.