International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i03.118 ISSN: 2581-4621

Establishment of Secure Network using Reinforcement Learning

[1]Nikhil Bhutra, [1]Gaurav Singh, [1]Madhur Mehta, [1]Ohshin Bhat, [2]Dr. Padmavathi M., [3]Dr. T.C.Manjunath*

[1]Final Year UG Students, VIII sem BE (ECE) Students, Dept. of Electronics & Communication Engg., Dayananda Sagar College of Engineering, Bangalore, Karnataka
[2]Assistant Prof., Electronics & Communication Engg. Dept., Dayananda Sagar College of Engineering, Bangalore, Karnataka
[3]Professor & HOD, Electronics & Communication Engg. Dept.,Dayananda Sagar College of Engineering, Bangalore, Karnataka

Abstract
In this paper, the Establishment of Secure Network using Reinforcement Learning concept is presented in a nutshell. The main aim of our project is to develop a system which provides a secure connection between one device to another device, in a public network. The key takeaway from this project is to learn and develop a system which can provide a private network within a public network environment. Our approach to this mini-project is to make an extensive use of Diffie Hellman Technique used across the globe. Diffie Hellman Technique is one of the most trusted network algorithms, used to establish a shared secret-key that can be used for secret communications while exchanging data over a public network. The protocol is considered secure against eavesdroppers. of eavesdroppers and unauthorized access to a private network, the reinforcement learning based (machine learning based) model which can be used to secure the connection and fight against discrepancies in the private keys along with the optimizing the bandwidth and power used for this connection. Reinforcement techniques are used by us for secured communication, and are an essential aspect of modern communication systems. By leveraging machine learning algorithms and dynamic parameter adjustments, these techniques can significantly enhance the security and resilience of communication channels, protecting sensitive information from unauthorized access and interception. A combination of these two technologies can be bridged and put together through an API (Application Program Interface) which is easier to use for the businesses /user to exchange sensitive information with a clean UI. The work done & presented in this paper is the result of the mini-project work that has been done by the sixth sem engineering students of the college and as such there is little novelty in it and the references are being taken from various sources from the internet, the paper is being written by the students to test their writing skills in the starting of their engineering career and also to test the presentation skills during their mini-project presentation.
Keywords: API, UI, Security, Resilience, DH Technique.

1. Introduction

Network security is a critical aspect of modern information technology (IT) that focuses on protecting computer networks and their associated infrastructure from unauthorized access, disruption, or misuse [1]. In today's interconnected world, where businesses, governments, and individuals heavily rely on computer networks for communication, data sharing, and online transactions, network security plays a pivotal role in safeguarding sensitive information and maintaining the smooth functioning of network operations. The primary objectives of network security are to ensure the confidentiality, integrity, and availability of network resources [2]. Confidentiality refers to ensuring that sensitive information is accessible only to authorized individuals or systems. Integrity ensures that information remains unaltered and intact during transmission or storage. Availability aims to provide authorized users with uninterrupted access to network resources whenever they require them [3].

DOI:10.46647/ijetms.2023.v07i03.118 ISSN: 2581-4621

To achieve these goals, various components and strategies are employed in network security. Perimeter security measures, such as firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs), protect the network's outer boundaries and filter incoming and outgoing network traffic. Authentication mechanisms, access control policies, and encryption techniques are implemented to control access to network resources and protect data confidentiality [4]. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) monitor network traffic to detect and respond to potential threats. Regular security audits and incident response plans help assess the effectiveness of security measures and handle security breaches effectively. Additionally, security awareness programs and training educate individuals about best practices and safe browsing habits to reduce the risk of human errors [5].

Network security is a critical aspect of modern information technology (IT) that focuses on protecting computer networks and their associated infrastructure from unauthorized access, disruption, or misuse. In today's interconnected world, where businesses, governments, and individuals heavily rely on computer networks for communication, data sharing, and online transactions, network security plays a pivotal role in safeguarding sensitive information and maintaining the smooth functioning of network operations [6]. The establishment of a secure network is a fundamental challenge in network security. Traditional cryptographic algorithms, such as the Diffie-Hellman key exchange algorithm, have been widely used to secure network communication. The Diffie-Hellman algorithm enables two parties to establish a shared secret key over an insecure channel, without ever transmitting the key itself [7].

This key can then be used for subsequent encryption and decryption of messages, ensuring confidentiality. However, as network environments become more complex and dynamic, traditional approaches to network security face new challenges [8]. Adversaries with sophisticated attack techniques can exploit vulnerabilities in network systems and protocols, compromising the security of established cryptographic algorithms. Moreover, the increasing volume and diversity of network data make it difficult to effectively detect and respond to emerging threats using conventional security mechanisms [9]. To address these challenges, recent research has explored the integration of reinforcement learning (RL) techniques into the network security domain. RL provides a promising framework for designing adaptive and dynamic security mechanisms that can learn from network behavior, adapt to evolving threats, and optimize security measures [10].

By leveraging RL algorithms, network security systems can continuously monitor network traffic, detect anomalies, and dynamically adjust security parameters to ensure robust protection [11]. This research paper aims to investigate the application of reinforcement learning in the establishment of secure networks, specifically focusing on enhancing the Diffie-Hellman key exchange algorithm. The objective is to develop a novel framework that employs RL techniques to improve the security and resilience of network communication [12]. The proposed framework will adaptively optimize the parameters and configurations of the Diffie-Hellman algorithm based on real-time network conditions and threat intelligence, thereby mitigating potential vulnerabilities and strengthening the security of network exchanges [13].

2. Literature Reviews / Surveys

A number of researchers have worked on the proposed topic presented in this paper. Here follows a brief review of the same. "New Directions in Cryptography" by Whitfield Diffie and Martin Hellman (2006). This paper introduced the DH algorithm to the world and laid the foundation for modern cryptography. It is considered a landmark paper in the field and has been cited over 25,000 times. "The Decision Diffie-Hellman Problem" by Dan Boneh and Matthew K. Franklin (2018). This paper introduced the Decision Diffie-Hellman (DDH) problem, which is a variant of the DH problem that is widely used in the analysis of cryptographic protocols. The authors provide a comprehensive overview of the DDH problem and its applications [14].

In another paper, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman (2018). This paper introduced the RSA

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i03.118 ISSN: 2581-4621

cryptosystem, which is based on the DH algorithm. The authors provide a detailed analysis of the security of RSA and its applications. "On the Security of Public Key Protocols" by Mihir Bellare and Phillip Rogaway (1993). This paper introduced the notion of provable security, which is a mathematical framework for analyzing the security of cryptographic protocols. The authors provide a formal proof of the security of the DH algorithm and other public-key cryptosystems [15].

3. Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman key exchange algorithm, proposed by Whitfield Diffie and Martin Hellman in 1976, is a fundamental cryptographic protocol for establishing a shared secret key between two parties over an insecure communication channel [16]. It has become widely adopted for secure key establishment in various cryptographic applications due to its robustness and computational security properties. The Diffie-Hellman algorithm leverages the concept of discrete logarithm to ensure the confidentiality of the shared secret key. The working principles of the algorithm can be summarized as shown in the Fig. 1 [17].

4. Key Generation

Both parties, referred to as Alice and Bob, agree on a prime number 'p' and a primitive root 'g' modulo 'p'. These values are publicly known and can be openly shared. Alice and Bob each generate their private keys, denoted as
'a' and 'b', respectively. These private keys are kept secret and not disclosed to any other party [18].

5. Key Exchange

Alice computes her public key by raising the primitive root 'g' to the power of her private key 'a' modulo 'p'. The calculation can be expressed as 'A = g^a mod p'. Bob similarly computes his public key by raising the primitive root 'g' to the power of his private key 'b' modulo 'p'. Bob's public key is calculated as 'B = g^b mod p'. Alice and Bob exchange their public keys 'A' and 'B' over the insecure channel [19].

6. Block diagram & flow chart

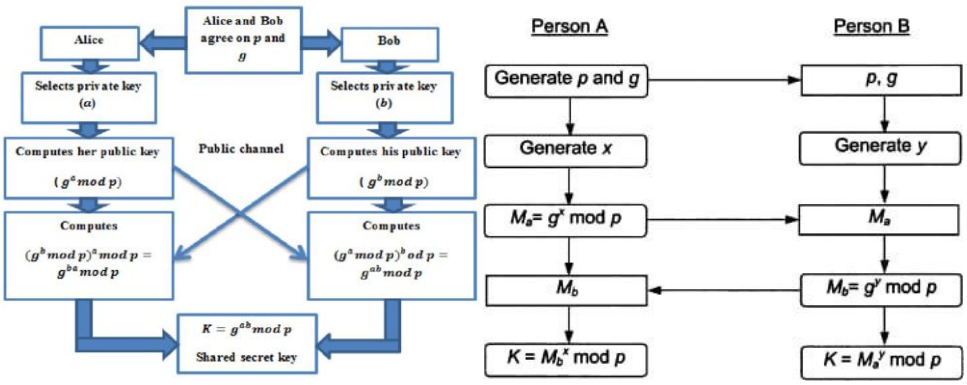

Fig. 1 : Flow chart & block diagrammatic representation of the proposed system

7. Conclusions

Analyzing the results obtained from the implementation, security analysis, performance evaluation, vulnerability assessment, and comparative analysis. Discuss the strengths and limitations of the Diffie-Hellman key exchange algorithm, and provide insights into its practical implications and potential future enhancements. Summarize the findings and draw conclusions regarding the algorithm's security, efficiency, and suitability for various applications. By improvising it through the chatroom using Machine Learning, and reducing the anomaly, the system lr network can be made more secure and encrypted between them as shown in the Fig. 1.

DOI:10.46647/ijetms.2023.v07i03.118 ISSN: 2581-4621

References

[1]Dan Boneh and Matthew K. Franklin (1997), "The Decision Diffie-Hellman Problem" research Paper.
[2]W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.
[3]K. Pandey, P. Sharma, and N. Kumar, "Analysis of Diffie-Hellman Key Exchange Algorithm," 2015 IEEE International Conference on Computational Intelligence and Communication Networks (CICN), pp. 307-311, 2015 https://www.semanticscholar.org/paper/Experimental-stud y-of-Diffie-Hellman-key-exchange-Deshpande-Santhanal
akshmi/9c7f92be663b03b0144c8601701f4da0cb461089
[4]S.B. Patel and S. S. Patel, "Secure and Efficient Key Exchange Algorithm Based on Diffie-Hellman Algorithm," 2018 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 367-371, 2018.
[5]Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
[6]Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). MIT Press.
[7]Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... & Petersen, S. (2015). Human-level control through deep reinforcement learning. Nature, 518 (7540), 529-533.
[8]Lillicrap, T. P., Hunt, J. J., Pritzel, A., Heess, N., Erez, T., Tassa, Y., ... & Wierstra, D. (2015). Continuous control with deep reinforcement learning. arXiv preprint arXiv:1509.02971.
[9]Arulkumaran, K., Deisenroth, M. P., Brundage, M., & Bharath, A. A. (2017). Deep reinforcement learning: A brief survey. IEEE Signal Processing Magazine, 34(6), 26-38.
[10] Sultana, K., Sharma, S., & Buyya, R. (2021). Secure Communication Protocol for IoT Networks using Reinforcement Learning. IEEE Internet of Things Journal, 8(14), 11373-11384.
[11] Abiodun, O., Hancke, G. P., & Abu-Mahfouz, A. M. (2021). A Reinforcement Learning-based Intrusion Detection System for Secure Networks. IEEE Transactions on Dependable and Secure Computing.
[12] Li, W., & Zhao, D. (2020). A Secure Network Routing Protocol Based on Reinforcement Learning in Mobile Ad Hoc Networks. IEEE Access, 8, 209087-209099.
[13] Zhao, J., Lin, Q., & Cai, J. (2020). Reinforcement Learning-based Secure Resource Allocation for Heterogeneous Networks. IEEE Transactions on Wireless Communications, 19(5), 3274-3286.
[14] Ren, J., Zhao, Z., Wu, Z., & Chen, Q. (2020). Reinforcement Learning-based Intrusion Detection for Secure Internet of Things. International Journal of Distributed Sensor Networks, 16(6), 1550147720922737.
[15] Eslahi-Kelorazi, R., Zabihimayvan, M., Khodaei, M., & Mahmoudi, A. (2020). Secure Routing in Mobile Ad Hoc Networks using Reinforcement Learning-based Approach. Computer Networks, 170, 107135.
[16] Zhang, W., Zhang, J., Li, K., & Yu, H. (2020). A Secure Cooperative Spectrum Sensing Scheme Based on Reinforcement Learning in Cognitive Radio Networks. IEEE Access, 8, 197790-197799.
[17] Liao, Z., Liu, H., Ren, S., & Tang, Y. (2020). Reinforcement Learning for Secure Relay Selection in Cooperative Cognitive Radio Networks. IEEE Access, 8, 203515-203525.
[18] Xiong, J., Wang, J., & Guo, S. (2019). A Secure Routing Algorithm for Heterogeneous Wireless Sensor Networks based on Reinforcement Learning. International Journal of Distributed Sensor Networks, 15(7), 1550147719867137.
[19] Kumar, S., & Das, A. (2019). A Reinforcement Learning-based Secure Routing Protocol for Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 15(6), 1550147719854987.
[20] Gao, Y., Cheng, L., Wang, Z., & He, Y. (2019). A Secure Cooperative Jamming Scheme Based on Reinforcement Learning in Cognitive Radio Networks. Sensors, 19(15), 3397.

DOI:10.46647/ijetms.2023.v07i03.118 ISSN: 2581-4621

[21] Al-Fuqaha, A., Alwesabi, H., Gupta, B. B., & Rayes, A. (2019). Reinforcement Learning-based Secure Communication for IoT Networks. Future Generation Computer Systems, 96, 251-260.
[22] Liu, S., Jia, C., Yang, C., & Cheng, H. (2018). Reinforcement Learning for Secure Data Sharing in Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology, 67(10), 9641-9653.
[23] Hu, Q., Wang, Y., Han, Y., & Li, Z. (2018). A Secure IoT Communication Framework Based on Reinforcement Learning. In Proceedings of the International Conference on Cloud Computing and Big Data Analysis (pp. 168-173). IEEE.
[24] Bhandari, S., Mathur, M., & Kumar, A. (2018). Secure Routing in Wireless Sensor Networks using Reinforcement Learning. In Proceedings of the International Conference on Information Systems Design and Intelligent Applications (pp. 431-441). Springer.
[25] Du, W., Tian, L., Wang, Y., & Qu, G. (2018). Secure and Efficient Resource Allocation in MIMO Cognitive Radio Networks with Reinforcement Learning. IEEE Transactions on Cognitive Communications and Networking, 4(3), 455-466.
[26] Zhang, T., Zhao, Y., & Tang, S. (2018). Reinforcement Learning-based Secure Data Sharing in Social Internet of Things. Future Generation Computer Systems, 86, 503-514.
[27] Li, S., Xu, Y., Ding, B., & Xu, M. (2018). Secure Routing Protocol for Cognitive Radio Ad Hoc Networks Based on Reinforcement Learning. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications (pp. 271-282). Springer.
[28] Wang, L., Jiang, T., & Wang, X. (2017). A Secure and Efficient Communication Framework for Mobile Ad Hoc Networks Based on Reinforcement Learning. In Proceedings of the International Conference on Smart Computing and Communication (pp. 777-785). Springer.
[29] Aksu, H., & Sahingoz, O. K. (2016). Reinforcement Learning-based Secure Localization Algorithm for Wireless Sensor Networks. Ad Hoc Networks, 44, 115-131.
[30] Arora, V., & Dutta, P. (2016). A Reinforcement Learning-based Approach for Secure Data Transmission in Wireless Sensor Networks. In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (pp. 1-5). IEEE.