AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

A SUBJJECTIVE STUDY ON INDUSTRIAL WIRELESS NETWORK: GENERIC OPTIMIZATION

Vineeta Babu
Research Scholar
University of Technology, Jaipur
Dr. Pramod Sharma
Professor
University of Technology, Jaipur

Abstract:

When it comes to wireless sensor networks (WSNs), we believe that traditional special structured problems, such as the minimal spanning tree and network flow issues, can be of great assistance. The linear optimization section of this article explains these challenges. . In order for the sensors to effectively monitor the area of interest and communicate the information they have observed to the central processing station, one of the primary objectives of the design is to extend the lifetime of the sensor network as much as possible while maintaining its current functionality. In order to guarantee an even rate of energy consumption across the system, a multi-objective optimization strategy has been suggested in for the modular design architecture of the QoS aware routing protocol. In this paper we have discussed about security and optimization and its involvement in industries wireless network.

Keywords: Security, Optimization, Industry, Network, Energy.

I. INTRODUCTION

After four generations of development, wireless sensor networks integrate communication technology, embedded computing technology, distributed information processing technology, and sensor technology. This allows people to obtain information that is accurate and detailed, and brings the concept of "ubiquitous computing" one step closer to reality. It has enormous potential applications in areas like as national defense and the military, medical and health care, and environmental monitoring. The term "wireless sensor network" (sometimes abbreviated as "WSN") refers to a fundamentally new kind of wireless network that is built on an endless number of micro sensors powered by a limited quantity of batteries and is intended to gather information and monitor things. WSN is advantageous in many ways, including the provision of wireless communication channels and the maintenance of constantly shifting topological structures. However, there are also some drawbacks, such as inadequate infrastructure, an excessive amount of data flow, an endless number of nodes, a restricted supply of battery power, and mobile nodes. Because of these issues, it is now

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

much simpler for attackers to study the security weaknesses of a network in order to launch an attack and either destroy the entire network or a specific controlled item.

In general, the objective of the great majority of assaults is to damage the whole network, as well as to disable sensor nodes and cause confusion in the routing protocol. There are primarily two ways to avoid attacks at this time: encrypted measures and no encrypted measures. Both of these strategies are available. The primary objective of encrypting sensitive data is to guard against external incursions and stop hackers from penetrating a network in order to obtain access to sensitive information. In this scenario, other nodes on the network will be put in danger if one of the nodes is compromised by an adversary or taken over by the adversary. Because encryption techniques need a significant quantity of memory in addition to a high level of power consumption during processing and communication, they are not ideal for WSNs because of their restricted resource capacities. As a result, it is essential to employ additional precautions for safety. The approach that does not use encryption is used for the purpose of preventing assaults from within the network itself. The examination of assaults reveals that the majority of attacks are what are known as active attacks. Active assaults in WSN can take a variety of forms, and inside attackers have the ability to bring data packets into the wireless channel without restriction.

II. SECURITY AND OPTIMIZATION

Although it provides theoretical explanations, Information Security and Optimization has a focus on practical applications throughout the book. This book delves into ideas that are vital not just for the business world but also for the academic world. It includes features of methods and tools, such as definitions, usage, and analysis, that are extremely helpful for academics at any stage of their careers, from novices just starting out in their subject to seasoned professionals. What are the criteria for the policies? What exactly are vulnerabilities, and how can patches be used to correct them? What are some ways that data may be sent safely? How can the data that is stored in the cloud, as well as bitcoin that is stored on the block chain, be protected? How may algorithmic processes be improved? These are some of the questions that may arise, and the answers to them are provided in this article by making excellent use of examples from real life and case studies.

Features:

- An extensive collection of case studies and examples generated from real-life circumstances that match theoretical explanations with real happenings.
- Detailed explanations of several digital forensics-related security technologies, including their distinguishing characteristics and the procedures to follow in order to get practical experience with them.
- Innovative contributions to the formulation of security rules for organizations and lightweight cryptography.
- Discussion of the practical applications of block chain technology with biometrics in the context of crypto currencies and customizable authentication systems.
- Discussion and analysis of security in the cloud, which is significant due to the widespread usage of cloud services to satisfy the expectations of organizations and research, such as the

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

requirements for data storage and computing.

Students at both the undergraduate and postgraduate levels, in addition to researchers actively engaged in the field, can benefit much from studying Information Security and Optimization. It is possible to suggest it to students taking cyber security-related classes either as a reference book or a textbook.

The fact that security is an optimization problem is becoming progressively more obvious to people. The goal is often of an economic character the vast majority of the time. But achieving a safe system should be the goal, and this may be done by paying attention to things like limits and the implications of outages (contingencies). At the moment, the issue of security is predominantly dealt with in distinct phases in accordance with various models. It's possible that there's dispatch software that solely controls active power. A screening programme and a load flow both do their own independent examination of potential contingencies. In another scenario, an optimum power flow may be implemented based on an AC model that strictly adheres to a set of restrictions; nonetheless, contingencies would still be handled independently. Insofar as the strengthening of security, also known as the real control, is concerned, various ways apart from the 'optimal power flow are starting to become accessible. These are several strategies for effecting a corrective switch. They have not yet been presented as programmes of the production type. At this point in time, the development of the optimal power flow, also known as OPF, may be distinguished by a significant shift toward the Newton method.

The solution, which is derived from a Lagrange formulation of the issue, possesses a number of appealing characteristics, including

- ✓ the maintenance of a sparse distribution of elements
- ✓ the appropriateness for extremely large-scale systems
- ✓ a potential for separation or decoupling
- ✓ a successful convergence

The management of boundaries and restrictions is a challenge that has not been successfully addressed or overcome. We make use of penalty functions, which, compared to their earlier application in reduced gradient approaches, appear to produce outcomes that are more favourable in the present context. Quadratic programming, which is carried out in an iterative manner, is the rival technique in the OPF area. The formulation is not difficult to understand. It is possible to get around limitations and limits pretty well. At each iteration, the linearization of the expression as well as the formulation of the quadratic form are required to be completed. As a direct result of this, the convergence is rather satisfactory. The size of the hessian is the only constraint we have. Since it is at capacity, a large-scale system cannot be successfully managed at this time.

III. INDUSTRIAL WIRELESS SENSOR NETWORKS

In the subsequent five years, it is anticipated that the number of industrial wireless sensor networks (WSN) would expand by 553%, reaching over 24 million sensor points deployed. Recent advancements in wireless communication, power efficiency, extreme miniaturisation (made possible by MEMS

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

sensors, for example), and embedded computing technologies have led to the rise of viable wireless sensor networks for demanding industrial environments. These networks are able to monitor and collect data from a wide variety of objects, including people, vehicles, and machinery. Other factors contributing to this expansion include the fact that wireless sensor networks (WSNs) have reached a level of reliability that is suitable for the majority of industrial applications, the development of WSN standards tailored specifically for use in industrial settings, and an increase in public awareness and education regarding the advantages offered by WSNs. It would appear that wireless technology has arrived at a critical juncture in the industrial sector. WSNs are bringing about new uses, solutions, and applications; they provide huge advantages to many different industries; and they are effectively altering the paradigm by which industry functions. The fact that integrated chip solutions are now accessible at rates that the market can pay is the most important aspect of all of this.

A wireless sensor network is a network that can contain up to thousands of small autonomous sensors, also known as nodes that are physically dispersed over an area. These sensors are successfully linked and communicate with each other peer-to-peer through the use of radio frequency (RF) waves. While doing so, they monitor and communicate any local status or circumstances, such as temperature, vibration, pressure, pollution, motion, and so on. These intelligent sensors are able to autonomously monitor processes and do not ask for any human intervention unless a defect in the process develops that cannot be remedied by either the activity of the smart node or by human instructions that are launched remotely.

The smart sensors and nodes share data with one another and pass it along to other smart sensors through the network's myriad of possible pathways. These pathways may eventually lead to a central location where the information can be examined by a person, Each sensor or node may be as small as a pepper flake, but they still contain a CPU, a little memory (for example, 12 KB of on-chip RAM), low data rates (40 KB/s), a short range (most are 100' or less), and a low energy consumption rate. Moreover, they may be as small as a pepper flake. As a result of decreased costs, more integration, improved power management capabilities, and the use of more intelligent algorithms, it is currently feasible to reduce overall energy usage. In addition to that, energy harvesting brings power budgets to a point where there is no net consumption, and battery-less intelligent operation opens up new avenues for solutions that are only made feasible by this evolving technology.

IV. SECURITY AND OPTIMIZATION TECHNIQUE FOR INDUSTRIAL WIRELESS SENSOR NETWORK

Wireless sensor networks (WSNs) make it possible to monitor and control aspects of the physical environment from a remote place while maintaining a high degree of precision. The enabling technology is used in a variety of fields, including the monitoring of the environment, agriculture, healthcare, public safety, the military, industry, transportation systems, and smart homes for appliances. It is critical to have effective early warning systems in place for natural catastrophes including earthquakes, tsunamis, mudslides, flash floods, wildfires, and hurricanes. Integrating sensors into a network, which may be wired or wireless, is the primary supporting technology for early-warning-detection systems. This technology can be either wired or wireless.

WSNs often consist of components that are more compact compared to those used in wired

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

networks. These components are also typically more affordable and may be utilized in a diverse selection of contexts. The sensor, processing, communication, and power units make up the majority of the device. Because it is feasible to gather, analyses, and analyses data using these WSNs, as well as convey the findings, their location can be flexible. WSNs are very powerful because of these advantages; however, they also have many limitations, such as reliance on batteries as energy sources, lower central processing unit (CPU) and memory capacity, security vulnerabilities, and radio inference. These limitations make WSNs less desirable for some applications. Because of these constraints, it is necessary to have both a policy that is resource-aware for adaptation mechanisms and a policy that is security-aware for data security, both of which are based on the available resources of sensor nodes.

The location of a sensor node is not always in an area that is simple to access; in fact, there are occasions when they are put in locations that are exceedingly hazardous. When a sensor node has been installed to monitor a location that is inaccessible for ordinary maintenance, such as the replacement of batteries, it might be challenging to perform maintenance on the node. As a result, wireless sensor networks are required to function for extended periods of time, and their resources must be utilized in the most effective manner feasible. Increasing the lifetime of a sensor node may be accomplished in a number of ways, one of which is through the management and adaption of its energy consumption.

Our earlier research, in which we presented an Adaptable Resource and Security (ARSy) Framework, which incorporates resource and security adjustments, will be continued in this study as a continuation. The term "resource adaptation" refers to the process of managing a sensor node's usage of its battery, CPU, and memory. The term "security adaptation" refers to the process of implementing a certain security level in order to compensate for the excessive use of resources. The availability of resources is taken into account while adapting security measures. If a resource is used on average at a rate that is higher than a certain critical threshold, then the data that is generated has a level of security that is either high or medium. On the other hand, if the availability of the resource drops below the critical threshold, then the data's security is either low or even very low.

V. Generic Multi-Objective Optimization Problem in Wireless Sensor Networks

The network operators or the regulatory authorities are responsible for determining the values of the input parameters and decision variables in the generic resource allocation issue. For instance, the selection of the transmit frequency is impacted by the surrounding radio frequency environment as well as the laws governing the regulating body. The choice of frequency can have an impact on the sensors' transmission range, which in turn can have an effect on a number of crucial performance characteristics, such as coverage, bit error rate, and latency. Increasing or reducing the transmit power can have a major influence on a number of desirable objectives, including maximum energy efficiency, connection quality, network life time, dependability, coverage, cost, and packet error rate. These objectives can be reached by maximising energy efficiency. An optimization formulation was developed by the authors in for the purpose of maintaining sensing coverage in wireless sensor networks while preserving a limited number of active sensor nodes and a small amount of energy consumption. This was done. By concurrently satisfying latency and dependability through the use of a multi objective optimization

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

technique, energy consumption has been taken into consideration. Many performance measures, like as coverage, throughput, network life time, and packet error rate, can be affected by both the total energy and the residual energy of the nodes. In order to find a solution that strikes an acceptable balance between energy consumption and packet error rate, a multi-objective formulation has been utilized. The location and density of the sensors are the primary factors that influence the total cost as well as the performance of the network in terms of observability, coverage, transmission range, dependability, and the amount of energy that is consumed. Problems of practical optimization in wireless sensor networks are bound by a wide variety of parameters, including network connection, interference, and quality of service, transmit energy, coverage, topology, density, cost, latency, and dependability. The optimal location of sensors, optimal number of sensors, optimal scheduling, optimal transmit power, optimal coverage, optimal throughput, optimal delay, optimal cost, optimal packet error rate, fairness, and reliability are all expected to be the outcomes of these constrained optimization problems. The nature of the multi-objective optimization issue will shift in accordance with certain input parameters, the needed objective function to optimize, and the limits imposed by the particular region in which the sensor network is being deployed.

VI. CONCLUSION

In the late 1990s, researchers first started looking at wireless sensor networks. Since the turn of the 21st century, sensor networks have been the focus of significant interest from the military, business, and academics. Both the United States and Europe have initiated a significant number of research initiatives on sensor networks in rapid succession. The wireless sensors that are now being developed are becoming technically more powerful and economically viable as the technology continues to advance. Each node in a wireless sensor network (WSN) is made up mostly of units that are responsible for sensing, processing, radio transmission, determining their position, and occasionally mobilizers. These sensors take readings of the phenomenal circumstances in their immediate surrounds, digitize those readings, and then interpret the signals they receive to provide information about the conditions in their immediate surroundings.

REFERENCES

1. Beom-Su Kim , Ki-Il Kim ID , Babar Shah , Francis Chow and Kyong Hoon Kim, Wireless Sensor Networks for Big Data Systems, Sensors 2019, 19, 1565; doi:10.3390/s19071565 www.mdpi.com/journal/sensors, 2 of 18

2. Sari, Arif & Akkaya, Murat. (2016). Security and Optimization Challenges of Green Data Centers. International Journal of Communications, Network and System Sciences. 8. 492-500. 10.4236/ijcns.2015.812044.

3. Almohri, Hussain & Watson, Layne & Yao, Danfeng & Ou, Xinming. (2015). Security Optimization of Dynamic Networks with Probabilistic Graph Modeling and Linear Programming. IEEE Transactions on Dependable and Secure Computing. 10.1109/TDSC.2015.2411264.

4. Vishwakarma, Prabhat. (2011). Optimizing And Analyzing The Effectiveness Of Security Hardening Measures Using Various Optimization Techniques As Well As Network Management Models Giving Special

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

Emphasis To Attack Tree Model. International Journal of Network Security & Its Applications. 3. 100-109. 10.5121/ijnsa.2011.3409.

5. HU, ZHENGBING & Khokhlachova, Yulia & Sydorenko, Viktoriia & Opirskyy, Ivan. (2017). Method for Optimization of Information Security Systems Behavior under Conditions of Influences. International Journal of Intelligent Systems and Applications. 9. 46-58. 10.5815/ijisa.2017.12.05.

6. Doinea, Mihai & Sorin, PAVEL. (2010). Security Optimization for Distributed Applications Oriented on Very Large Data Sets. Informatica Economica Journal. 14.

7. Jiang, Ke & Pop, Paul & Jiang, Ke. (2016). Design Optimization for Security- and Safety-Critical Distributed Real-Time Applications. Microprocessors and Microsystems. 52. 10.1016/j.micpro.2016.08.002.

8. Dušan, Bogićević & Ivan, Tot & Sendelj, Ramo. (2016). IoT Security Optimization.

9. Bu, Jiahui & Liu, Ziang & Wu, Junlin. (2021). Research on Food Security system and Optimization method based on multiple regression Analysis. Journal of Physics: Conference Series. 1952. 042085. 10.1088/1742-6596/1952/4/042085.

10. Nandina, Viswanath & Luna, Jose & Lamb, Christopher & Heileman, Gregory & Abdallah, Chaouki. (2014). Provisioning Security and Performance Optimization for Dynamic Cloud Environments. IEEE International Conference on Cloud Computing, CLOUD. 979-981. 10.1109/CLOUD.2014.150.

11. Zhang, Xia & Zhan, Jinyu & Jiang, Wei & Ma, Yue. (2013). A Vulnerability Optimization Method for Security-Critical Real-Time Systems. Proceedings - 2013 IEEE 8th International Conference on Networking, Architecture and Storage, NAS 2013. 215-221. 10.1109/NAS.2013.34.

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification/ Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright / Patent/ Submission for any higher degree or Job/ Primary Data/Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and thereforethe process of resubmission is there for the scholars/students

ISSN:2320-3714
Volume:3 Issue:3
September 2021
Impact Factor:5.7
Subject:Engineering

who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything isfound illegal publisher may also take legal action against me.

Vineeta Babu
Dr. Pramod Sharma

*****