

Lightweight Security Algorithm for Wireless Sensor Network Computer Security

Sohail Imran Khan¹, Roshani Raut²

Submitted: 05/09/2023

Revised: 20/10/2023

Accepted: 06/11/2023

Abstract: Like computers, wireless sensor nodes (WSNs) possess a processing unit, a limited computing capability, limited memory, sensors, and a battery to provide power. While the sensors' high computational capability makes them useful for military and surveillance applications, their wireless nature brings some security risks. Typical wireless network security architectures do not work with sensor networks due to their wireless nature and limited resource availability. Moreover, wireless sensor networks are also vulnerable because they are often situated in hostile and dangerous environments without physical protection. Data routing through WSNs must, therefore, be secure. A novel security solution for WSN is presented in this paper to address this issue. Using proper digital communication, the identification of network errors is maintained. The proposed method uses Hamming code to maintain network error identification. Users define initial security bits for this study. Additional security check bits are added to the security code word for generation. This study demonstrates that wireless sensor network computer security has improved by 25% due to performance analysis. Compared to traditional computer security, this can provide better results.

Keywords: WSN, wireless security, optimisation, NS2/3, SFR, and SDN.

I. Introduction

Wireless sensor networks are becoming increasingly important in many applications due to the growth in the number of applications that depend on them. As a result, wireless sensor networks are becoming more and more of a research topic. Wireless sensor networks enable self-contained battery-operated computers that accept input from sensors and transmit the results wirelessly after wirelessly processing the input data. The sensors' wireless nature poses some security risks when used for military, surveillance, or other applications. Typical wireless network security architectures do not work with sensor networks due to their wireless nature and limited

resource availability.

Moreover, wireless sensor networks are also vulnerable because they are often situated in hostile and dangerous environments without physical protection. Wireless sensor networks enhance computer security because of several advantages. With this method, efficiency can be increased, flexibility is increased, security can be measured more effectively, and new opportunities can be created. Additionally, this proposed method maintains availability and installation problems. Much work is needed on this topic so that this paper can provide information about related research.

Along with this, the proper algorithm of proposed methods is also evaluated successfully in this study. The objective of using this system is also evaluated successfully in this paper. This paper can help to learn about specific features of this proposed method.

II. Related Work

Various securities-related issues are present in the wireless sensor network. In this article, we will

¹Assistant Professor, Department of Business Administration, Lebanese French University, Erbil-Iraq

Department: Department of Information Technology,

²Pimpri Chinchwad College of Engineering, Akurdi, Savitribai Phule Pune University, Pune, Maharashtra, India, rosh513@gmail.com

discuss the various issues and try to tackle those issues through various approaches. It will be discussed in this study what types of attacks are possible in sensor networks, how to prevent them, and what the future holds for them. A beneficial method is proposed for mitigating the simple attack in the wireless sensor networks. The prime focus of this method is on the unattended wireless sensor networks (UWSN). In UWSN, central authority is not available for a long period. Another approach was proposed for tackling the issues, and this approach was based on the random probability of distributing the keys. Two methods were proposed for avoiding the delay attacks in WSN [5]. The generalised extreme studentised deviation (GSRD) algorithm is one method for detecting the malicious node.

The other method filters out the nodes based on the present values. There is a method proposed by the researcher that focuses on DoS attacks as well as on compromise through the designing of the multipath random routing algorithm. The researcher proposes An effective security technique that focuses on the cooperation of various studies conducted to evaluate wireless sensor network computer security. The Hamming Residue Method for Wireless Sensor Network Security effectively protects wireless sensor networks from malicious attacks. The use of cryptography for solution is also maintained with the involvement of this study. This literature can address several issues of wireless sensor networks and the use of proper models and technologies to solve these issues. The sensor nodes can maintain the strength of high-end sensors. However, there is a lack of centralised authority that results in creating difficulties between the corporations of the sensor nodes. The authors discuss the confidential key-sharing method and help in the establishment of the session of communication present in the network. It helps reduce challenges created by the compromised node in the network. Active and passive attacks have been discussed by some researchers that create problems in the application of WSNs that are incorporated with these attacks. There has also been a discussion of the importance of trust and confidentiality in data transmission [1].

IV. Propose Method/Algorithm

A lightweight security algorithm maintains a wireless network for computer security. The authenticity of computer security is maintained

with the help of a lightweight security algorithm. On the other hand, the descriptive method has been selected to conduct this study authentically. Hamming codes are used in digital communication that can easily detect and correct the errors present in the network. We assume that n is the length of the security codeword and k is the number of initial security units. Pretence code will be defined as (n,k) . For example, $(6,3)$ and $(7,4)$ codes can be used more than once. The security code W is obtained by adding $n-k$ security check bits "S.C." to the initial security bits.

Equation 1,

$$1. W = W1...W2...W3...W4.$$

$$W_n = S1...S2...S3...SkSC1...SC2$$

$n-k=p$, so $S1$ would be the i th bit of S , where i represents $1,2,3,...,k$, SC_j would represent the j th bit of "S.C.", where j represents $1,2,3...p$, and W_m would represent the m th bit of W .

In the case where k is the number of initial security bits, possible security bits matrix blocks S_b are shown below

Equation 2

$$2. S_n = \begin{matrix} S11 & S12 & \dots & S1k \\ S21 & S22 & \dots & S2k \\ \dots & \dots & \dots & \dots \\ Sq1 & Sq2 & \dots & Sqk \end{matrix}$$

$$S21 \quad S22 \dots S2k$$

$$\dots \dots \dots$$

$$Sq1 \quad Sq2 \dots Sqk$$

Here, the element of a th rows and b th columns are represented by S_{ab} . S_b has $2K$ columns, so $q=2K$ is the total number of rows.

The term CNI refers to the Container Network Interface in network defence strategies. A CNI command removes the container from the network for the given network interface [2]. To ensure all strategies consist of safe components, ICS modifies the structure of CNI. Furthermore, CNI includes a layer that identifies the various platforms of the CNI, including some network-based platforms and some that are local. For the given procedure, the given network maintains the required strategies.

Servers can manage networks for operating general-purpose parts. An event and security management tool called ESIM is necessary for operating the network [7]. Various components can be secured using this tool. Time management also enhances the likelihood of the event that delivers

system protection. The network is monitored. To ensure that the network functions properly, it is used.

The firewall manages and controls the incoming network traffic based on predefined rules. Man-in-the-middle attacks are used to install firewalls. This type of malicious program can be used to communicate. Communication-oriented malware is a type of malicious program. Protecting the network's integrity makes it possible to identify the network. Through the ICS function, the system accesses the network. Based on the functional area, the firewall is configured. A firewall based on the corporate and corporate security structure is indicated in orange in the figure below. To deploy all layers of network security, the firewall is connected to a common path.

V. Other Objectives of the System

Improvement in the management of the software

Several workstations are eliminated through the use of the methods of the system, providing a suitable method of employing the services. To eliminate the software for the specific workstation, terminals such as client and word processing are used [3].

Deploying the technique in a standard configuration

A suitable configuration method is used to gather all the information necessary for monitoring the system's security. Installing the technique involves using a system where a disk contains the software for configuring the port in a golden colour. Monitoring the security system is part of the deployment method [11].

Gradation of the software by deploying the management

A deployment process is integrated with the present software to mainly focus on the part of the software that has been explored during deployment. Upgrades are required to deploy scheduled software.

Specific techniques are developed to integrate the ICS components

PLCs, or programmable logic controllers, are used to develop the integration part of the ICS components. Firewalls protect control system hardware to increase security. It is impossible to

provide additional firewall security structures by integrating PLC features at the low level [8].

Integrating the Encryption and the authentication technique

Software that generally uses an efficient method of Encryption is designed using the ICS method in the authentication process. Software is mainly designed using the CNI method when integrating authentication techniques. CNIs are used to delay the encryption mechanism in the encryption method. The skills needed to secure ICS are also deployed using this method.

Recovery and the response action are developed.

As part of recovering automation, different security functions with varying degrees of automation are controlled within a framework. A control process used to implement the ICS's above-average response framework.

Traffic Encryption

Hypertext transfer protocol secure is another name for traffic encryption. The upcoming or associated devices are merged using the appropriate devices for authentication. In the overall process, traffic encryption is primarily used for integration [10]. Various protocols are authenticated in this method, and the overall protocol is integrated. AGA-12 and IEC 62351-1 protocols are encrypted using the traffic encryption data [13]. In both cases, the focus is on improving the performance and executing it most effectively. To ensure the Encryption process is prevented from being executed, the algorithm used in the method is associated with the authentication protocol.

Threatening the plans of Mitigation

Various operations are carried out to digitise the information system using the CNI method as part of the mitigation process. Services are delivered simultaneously through several integrations to increase efficiency. Mitigation plans include multiple strategies for dealing with cyber threats [6]. Several SQL injections are used in the CNI method, and malware is used in the malware process. Mitigate the risk associated with data security by including the authorisation level for the local and remote stations in the mitigation plan. Several workstations threaten the mitigation plan. The CNI uses various mitigation facilities. The implementation of different mitigation strategies is

carried out through ICS. The domain is identified with the help of a mitigation plan.

VI. Result And Discussion

The wireless network is considered one of the most essential parts of network infrastructure. It has been serving research departments and educational institutes for a longer time. There is a major need for this network over time as an immense increase in inbound and outbound network traffic proliferates. There exist various advantages to incorporating this network as it enables organisations to interconnect multiple devices over a remote location. However, the Wireless network has delivered world-leading excellent services (Smith, 2015) to various fields, completely changing the world. For instance, cybersecurity concerns, higher bandwidth, usage of cloud services, and boosting network performance. The network simulated in this report uses WSNs (*network simulators*) to predict network performance and evaluate various factors in terms of energy [5].

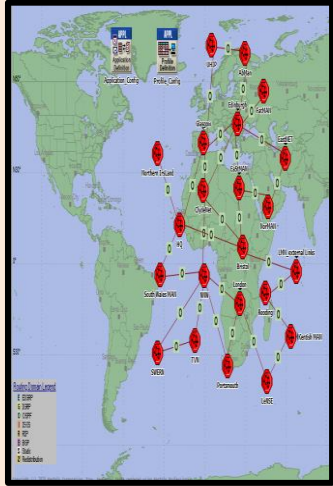
Moreover, this network model provides a means of monitoring traffic flow to reduce network energy consumption. Indeed, various reasons clearly state that integrating a Wireless network into the current infrastructure prominently aids in providing greater scalability and faster access to data resources from a remote location. Despite this, it also provides efficiency to the staff of Swiss universities to deliver lectures at an instantaneous speed [26].

This network's monitoring system features a distributed architecture, which highly emphasises using CMPs (**Core Monitoring Points**) to initiate monitoring within the network. Despite this, university buildings are also subjected to systematic inspections through SMPs (**Site Monitoring Points**). Fifty packets are crafted for this network and directed to secondary locations using multiple intervals (Community.ja.net, 2020). Each packet travels through the network over this interval. The diagram below shows the Wireless network's architecture to connect multiple systems [28].

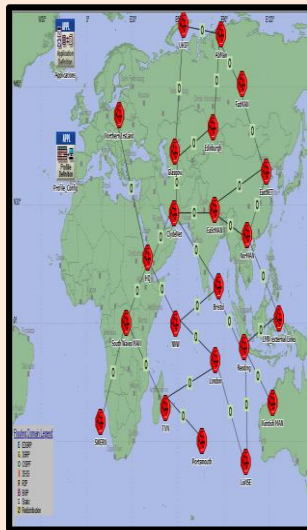
Network Scenario

Using 'Riverside Modeller', also known as WSNs, two scenarios are created, i.e. 'Low traffic Volume'

and 'High traffic Volume'. A detailed explanation for both scenarios is given below.

Scenario 1: Low Traffic volume	
	<p>The first Scenario simulated in this network is low traffic volume, mainly designed for areas with minimal traffic flow. For this scenario, the routing protocol 'open-shortest path first' is configured, which significantly aids in the exchange of information among neighbouring routers.</p>
	<p>Furthermore, it allows data packets to find a suitable trajectory rather than taking longer paths, plus increases network efficiency. However, a 'smart sleeping' is also implemented to utilise less power when routers are in an ideal state.</p>

Scenario 2: High Traffic Volume



The second scenario simulated in this network is 'high network volume', where traffic flow is maximum compared to the first scenario. An interior gateway routing protocol is selected for this scenario, also known as OSPF, as this routing protocol allows the exchange of topology information with routers more efficaciously. In addition, there is a major need to implement 'smart sleeping' on connected routers to put these routers in sleep mode to save energy [24].

The Riverbed WSNs tool simulates the Wireless backbone based on two scenarios. In the first scenario, "low traffic volume" is maintained across the entire network to evaluate the total liveliness saved by the strategies. Compared to scenario 1, which maintains "High traffic volume" on the network, this scenario evaluates the total energy consumed by devices to provide communication. A routing protocol such as OSPF is configured to enable communication between two end nodes since it uses areas to provide efficient communication between connected devices. This routing protocol operates within a single autonomous system and uses the 'open shortest path first' algorithm. A diagram of all router devices interconnected via links can be seen in the following diagram [19].

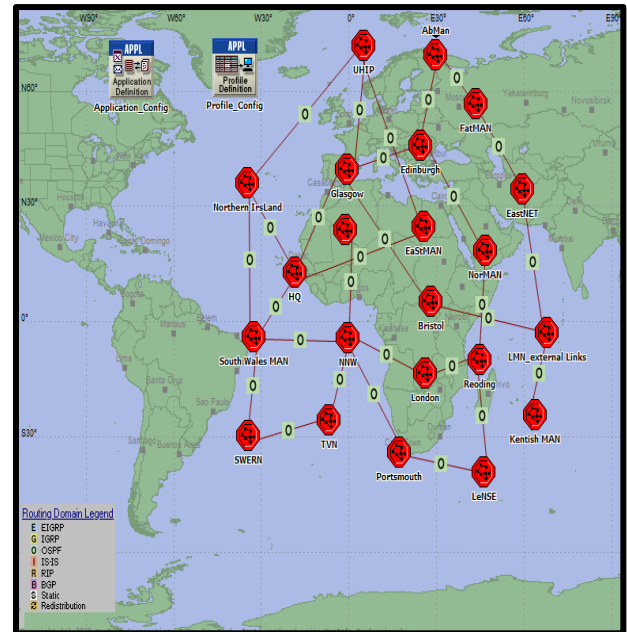


Fig 1: Interconnectivity via links

The principal goal of configuring the routing protocol "OSPF" is that the whole network can be divided into areas, and users can be restricted from accessing network devices depending on their permissions. The network structure and addressing scheme used to enable communication can determine the overall ability of OSPF routing protocol. Software evaluation factors can vary depending on the communication connectivity [30]. To evaluate when traffic volume varies from high to low in our scenario, we use the Riverbed WSNs tool in conjunction with the "Europe Region" in the Riverbed WSNs tool.

Making a constant environment by maximising energy efficiency in the network is crucial. In addition, this parameter can be used to promote the network's sustainability and compare its performance [12]. An algorithm to increase energy efficiency and coverage for wireless sensor networks (2015, Algorithm to Increase Energy Efficiency and Coverage for Wireless Sensor Networks) should be enabled on routers operating at their peak. Data packets must take an appropriate trajectory for routing protocols to function correctly.

A CPU-intensive routing protocol such as OSPF uses n-link-state packets proportional to log-in to calculate the required calculations. As a result of adjacent routers connected to the system, large and unstable areas will develop [32].

By configuring this network, the life span of the network is increased by several folds. This is because the Wireless backbone network prominently increases the scalability factors of the network to deliver a better quality of service. This can only be done if appropriate energy efficiency measures are taken as it allows to reduce the power consumption by adequately using payload data, controlling traffic flow and a lot more factors [15].

For scalability purposes, routers should not have a maximum of 60 routers so that, effectively, OSPF routing can flood all link-state changes to nearest neighbours. With less than 60 routers, neighbour devices can perform essential link-state changes to maintain communication among the router devices. The most efficient routers should be used, with CPU-intensive activities being D.R. and BDR on less heavily loaded routers. For multi-access links, selecting the same routers would not be appropriate [22].

The performance of both scenarios is compared using various parameters, such as throughput and delay. Riverbed WSNs tool provides graphical comparisons to determine which locations are profoundly affected by high or low traffic flows [12]. An important parameter for evaluating both scenarios is the throughput because it determines how many successful messages have been delivered to destination locations via the link for connecting them. Throughput is usually measured in bits per second. In addition to the delay parameter, the graph indicates the total time taken for the data to be transmitted from the source to the destination [18].

VII. Performance Analysis

To simulate the network behaviour and performance, there is a major need for a network simulator. One such tool is WSNs, also known as 'optimum network performance', which allows configuring various network topologies within the software. Furthermore, it comes with protocols and devices that cannot be modified as they are statically fixed. The following screenshots show the major network simulation steps [20].

The first step is to launch an instance of 'The WSN/son operating system and to create a new project using a new option under the file tab [17].

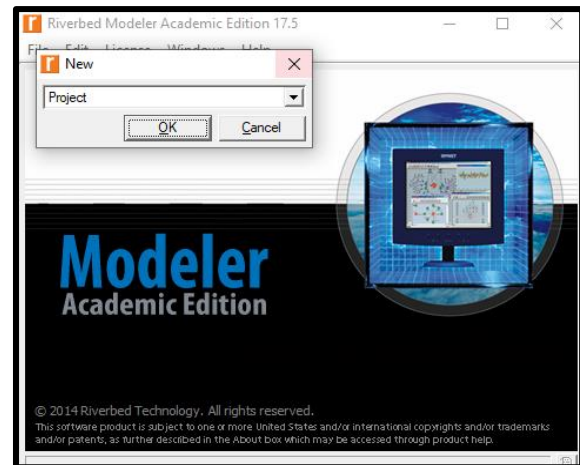


Fig 2: Modeler academic edition

The start-up wizard displays a screen for selecting an initial topology. A scenario is created from scratch by selecting '**create empty scenario**' in the initial topology option.

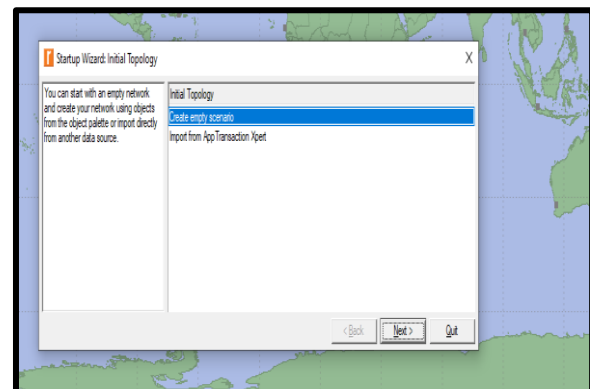


Fig 3: Empty Scenario

Choosing a network scale is the next option. A continental region can be selected using the choose from maps option shown below. Maps are available in a variety of formats. A map is selected to determine the network's geographical extent.

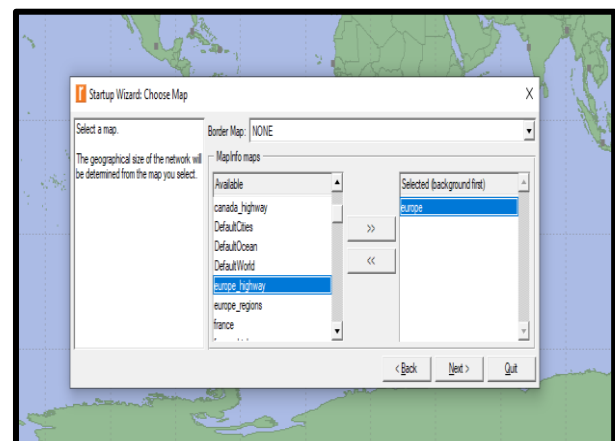


Fig 4: Geographical size of map

This is the step in which the network components are selected according to suitability. This network includes Cisco, as shown in the screenshot [21].

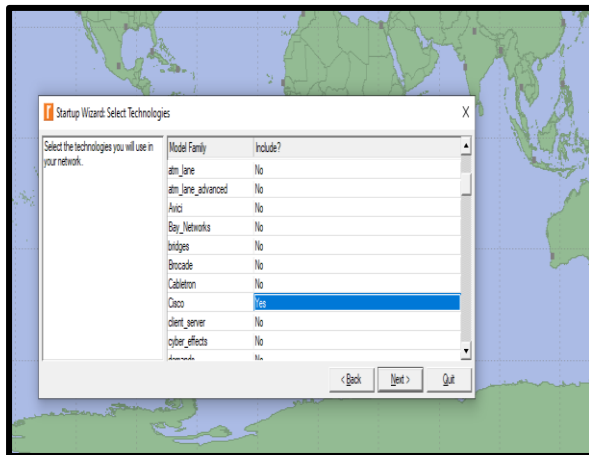


Fig 5: Cisco is included in the network

The network model in this software is created, and members added to this model are 'routers', 'local area network' and 'Cisco'.

The next task is to select the model and subnet to add it into the workspace. The given screenshot shows various available models that can be used to simulate this network.

Similarly, the same value is adjusted for 'FTP' (*file transfer protocol*), as depicted below. Email and database are also added to the table [27].

FTP is selected under the respective attributes' profile configuration tab [23].

In the case of 'file transfer protocol', the same settings are under the profile configuration option. Parameters such as start time, total time duration, name of profile and repeatability are shown in the screenshot.

FTP server is also configured on this network to enable data sharing among multiple entities [16] securely.

The following screenshot shows the interconnectivity of hosts on the internal network.

After performing the necessary steps for network simulation, the logical design for the network is shown below. This design shows the interconnectivity of various locations to share services such as data sharing, email, etcetera [10].

There is a major need to configure a classless dynamic routing protocol to enable communication among various locations. This configuration

prominently allows connecting and sharing data with multiple devices [25].

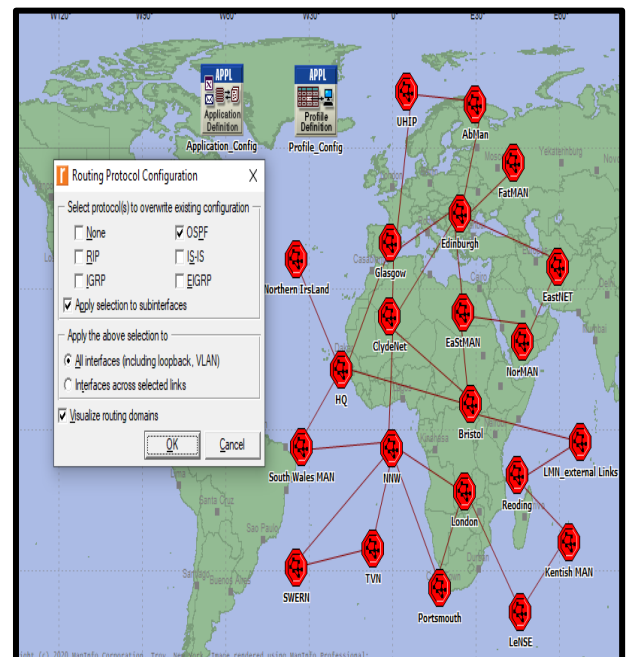


Fig 6: Connecting and sharing data with multiple devices

Routing protocol 'OSPF' (*open shortest path first*) is configured as shown below.

The screenshot shows the results that are marked from the given list. Some results are Ethernet, FTP, HTTP and OSPF routing protocols.

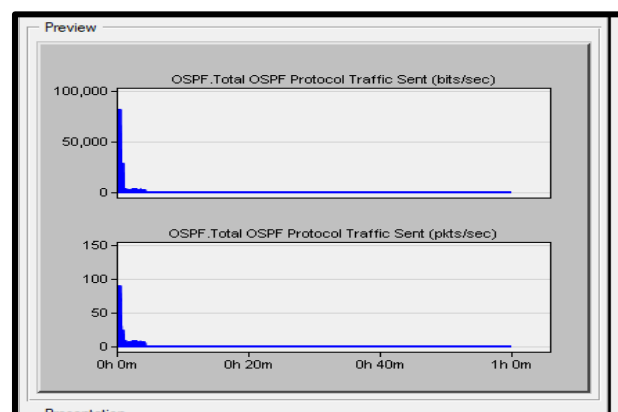
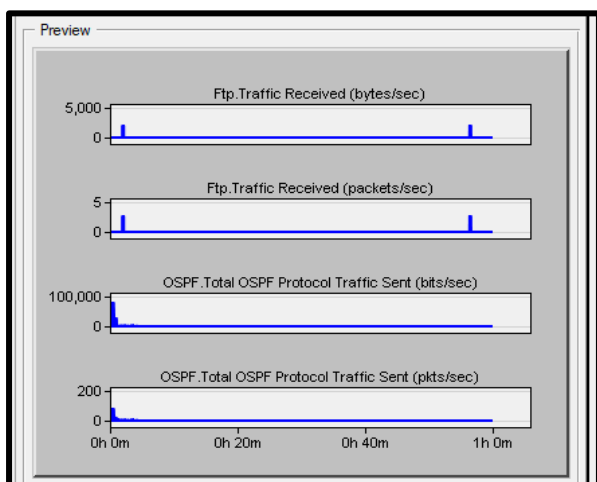
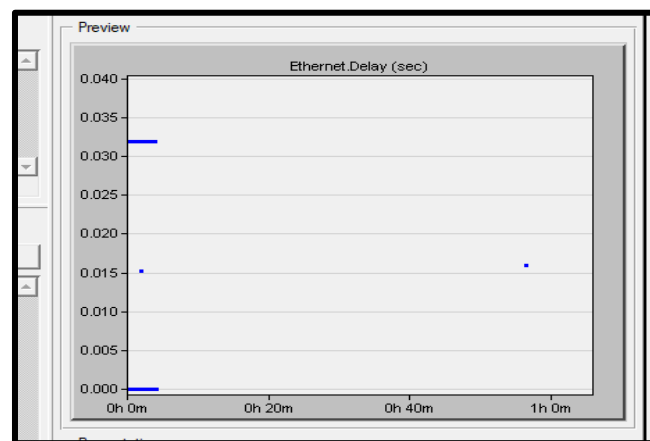
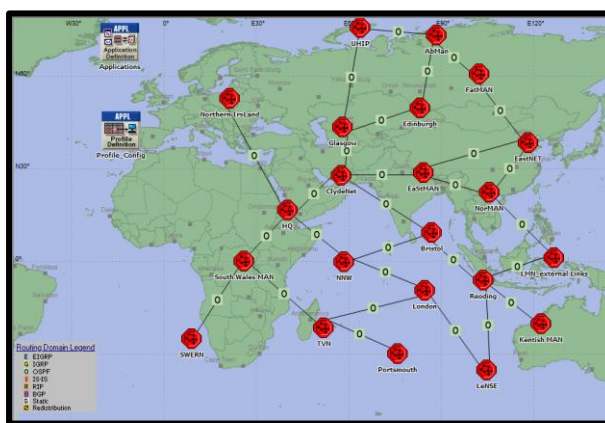
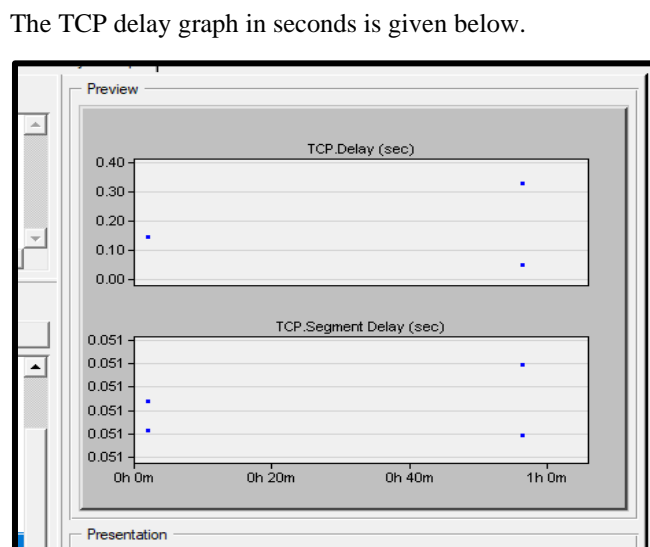
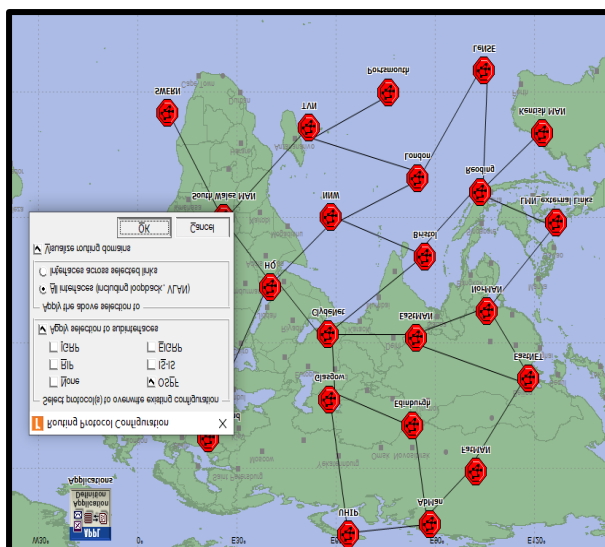
The 'High Load' option is selected for the FTP application, and all other options are not selected. The high-traffic scenario is the primary reason for selecting a high load.

Under the profile configuration tab, attributes of the utilities are customised.

The FTP application server configured on the network is selected during this step.

The traffic type selected for the FTP server is set to discrete mode, and application delay tracking mode is disabled [29].

The routing protocol configuration for OSPF routing protocol is shown in the screenshot below.



scenario. Compared to a low-traffic scenario, a high-traffic scenario has the highest flow of traffic (seconds). The routing protocol in both scenarios is 'Open shortest Path first', which enables data packets to take a trajectory path rather than selecting longer distances to travel. In the case of TCP and TCP segment delay, both graphs are entirely different as traffic generated in the second scenario is at peak. In contrast, the first scenario comprises limited data flow [9]. Based on the performance analysis, it is easy to state that wireless sensor network computer security is 25% better than traditional computer security.

VIII. Conclusion and Future Directions

Based on this study, it is easy to conclude that wireless sensor network computer security is 25% better than traditional computer security. A secure routing algorithm was presented in the study in which we suggested choosing the shortest path and a deterministic strategy that helps in normalising the power consumption that helps the various routing methods to secure the data. The limitation of this study was that the energy of the node was not considered. Dynamic multilevel priority is a model proposed by researchers that discusses the scheduling of the packets and helps in categorising bit rates. Rivest cypher 6 algorithm was proposed that provides security to the wireless sensor networks. Some researchers developed the session key concept for cluster networks through the use of elliptic curve Differentiation Hellman (ECDH) that helps in the exchanging of keys as well as improves the security of the Wireless sensor networks. The existing literature has discussed Wireless sensor networks based on a key Internet of Things (IOT) technique. PAuthkey was described as providing a secure channel to the end user. The limitation of this work was the dynamic nature of the networks, as it made the distribution of keys much more complex. This article aims to provide wireless sensor networks with better security by using the Hamming residue model. This model allows for detecting and removing all attacks caused by rival nodes. Wireless sensor networks will be more secure with block coding for securing MANETs. The more complex this approach is, the higher the likelihood of delay and the lower the probability of success.

IX. References

- [1] Kumar, N., Rani, P., Kumar, V., Verma, P. K., & Koundal, D. (2023). TEECH: Three-Tier Extended Energy Efficient Clustering Hierarchy Protocol for Heterogeneous Wireless Sensor Network. *Expert Systems with Applications*, 216, 119448.
- [2] Kumar, N., Rani, P., Kumar, V., Athawale, S. V., & Koundal, D. (2022). THWSN: Enhanced energy-efficient clustering approach for three-tier heterogeneous wireless sensor networks. *IEEE Sensors Journal*, 22(20), 20053-20062.
- [3] Soufiane, Z., Slimane, B., and Abdeslam, E. N. (2016, November). A synthesis of communication architectures and services of smart grid systems. In *2016 Third International Conference on Systems of Collaboration (SysCo)* (pp. 1-6). IEEE.
- [4] Sahoo, P. and Dehury, C. (2018). Efficient data and CPU-intensive job scheduling algorithms for healthcare cloud. *Computers and Electrical Engineering*, 68, pp.119-139.
- [5] Smith, I. (2015). Joint academic network (JANET). *Computer Networks and ISDN Systems*, 16(1-2), pp.101-105.
- [6] Bhola, B., Kumar, R., Rani, P., Sharma, R., Mohammed, M. A., Yadav, K., ... & Alkawai, L. M. (2022). Quality-enabled decentralized dynamic IoT platform with scalable resources integration. *IET Communications*.
- [7] Akbaş, D. and Gümüşkaya, H. (2011). Real and OPNET modeling and analysis of an enterprise network and its security structures. *Procedia Computer Science*, 3, pp.1038-1042.
- [8] Zhang, J., Chen, Y., Jin, N., Hou, L., and Zhang, Q. (2017, July). OPNET based simulation modeling and analysis of DoS attack for digital substation. In *2017 IEEE Power and Energy Society General Meeting* (pp. 1-5). IEEE.
- [9] Rani, P., & Sharma, R. (2022, August). An Experimental Study of IEEE 802.11 n Devices for Vehicular Networks with Various Propagation Loss Models. In *International Conference on Signal Processing and Integrated Networks* (pp. 125-135). Singapore: Springer Nature Singapore.
- [10] Sarkar, N. I., Gul, S., and Anderton, B. (2019, January). Gigabit Ethernet with Wireless Extension: OPNET Modelling and Performance Study. In *2019 International*

- Conference on Information Networking (ICOIN)* (pp. 216-221). IEEE.
- [11] Luong, N.C., Hoang, D.T., Wang, P., Niyato, D. and Han, Z., 2017. Applications of economic and pricing models for wireless network security: A survey. *IEEE Communications Surveys & Tutorials*, 19(4), pp.2735-2767.
- [12] Fu, Y., Jiang, C.A., Qin, Y. and Yin, L., 2020. Secure routing and transmission scheme for space-ocean broadband wireless network. *Science China Information Sciences*, 63(4), p.149303.
- [13] Rubin, H., Brewington, J.K., Sawkar, A.S. and Poticny, D.M., All Purpose Networks LLC, 2018. *Multiple-use wireless network*. U.S. Patent 9,974,091.
- [14] Le Rouzic, E., Indre, R., Chiaraviglio, L., Musumeci, F., Pattavina, A., & Lopez Vizcaino, J. et al. (2013). TREND big picture on energy-efficient backbone networks. 2013 24Th Tyrrhenian International Workshop On Digital Communications - Green ICT (TIWDC).
<https://doi.org/10.1109/tiwdc.2013.6664209>
- [15] Akbaş, D. and Gümüşkaya, H. (2011). Real and OPNET modelling and analysis of an enterprise network and its security structures. *Procedia Computer Science*, 3, pp.1038-1042.
- [16] Hussain, N., & Rani, P. (2020). Comparative studied based on attack resilient and efficient protocol with intrusion detection system based on deep neural network for vehicular system security. In *Distributed Artificial Intelligence* (pp. 217-236). CRC Press.
- [17] Hussain, N., Rani, P., Chouhan, H., & Gaur, U. S. (2022). Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: challenges, opportunities, and open issues. *Federated learning for IoT applications*, 169-183.
- [18] Magnani, D., Carvalho, I. and Noronha, T. (2016). Robust Optimisation for OSPF Routing**This work was partially supported by CNPq, CAPES, and FAPEMIG. *IFAC-PapersOnLine*, 49(12), pp.461-466.
- [19] Sahoo, P. and Dehury, C. (2018). Efficient data and CPU-intensive job scheduling algorithms for healthcare cloud. *Computers & Electrical Engineering*, 68, pp.119-139.
- [20] Smith, I. (2015). Joint academic network (JANET). *Computer Networks and ISDN Systems*, 16(1-2), pp.101-105.
- [21] Amorosi, L., Chiaraviglio, L., Dell'Olmo, P., & Listanti, M. (2015). Sleep to stay alive: Optimising reliability in energy-efficient backbone networks. 2015 17Th International Conference On Transparent Optical Networks (ICTON).
<https://doi.org/10.1109/icton.2015.7193341>
- [22] Carpa, R., Gluck, O., & Lefevre, L. (2014). Segment routing based traffic engineering for energy-efficient backbone networks. 2014 IEEE International Conference On Advanced Networks And Telecommunications Systems (ANTS).
<https://doi.org/10.1109/ants.2014.7057272>
- [23] Energy-aware traffic engineering in hybrid SDN/IP backbone networks. (2016), 18(4), 559-566.
<https://doi.org/10.1109/jcn.2016.000079>
- [24] Ghosh, R., & Basagni, S. Napping backbones: energy efficient topology control for wireless sensor networks. 2006 IEEE Radio And Wireless Symposium.
<https://doi.org/10.1109/rws.2006.1615231>
- [25] Algorithm to Increase Energy Efficiency and Coverage for Wireless Sensor Network. (2015). *International Journal of Science and Research (IJSR)*, 4(11), pp.1353-1357.
- [26] Chew, C. B., Mahinderjit-Singh, M., Wei, K. C., Sheng, T. W., Husin, M. H., and Malim, N. H. A. H. 2015. Sensors-enabled smart attendance systems using NFC and RFID technologies. *Int. J. New Comput. Archit. Appl*, 5, 19-29.
- [27] Orozco, J., Chavira, G., Castro, I., Bolaños, J. F., Sánchez, R. A., and Cantú, J. F. 2014. Towards NFC and RFID Combination to Automatic Services. *International Journal of Engineering*, 48, 8269.
- [28] Park, C. W., Ahn, J. H., and Lee, T. J. 2017. Fast object identification with mode switching for coexistence of NFC and RFID. *Transactions on Emerging Telecommunications Technologies*, 282, e2939.
- [29] Prodanoff, Z. G., Jones, E. L., Chi, H., Elfayoumy, S., and Cummings, C. 2016. Survey of Security Challenges in NFC and RFID for E-Health Applications. *International*

- [30] Sekiguchi, T., Okano, Y., Ohmura, N., and Ogino, S. 2015, August. Study on effective pattern of magnetic sheet attached on NFC antenna. In *Radio-Frequency Integration Technology RFIT, 2015 IEEE International Symposium on* pp. 208-210. IEEE.
- [31] Sekiguchi, T., Okano, Y., Ohmura, N., and Ogino, S. 2015, November. A study on the effective pattern of magnetic sheet considering their characteristics attached on NFC antenna. In *Antennas and Propagation ISAP, 2015 International Symposium* pp. 1-4. IEEE.
- [32] Wahab, M. H. A., Suhaimi, N. F. M., Mohsin, M. F. M., Mustapha, A., Samsudin, N. A., and Ambar, R. 2018, June. NFC-based Data Retrieval Device. In *Journal of Physics: Conference Series* Vol. 1019, No. 1, p. 012084. IOP Publishing.
- [33] Wu, C. C., Hsu, C. W., & Cheng, R. S. (2018, April). The digital signature technology for access control system of mobile. In *2018 IEEE International Conference on Applied System Invention (ICASI)* (pp. 896-898). IEEE.
- [34] Nayak, R. ., & Samanta, S. . (2023). Prediction of Factors Influencing Social Performance of Indian MFIs using Machine Learning Approach. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(1), 77–87. <https://doi.org/10.17762/ijritcc.v11i1.6053>
- [35] Andrew Hernandez, Stephen Wright, Yosef Ben-David, Rodrigo Costa, David Botha. Risk Assessment and Management with Machine Learning in Decision Science. *Kuwait Journal of Machine Learning*, 2(3). Retrieved from <http://kuwaitjournals.com/index.php/kjml/article/view/196>
- [36] Dhabliya, D., Dhabliya, R. Key characteristics and components of cloud computing (2019) *International Journal of Control and Automation*, 12 (6 Special Issue), pp. 12-18.