The Seybold Report

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

ENHANCING SECURITY AND ENERGY EFFICIENCY IN SDN NETWORKS THROUGH MACHINE LEARNING-ASSISTED TRUST SECURE ATTACKER

M. SABARISH

Research Scholar, Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamilnadu. Email: sabarish84@gmail.com

Dr. A. S. ARUNACHALAM

Associate Professor, Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamilnadu. Email: arunachalam1976@gmail.com

Abstract

SDN networks become more vulnerable to assaults as they grow in size, necessitating the use of strong security methods. Due to the sensor nodes' limited energy, compute capabilities, and storage resources, identifying adequate cryptography for wireless sensor networks is a serious problem. For Adhoc networks, new energy-aware routing algorithms called trustworthy Machine Learning Trust Secure Attacker Detection will be provided. Energy efficiency, reliability, data aggregation, and attacker detection are all essential SDN criteria addressed by MLTSAD. MLTSAD is an energy-efficient routing method that creates routes for end-to-end packet traversal that utilize the least amount of energy while simultaneously increasing malicious node detection. We presented a cryptography-based security method to deploy the encryption approach in SDN. Improving the encryption and decryption features of an existing method, allowing for high security. In a series of studies, we examined the MLTSAD and DLTSAD algorithms in order to increase network performance in terms of metrics like energy consumption, packet delivery ratio, latency, and network longevity.

Keywords: SDN networks, Security, MLTSAD, DLTSAD, Latency, Network reliability

1) INTRODUCTION

Wireless Sensor Networks are frequently used in dangerous areas to monitor key characteristics like earthquakes, temperature, and floods. It's likely that the sensor node's battery won't be able to be recharged. Using a smart routing protocol to make the most of the battery resource can help to extend the life of the WSN. The use of Machine Learning (ML) methods to manage WSN resources is more helpful than using standard resource management techniques. To decrease the energy depletion caused by irregular paths, many machine learning techniques have been added into the WSN routing protocol to construct smart routes among the sensor nodes. WSNs are being divided into a number of clusters, each with one cluster head and numerous sensor nodes, to improve energy consumption [1]. Wireless sensor networks (WSNs) have gotten a lot of press because of its applications in environmental monitoring, security surveillance, health, and underground mining. WSNs, on the other hand, have a major drawback in that the sensor nodes are powered by restricted power sources. Furthermore, owing to the hostile nature of some environments, such as battlefields and impenetrable forests. As a result, one of the most difficult concerns in WSNs is energy conservation of sensor nodes in order to increase network longevity. As a result, much research has been conducted to reduce

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/E8AVS

the energy consumption of sensor nodes in order to ensure the long-term functioning of WSNs [2] [3].

The new intelligent networking architecture, Software Defined Networking (SDN), gives opportunity to overcome IoT concerns. The use of SDN may greatly simplify network design and administration. SDN's widespread popularity in the industry demonstrates that it can create a stronger connectivity throughout the IoT ecosystem. From a global network perspective, it facilitates the design and operation of network control logic. Aside from the aforementioned benefits, SDN paves the way for the entire network to save green energy: it can collect the entire network topology as well as information on each device's real-time traffic; it can also obtain information on users' requests via a convenient northbound API interface [4] [5]. Schriegel developed a software-defined industrial IoT architecture to solve the problem of complex protocol administration in industrial control systems [6].

Both symmetric and asymmetric encryption methods have their own set of benefits and drawbacks. At the tradeoff of performance and hardware cost, asymmetric algorithms give greater capability than symmetric algorithms. Symmetric encryption, on the other hand, is a cost-effective and efficient way to protect data without losing security, and it should be considered the best and most appropriate security solution for a wide range of applications. In some circumstances, using both symmetric and asymmetric encryption in combination may be the best option. Hybrid encryption tries to take use of both sorts of algorithm classes' advantages while avoiding their disadvantages [7]. We proposed a Reliable Machine Learning Trust in this work. MLTSAD addresses major SDN requirements such as energy efficiency, reliability, data aggregation, and attacker detection. MLTSAD is a routing approach that identifies routes that require the least amount of total energy for end-to-end packet traversal while simultaneously increasing malicious node detection. We provided a cryptography-based security solution for implementing encryption in SDN. Improving the encryption and decryption portions of the method, which are now in place and provide excellent security. In order to increase network performance in terms of metrics like energy consumption, packet delivery ratio, latency, and network lifespan, we tested the MLTSAD and DLTSAD algorithms in a range of scenarios.

2) RELATEDWORKS

Sean W. Pritchard et al. [8] because their paradigm integrates WSN and SDN, it is possible to modify solutions from both paradigms to incorporate SDWSN. The inherent problems, such as resource restrictions, are one of the most critical obstacles in creating security in the WSN. The majority of these problems are addressed by the SDN paradigm's centralization of control, which allows for WSN security solutions.

Swapna B. Sasi et al. [9] some of the security challenges in wireless sensor networks are discussed, as well as ways for overcoming them. While some of the strategies used traditional cryptographic methods, others used cryptography optimization techniques. These diverse optimization methods-based concepts have been presented in this study, together with their benefits and drawbacks. This review presents numerous viewpoints on various cryptographic

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/E8AVS

optimization approaches, concluding that keeping keys necessitates a large amount of storage and energy. As a result, in the future, a new symmetric mechanism for lowering key size will need to be devised. The energy consumption and delay produced by the execution time when employed in the context of a dynamic security architecture in a wireless sensor network is another topic of interest.

Marcelo da Silva Conterato et al. [10] we've seen an increase in energy-saving research in data centres over the previous decade. Environmental factors such as concerns about long-term issues such as heat and gas emissions that deplete the ozone layer. The majority of the initiatives are targeted at reducing server and cooling system energy usage. Network devices, on the other hand, account for a significant amount of overall Data Center energy consumption, which is sometimes disregarded in studies. Their network allows devices to switch to a lower energy consumption mode to minimize the network layer's total consumption. The results suggest that energy usage in the network layer may be reduced by up to 70%.

Moustafa A. Youssef et al. [11] While typical routing methods aim to reduce end-to-end delays and increase throughput, most energy-aware routing algorithms for wireless sensor networks aim to extend the network's life by reducing energy consumption at the expense of other performance measures. We present a novel energy-aware routing protocol that attempts to reduce energy usage while maintaining good end-to-end latency and throughput performance. A limited shortest-path method underpins the novel approach. The novel method is compared to various standard and energy-aware routing techniques. The findings reveal that the new method performs satisfactorily across all performance parameters and provides a performance balance between traditional and energy-aware routing techniques. The constraint value can be adjusted to meet various performance goals for various sensor network missions.

Suneel Miriyala et al. [12] MANETs are proven to be a feasible platform for social networking on a larger scale. To what extent can mobile users trust it while safeguarding their privacy. We offer two techniques to overcome the aforementioned difficulties in this research. We first describe a basic dual-key methodology based on entirely homomorphic encryption, followed by a more complex hybrid structure-based system with a double decryption mechanism and fully homomorphic encryption.

Abdallah Ouhab et al. [13] they've introduced a novel large-scale network routing model that's both efficient and effective. A customized version of the RPL protocol is used to send packets over their network. When compared to traditional approaches, this combined approach allows the network to preserve energy, which is a major problem in the WSN industry, while also ensuring greater performance in terms of particular evaluation elements.

3) PROPOSEDMETHOD

The SDN paradigm is a new network paradigm that has grown in popularity in recent years. SDN, in essence, allows the network to be controlled from a conceptually central location and simplifies control and management activities by abstracting data and control planes from one

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

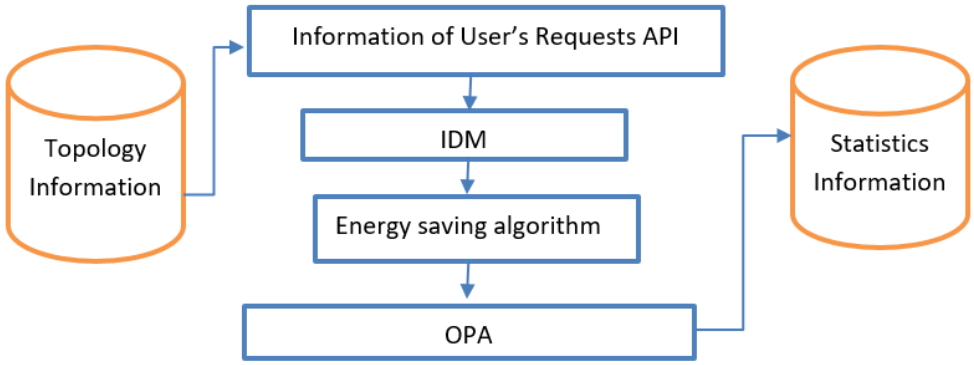
another. SDN was initially created for wired networks, but it has lately been adapted to other network designs such as data centres, clouds, and wireless networks.

As SDN networks expand, they become more vulnerable to assaults, necessitating the implementation of strong security systems. MLTSAD fulfils key SDN needs such as energy efficiency, dependability, data aggregation, and the identification of attackers. MLTSAD is an energy-efficient routing technique that finds routes that use the least amount of total energy for end-to-end packet traversal while also improving malicious node detection. To implement encryption in SDN, we presented a cryptography-based security method. Improving the algorithm's encryption and decryption elements, which currently exist and provide outstanding security. We examined MLTSAD and DLTSAD algorithms in a variety of scenarios to get which is better.

A. SDN

We construct energy-saving optimization algorithms in SDN using the third technique (SDNs). From a global network perspective, it facilitates the design and operation of network control logic.

Aside from the benefits described above, SDN lays the way for overall network green energy savings: it can gather the full network topology as well as information on real via the northbound API interface.



IDM: Intelligent Device Management; OPA: Open-flow Protocol Agent

Figure 1: SDN controller Energy Saving Components

It placed idle connections and line-cards to sleep after modifying the users' traffic to suitable pathways. And this can save a lot of electricity.

i. SDN Architecture

SDN is a new network paradigm that uses network programmability to simplify network control and administration. The fundamental idea behind SDN decoupling is that network devices make resource control decisions in a logically centralised way [16].

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

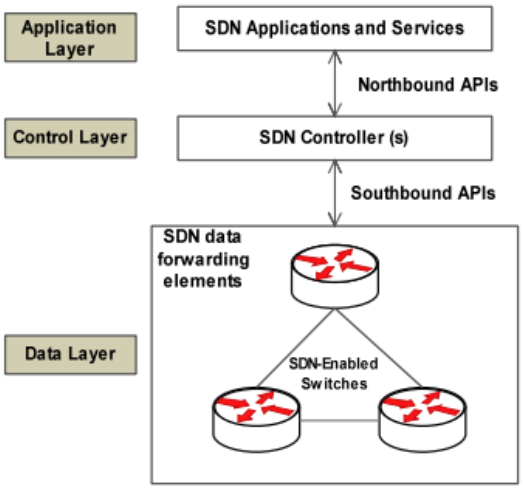


Figure 2: High-level view of SDN architecture

Since a result, network operations are more flexible as network administrators or users may control, programme, organise, and manage network resources directly.

A typical SDN design, as shown in Fig. 2, consists of three basic layers and two communication interfaces. A SDN layer is definition as follows:

Application layer: Other applications like Network virtualization, security monitoring and services that run on top of network infrastructure and consume network resources are all examples of application layers.

Data layer: The data layer contains the forwarding devices that are used for data forward in the SDN. The SDN enabled switch is used to implement the controller's management capability in this layer.

Control layer: The SDN controller is a conceptually centralised but physically dispersed component. The network's intelligence, programmability, and interactions between the data layer and the application are all managed by the controller. It provides programs with network-oriented high-level services while retaining strong connectivity.

Northbound SDN interface: The application programming interfaces (APIs) that are utilised to between application layers to control layer communication make up the majority of this interface. It adds the essential abstraction to the core network to allow for a more abstract perspective.

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

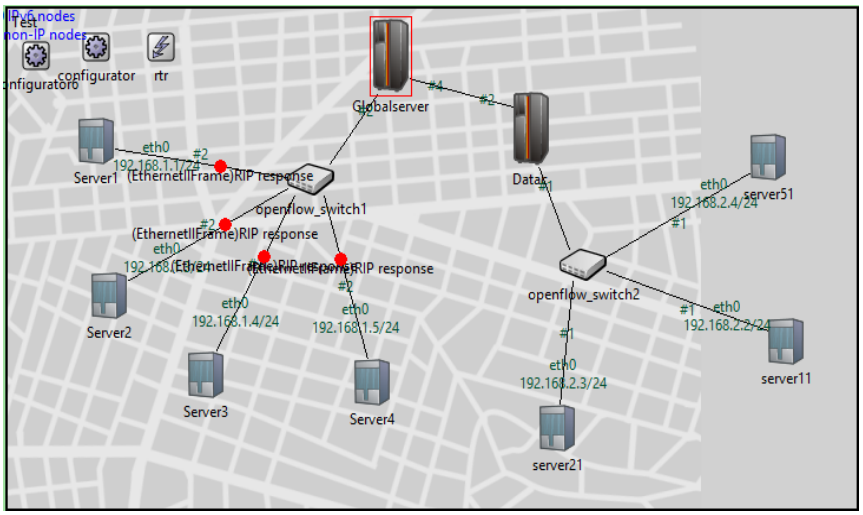


Figure 3: SDN Networks

Southbound interface: This interface is used to communicate from the control plane to the data plane. It implements the protocols necessary for successful network connectivity with a variety of devices...

B. Energy Consumption

One of the key difficulties to the effective implementation of WSNs is energy efficiency and balance, because sensor nodes are powered by finite batteries that cannot be readily refilled once installed. The remaining sensor nodes will lose a lot of energy since the network lifespan is typically defined as the time it takes for the first node to die due to a lack of energy [15].

Algorithm1. Algorithm for implementing energy-saving methods

Algorithm- Enery Saving
For all connect ∈connect devices
do
If maximum connection capacity = connection capacity
Then
Status of connection ← off
Endif
Endfor
For every changes ∈ change devices
Do
Connections used ← 0

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

```
If
Connection status = on
Then
Connections used= connections used+1
Endif
If
Connection status = on
Then
Status of connection ← off
Endif
Endfor
Capacity of connections ← [10, 100, 1k, 10k, 100k]
For all connect ∈connect devices
do
If maximum connection capacity = connection capacity
End for
```

The first algorithm covers the steps needed in putting energy-saving measures in place. The verification of links that lack mapped flows and, as a result, their disconnection are addressed in lines 2, 3, and 4. The switches are examined for active linkages between lines 7 and 15, and if none are found, the switch is turned off. Lines 18, 19, and 20 slow down the underutilised ports.

C. Cryptography

The majority of encryption methods must perform two purposes. The first purpose is key expansion, and the second is encryption and decryption using the extended key. The encryption process involves distributing and confounding plaintext characteristics in order to produce cipher texts; the decryption process involves returning cipher texts to plaintext.

Further down, we'll go through how to put these algorithms into practise.

i. Symmetric Cryptography: AES Algorithm

AES is a symmetric block cypher that can handle 128-bit data blocks and keys with lengths of 128, 192, and 256 bits.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/E8AVS

To encrypt a data input, four distinct transformations are done, as shown below (this is referred to as the cypher).

- Using a Substitution Table to Substitute Bytes (S-box).
- Modifying the row offsets in the state array.
- Data mixing inside the columns of the state array.
- Including a circular key in the state's design.

The encryption technique is shown in Fig. 4 as a block diagram.

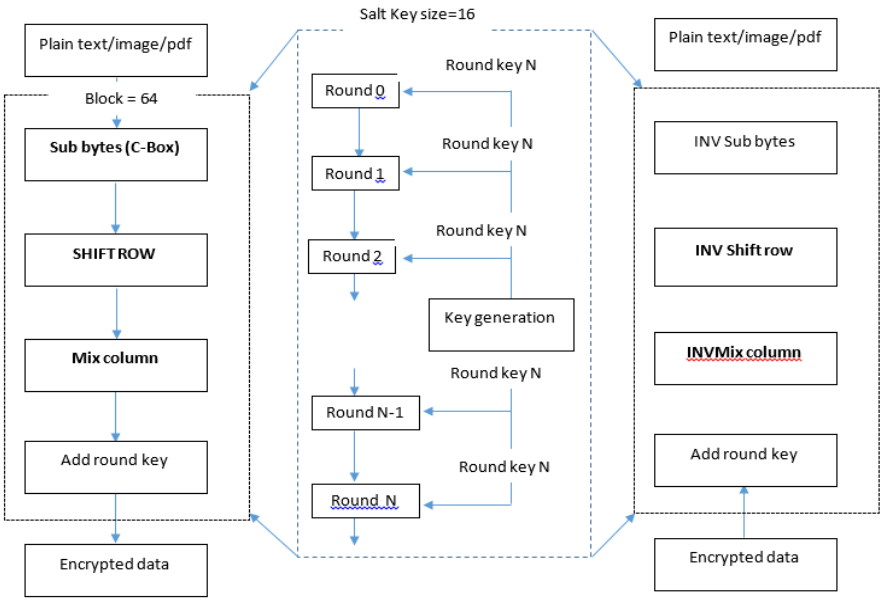


Figure 4: AES Cipher block diagram

The function that creates a key schedule from a given key is known as key expansion. The inverse cypher is then used to decipher the cipher text after all of the cypher changes are inverted in reverse order.

ii. Asymmetric Cryptography: RSA Algorithm

The RSA algorithm is named after its founders, and it was initially introduced in 1978. It is one of the most extensively used varieties of PKC. It uses both a PKC and digital signatures in addition to a PKC.

By combining two prime numbers, the technique yields a large prime number, which is then utilised to encrypt and decode a message. Huge mathematical functions and several multiplications are necessary to build a strong key and encryption system, which is why the RSA approach has hitherto been too resource expensive to implement inside MLTSAD.

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

D. Results

1. Throughput Ratio

Encryption time is used to calculate an encryption scheme's throughput. It denotes the encryption speed. The encryption scheme's throughput is estimated as follows:

$$\text{Throughput of encryption} = \text{Tp (Bytes)} / \text{Et (Second)} \quad (1)$$

The total plain text (in bytes) is Tp, while the encryption time is Et (second). For various plain text sizes, Figure5 compares the throughput of the proposed MLTSAD to that of the DLTSAD. It is shown that the recommended procedure and the (Zhu) protocol generate identical results and yield the greatest values.

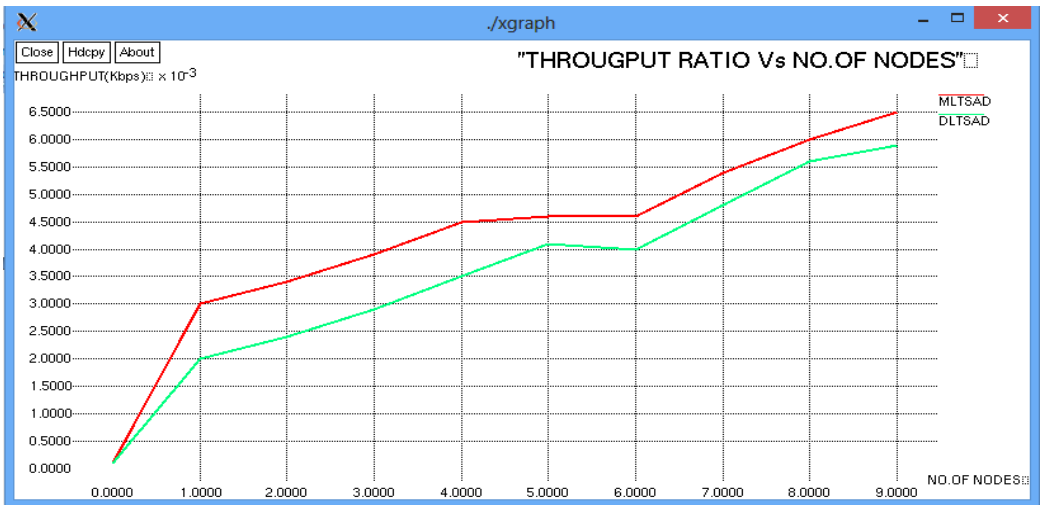


Figure 5: Throughput Ratio

2. Packet Delivery Ratio

When malicious switches are present in a network, the Packet Delivery Ratio (PDR) is one of the most important metrics to use to evaluate system performance. Figure 6 shows how packet delivery is gradually reducing or ceasing. The fundamental cause of this trend is that packet losses rise or increase when data packets choose different pathways owing to timeout.

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

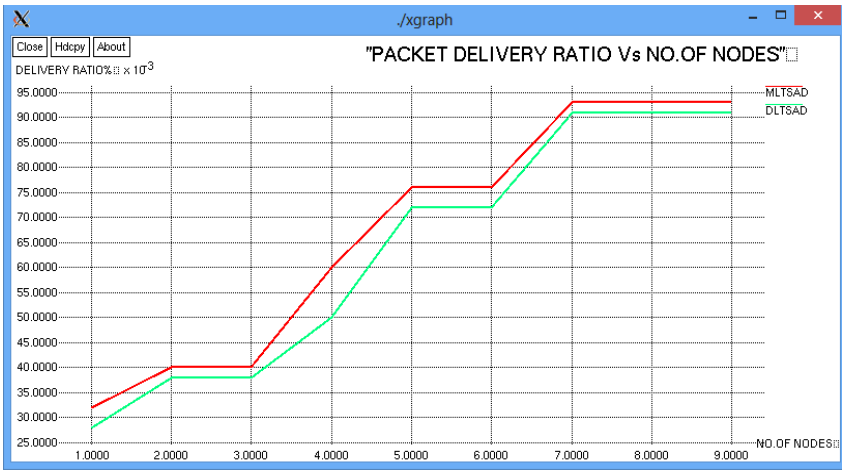


Figure 6: Packet Delivery Ratio (PDR)

3. Network Lifetime

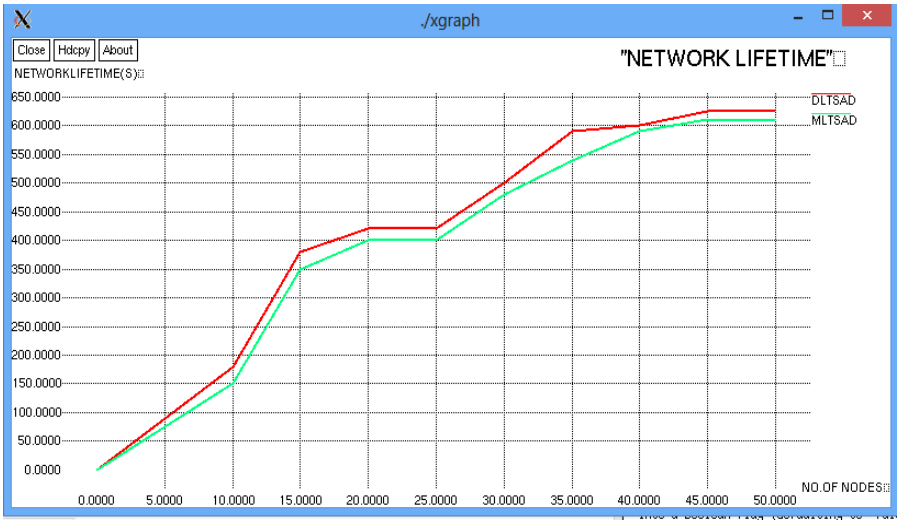


Figure 7: Network Lifetime

4. Energy consumption

Sensor energy usage varies significantly based on the communication protocols utilised by the sensors in an MLTSAD. One basic assumption is that sensors run on batteries, which are difficult to replace or recharge when there are hundreds of sensors in a network. Because power sources are limited, all processes, communication protocols, and networks must consume as little power as possible in order to maximise power lifetime.

ISSN 1533-9211

DOI 10.17605/OSF.IO/E8AVS

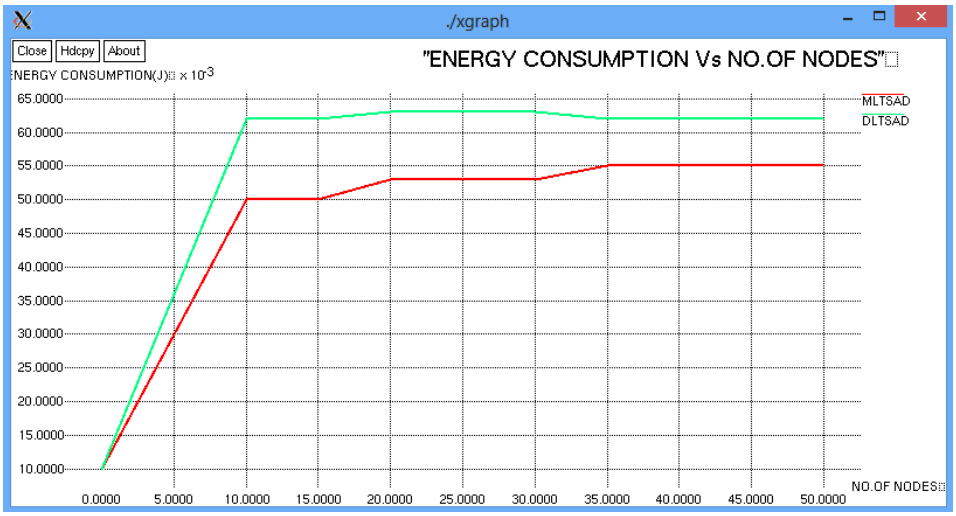


Figure 8: Energy consumption

5. Average End-to-End Delay

End-to-end latency is another significant measure to consider when assessing system performance, particularly if rogue switches are present in the network. The end-to-end latency rapidly increases in the presence of 20 switches, as seen in Figure 9. Because to timeouts, data packets are choosing alternate paths, costing more time.

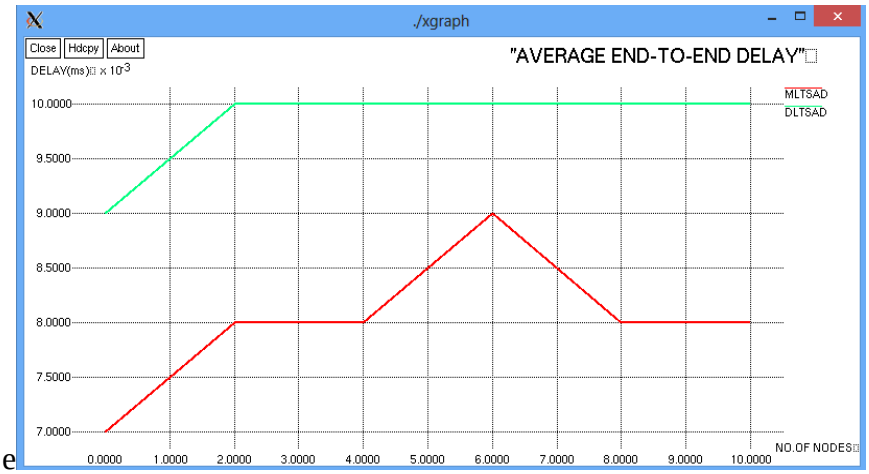


Figure 9: Average End-to-End Delay

Several benefits of this strategy include improving the network's lifespan and obtaining a greater degree of security. As a result of the lower overall energy usage, network performance is enhanced. The lifetime throughput and packet delivery ratio of a network may be significantly boosted with just a few adjustments. Message routing overhead and average end-to-end delay have been reduced. From above figures we can prove that the MLTSAD is better than DLTSAD.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/E8AVS

4) CONCLUSION

For effectively minimizing and balancing energy usage in SDN, we introduced the Machine Learning Trust Secure Attacker Detection (MLTSAD) method. MLTSAD is a method for finding routes that consume the least amount of energy overall for end-to-end packet traversal while also enhancing the identification of malicious nodes. We presented a cryptography-based security mechanism that can be used to create encryption in SDN. Enhancing the encryption and decryption components of the algorithm, which are already present and offer excellent security. In order to enhance network performance in terms of metrics like energy consumption, packet delivery ratio, latency, and network lifespan, we looked at MLTSAD and DLTSAD algorithms in a number of scenarios. We can infer from the results above that the MLTSAD is superior to the DLTSAD.

References

1. Khan, F., Memon, S., &Jokhio, S. H. (2016, November). Support vector machine based energy aware routing in wireless sensor networks. In 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI) (pp. 1-4). IEEE.
2. Amgoth, T., & Jana, P. K. (2015). Energy-aware routing algorithm for wireless sensor networks. Computers & Electrical Engineering, 41, 357-367.
3. Younis, M., Youssef, M., &Arisha, K. (2002, October). Energy-aware routing in cluster-based sensor networks. In Proceedings. 10th IEEE international symposium on modeling, analysis and simulation of computer and telecommunications systems (pp. 129-136). IEEE.
4. Wang, R., Jiang, Z., Gao, S., Yang, W., Xia, Y., & Zhu, M. (2014, June). Energy-aware routing algorithms in software-defined networks. In Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014 (pp. 1-6). IEEE.
5. Vandana, C. (2016). Security improvement in iot based on software defined networking (sdn). International Journal of Science, Engineering and Technology Research (IJSETR), 5(1), 2327-4662.
6. Ma, D., & Shi, Y. (2019, December). A lightweight encryption algorithm for edge networks in software-defined industrial Internet of Things. In 2019 IEEE 5th International Conference on Computer and Communications (ICCC) (pp. 1489-1493). IEEE.
7. Alkady, Y., Habib, M. I., &Rizk, R. Y. (2013, December). A new security protocol using hybrid cryptography algorithms. In 2013 9th International Computer Engineering Conference (ICENCO) (pp. 109-115). IEEE.
8. Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2018, June). Cryptography methods for software-defined wireless sensor networks. In 2018 IEEE 27th international symposium on industrial electronics (ISIE) (pp. 1257-1262). IEEE.
9. Sasi, S. B., &Sivanandam, N. (2015). A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology, 8(3), 216.
10. Conterato, M. D. S., Ferreto, T. C., Rossi, F., Marques, W. D. S., & de Souza, P. S. S. (2019, April). Reducing energy consumption in SDN-based data center networks through flow consolidation strategies. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (pp. 1384-1391).

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/E8AVS

11. Youssef, M. A., Younis, M. F., &Arisha, K. A. (2002, March). A constrained shortest-path energy-aware routing algorithm for wireless sensor networks. In 2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002 (Cat. No. 02TH8609) (Vol. 2, pp. 794-799). IEEE.
12. Miriyala, S., &Sairam, M. S. (2020). Improving privacy in SDN based MANET using hybrid encryption and decryption algorithm. Microprocessors and Microsystems, 103501.
13. Ouhab, A., Abreu, T., Slimani, H., &Mellouk, A. (2020, June). Energy-efficient clustering and routing algorithm for large-scale SDN-based IoT monitoring. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
14. Thangaramya, K., Kulothungan, K., Logambigai, R., Selvi, M., Ganapathy, S., & Kannan, A. (2019). Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. Computer Networks, 151, 211-223.
15. Cicioğlu, M., &Çalhan, A. (2020). Energy-efficient and SDN-enabled routing algorithm for wireless body area networks. Computer Communications, 160, 228-239.
16. Isong, B., Kgogo, T., Lugayizi, F., &Kankuzi, B. (2017, June). Trust establishment framework between SDN controller and applications. In 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD) (pp. 101-107). IEEE.