International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Novel Distributed Mac Security Implementation in Switching Networks Using BMP-MACSEC and BP-SKEIN

Amaresan Venkatesan

v.amaresan@gmail.com

Abstract:
Distributed MAC security is implemented in SN to collectively protect the data at the MAC layer. However, the existing studies didn't concentrate on the MAC address flooding attacks and MAC table overflow in SN. Therefore, this paper presents distributed MAC security implementation in SN using BMP-MACSEC and BP-Skein. Primarily, users register in the network; afterward, data transmission is initiated. Blockchain-based MAC address maintenance is created for each port by using the BP-Skein. Then, switches are clustered by employing DB-DBSCAN. Next, data is transmitted through the clustered switches. At this point, the MAC address details of the transmitted data are hashed and verified. If both MACs are matched, then the data is transmitted to the corresponding port. Next, MAC security is done by employing BMP-MACSEC. Then, the obtained symmetric key is split and reconstructed by employing NI-SSS. Likewise, the split key with the data packet is subjected to IDS for attack detection. If attacked, then the access is denied; otherwise, key verification is done. If verified, then the data is accessed; otherwise, it is blocked. The results proved that the proposed model achieved a high-security level of 98.68%, thus outperforming the prevailing techniques.

Keywords: Baker's Map Playfair Media Access Control Security (BMP-MACSEC), Intrusion Detection System (IDS), Switching Network (SN), Newton InterpolationShamir's Secret Sharing (NI-SSS),Bit Permutation–Skein (BP-Skein), Variational Dropout Cauchy Linear UnitRecurrent Neural Networks (VDCLU-RNN), Media Access Control (MAC), and Davies-Bouldin Density-Based Spatial Clustering of Applications with Noise (DB-DBSCAN).

1. INTRODUCTION

Generally, SNs are communication networks that employ switches to connect devices and handle the flow of data (Fathurrahmad et al., 2020). Actually, SN transmits data from source to destination through switching nodes. In SN, each data from a network connection can take distinct routes to reach the destination (Groma et al., 2019) (Bhola et al., 2019). Likewise, MAC protocol is important for SN to support transmission with high security (Sahoo et al., 2019). Still, SN is prone to network traffic and burst duplication attacks (Kesar & Sandhu, 2019). Therefore, many techniques are developed to identify malicious behaviors and secure the SNs.

In prevailing studies, DT and Random Forest (RF) algorithms are used for identifying network intrusions (Alzahrani&Alenazi, 2021). Also, a Deep Neural Network (DNN) and Convolutional Neural Network (CNN) are employed for network traffic analysis during data transmission (Krupski et al.,

2021) (Farhana et al., 2020). Additionally, MAC address filtering authentication methods and route tracing algorithms are used to provide MAC security (Jouma Ali AlMohamad, 2021) (Anathi& Vijayakumar, 2020). However, the prevailing works didn't focus on the MAC address flooding attacks and MAC table overflow in SN. Therefore, distributed MAC security implementation in SN using BMP-MACSEC and BP-Skein is proposed.

1.1 Problem Statement

qNone of the conventional works focused on MAC address flooding attacks and MAC table overflow in SN.

qIn prevailing (Liu et al., 2021), the same key was shared between parties, thus ensuring whether the keys were securely distributed or not was challenging.

qThe existing (Fan et al., 2021) did not analyze network traffic for signs of malicious behavior.

qDue to the complex topologies, misconfigurations and inconsistencies occurred in the network.

1.2 Objective

ÄBP-Skein is introduced to perform Blockchain-based MAC address maintenance and MAC address aging-based MAC table overflow reduction in SN.

ÄBMP-MACSEC is employed for MAC security.

ÄIDS are established, where the VDCLU-RNN classifier is used to identify malicious behaviors.

ÄDB-DBSCAN is utilized for clustering the switches to avoid complex topologies.

The paper is organized as: Section 2 illustrates the literature survey, Section 3 describes the proposed methodology, Section 4 conveys the result, and Section 5 concludes the proposed model with future work.

2. LITERATURE SURVEY

(Liu et al., 2021) introduced a Burst Header Packet (BHP) flooding attacks identification model in SN. Here, a particle swarm optimization-support vector machine technique was employed to identify the BHP flooding attacks. The research effectively maintained network security. Moreover, the same key was shared between parties, thus ensuring secure distribution of keys was challenging.

(Fan et al., 2021) presented a cross-network-slice authentication scheme for SN. Here, a secure session key exchange protocol was employed for authentication. Also, the research was secured against intruders. Furthermore, the model didn't analyze network traffic for signs of malicious behavior.

(Almaslukh, 2020) explored a flooding attack identification framework in optical burst switching networks. Here, the flooding attack detection was performed by utilizing the Decision Tree (DT) classifier. The research effectively solved the overfitting issues. But, misconfigurations occurred in the network owing to the complex topologies.

(Mebawondu et al., 2020) explained a supervised learning paradigm-based network IDS. In this research, a lightweight IDS based on information gain and a multi-layer perceptron neural network was utilized to detect malicious behaviors. The works proficiently classified the attack and normal traffic. Yet, the model failed to secure the data packets during the transmission.

(Adil et al., 2020) described a MAC- Ad-hoc On-demand Distance Vector (AODV)-based mutual authentication scheme in constraint-oriented networks. Here, an elliptical curve integrated encryption standard was used to authenticate the data. The research provided improved authenticity. Yet, the improperly selected curves might compromise the encryption's security.

3. PROPOSED DISTRIBUTED MAC SECURITY IMPLEMENTATION IN SN FRAMEWORK

Here, the BMP-MACSEC is introduced for MAC security. The structural representation of the proposed model is displayed in Figure 1.

Figure 1: Structural representation of the proposed model

3.1 Network User Registration

Initially, the network users register in the network by using their username and password. Thus, the registered network users are defined as,(1) Where, specifies the number of . After registration, the data is transmitted through the switches to the corresponding port.

3.2 Blockchain-based MAC Address Maintenance and MAC Address Aging-based MAC Table Overflow Reduction

Blockchain-based MAC address maintenance is created for each port. Here, the details of the port, including maximum MAC address, sticky MAC address, static MAC address, MAC address aging, and port security aging are maintained in the blockchain to avoid MAC address flooding attacks. Among that, the MAC address aging is considered to reduce MAC table overflow, where the inactive MAC addresses from the MAC address table are removed after a particular period of inactivity. The port details are given as,(1)

Where, signifies the number of . Also, based on BP-Skein, the maintained port details are hashed and stored in the blockchain. Generally, the Skein hash function is fast, secure, and resistant to traditional attacks. However, Skein has possibilities of pseudo-collision owing to the usage of fixed-length message value. Therefore, the Bit Permutation technique is used. Initially, the is padded and then divided into blocks.(2)

Where, is the number of divided message blocks. Then, each is processed utilizing the Unique Block Iteration (UBI) mode with Threefish.(3)

Where, implies the UBI function, and and denote the current state and previous state of the hash, respectively. Likewise, the UBI function is equated as,(4)

Here, indicates the Threefish operation and demonstrates the tweak value. Eventually, the final hash value is generated by transforming the final state . Here, the bit permutation technique is included and is formulated as,(5)

Where, represents the finalization tweak, defines the rotation, signifies the XOR operation, and implies the addition. Thus, the hashed port details are represented as.(6)

3.3 Clustering

Then, the switches are clustered by using DB-DBSCAN based on maximum linkage. DBSCAN effectively identifies the clusters based on the density of points. But, the same epsilon and minPts values didn't work well across clusters with varying densities. To address this problem, the Davies-Bouldin Index is employed.

Firstly, the Davies-Bouldin Index is used to compute the epsilon parameter that evaluates the average similarity ratio of each cluster with its most similar cluster.

Where, defines the average distance between points in cluster , signifies the average distance between points in cluster , is the number of , and depicts the distance between the centroids of clusters and . Then, the clusters are formed by minPts as follows,(7)

Where, depicts the number of dimensions. Afterward, the core point that helps in identifying the clustering is estimated as(8)

Thus, based on the , , and , the switches are clustered according to the minimum linkage. This clustering

is continued until convergence. The clustered switches are indicated as.(9)

3.4 Hash Verification

Then, the data is transmitted through the clustered switches and is given as,(10)

Where, signifies the number of data to be transmitted. At this point, the MAC address details of are hashed by employing BP-Skein, which are indicated as . Then, the hash verification is done.(11)If both hashed MAC addresses are matched, then only is transmitted to the corresponding port; otherwise, it is blocked.

3.5 MAC Security

Subsequently, the MAC security is performed for by using BMP-MACSEC. MACSEC enhances the security of data transmitted across the network. If the authentication key is compromised, all communications protected by that key are at risk. So, the key is created by using Baker's map, and the Playfair cipher technique is used for ciphering.

At first, the MACsec Key Agreement Protocol (MKA) policy is created. Then, the key is generated by using the Baker's map.(12) Where, and specify the coordinates. Then, the is ciphered by using the Playfair cipher technique.(13) Here, and specify the positions in the key square and depicts the constant value. Then, the encryption is performed as,(14) Where, is the decrypted data and demonstrates the encryption function. Next, the decryption is done to decrypt the encrypted data.(15) Where, depicts the decrypted data and is the decryption function. Then, the obtained symmetric ciphered key is split and reconstructed in the blockchain.

3.6 Key Splitting and Reconstruction in Blockchain

Thereafter, the is split and reconstructed by employing the NI-SSS. Shamir's Secret Sharing (SSS) can easily split and reconstruct the key without exposing the original secret. However, SSS has polynomial interpolation, which is computationally intensive for large secrets. Therefore, Newton interpolation is used in SSS.

Primarily, the is divided into number of shares. Then, a prime number is chosen, which is larger than . Next, the Newton interpolation is constructed instead of polynomial interpolation to avoid computational complexity (16) Afterward, the Newton interpolation is evaluated at distinct non-zero values to generate the shares. Then, the shares are distributed. Lastly, the key is reconstructed by using the Lagrange interpolation.(17) Where, indicates the index of the share, defines the value of the share, is the Lagrange factor, and defines the degree. Then, the obtained reconstructed key is stored in the blockchain; also, the obtained split key and are subjected to IDS.

3.7 IDS

Next, and are fed to the IDS; here, the IDS is trained by the following processes.

3.7.1 Data Acquisition

Here, the CIC-IDS2017 dataset is collected from publicly available sources and is defined as .

3.7.2 Pre-Processing

Next, the is preprocessed to improve the quality of the data. Firstly, the missing values of are imputed by the mean value of the non-missing data and are indicated as . Then, one-hot encoding that converts into binary (0 and 1) representation is done and is expressed as . The pre-processed data is represented as] .

3.7.3 Feature Extraction and Selection

Afterward, the features, such as Destination Port, Flow Duration, Fwd Packet Length Std, Bwd Packet

Length Max, and Flow IAT Mean, are extracted from the . Thus, the extracted features are represented as . Then, optimal features are selected from the and are signified as .

3.7.4 Attack Detection

Then, from the , the attack detection is performed by utilizing VDCLU-RNN. RNNs effectively capture the temporal patterns and dependencies in network traffic. But, Recurrent Neural Networks (RNNs) have a vanishing gradient problem. Therefore, variational dropout regularization and the Cauchy linear unit activation function are employed in RNN. The VDCLU-RNN classifier is displayed in Figure 2.

Figure 2: VDCLU-RNN classifier

Firstly, the input layer gathers as an input. Then, is fed to the hidden state for the remaining process. Afterward, the hidden state is updated regarding the current input and the previous hidden state. The hidden state is determined by,(18)

Where, specifies the bias value, is the variational dropout regularization-based weights, and denotes the Cauchy linear unit activation function. Here, is given as,(19)

Here, specifies the expectation over the dropout masks , is the probability, denotes the observed data, signifies the Kullback-Leibler divergence between a variational distribution and prior distribution , and represents the dropout-modified weights. Similarly, is equated as,(20)

Where, is the positive constant. Afterward, the output layer decides the information, which is needed to be presented as an outcome.(21)

Eventually, the attack detection outcomes are represented as,(22)

Where, denotes the attacked data and demonstrates the non-attacked data.

Pseudocode for VDCLU-RNN

Input: Selected features
Output: Attack detection outcomes
Begin
Initialize,
For
Perform input layer
Estimate hidden state
Discover
Determine
Evaluate
End For
Obtain
End

In the testing time, if the data is attacked, then access is denied; otherwise, the is decrypted at the receiver side to access the data.

3.8 Key Verification

Before decrypting the data, the is verified with the in the blockchain. If both keys are equal, then the data is decrypted and accessed; otherwise, access is denied.

4. RESULT AND DISCUSSION

Here, the performance analysis is done to prove the proposed model's trustworthiness, and the proposed model is implemented in the working platform of PYTHON.

4.1 Dataset Description

The CIC-IDS2017 dataset is employed to assess the proposed model. This dataset is collected from publicly available sources and the reference link is mentioned under the reference section. Here, the dataset comprises 632 number of data. Among that, 80% of the data is used for training and the remaining 20% of data is employed for testing.

4.2 Performance Assessment

Here, the proposed model is compared with prevailing techniques to prove the model's reliability.

Figure 3: Graphical analysis based on performance metrics

Figure 3 depicts the graphical analysis regarding key generation time, encryption time, and decryption time. Here, the proposed BMP-MACSEC obtained a low key generation time, encryption time, and decryption time of 253ms, 1137ms, and 1273ms, respectively. But, the prevailing techniques like MACSEC, Rivest, Shamir, Adleman (RSA), Data Encryption Standard (DES), and ElGamal obtained high-performance metrics. The proposed BMP-MACSEC provided enhanced security due to the usage of Baker's map and Playfair cipher technique.

Table 1: Security level analysis

Method	Security Level (%)
Proposed BMP-MACSEC	98.68
MACSEC	95.57
RSA	92.13
DES	89.63
ElGamal	88.57

Security level analysis of the proposed and existing techniques is displayed in Table 1. Here, the proposed BMP-MACSEC obtained a high-security level of 98.68%. But, the existing techniques attained a low average security level of 91.47%. Thus, the high-security level of the proposed model is proved.

Figure 4: Performance Validation

Figure 4 shows performance validation regarding hashcode creation and hashcode verification time. Here, the proposed BP-Skein achieved a low hashcode creation and hashcode verification time with the help of the Bit Permutation Technique. Likewise, the prevailing techniques like Skein, whirlpool, Secure Hash Algorithm-512 (SHA512), and Message Digest-5 (MD-5) attained high hashcode creation and hashcode verification time.

Figure 5: Comparative estimation of the proposed model and prevailing techniques

A comparative estimation of the proposed and prevailing techniques is shown in Figure 5. Here, the proposed VDCLU-RNN achieved a high precision, recall, F-measure, accuracy, sensitivity, and specificity of 98.75%, 98.89%, 99.01%, 98.42%, 98.89%, and 98.12%, correspondingly. But, the prevailing RNN, Deep Belief Network (DBN), DNN, and Artificial Neural Network (ANN) obtained low performance metrics. Here, variational dropout regularization is modified with RNN for effective attack detection.

Figure 6: Graphical representation regarding (a) clustering time and (b) silhouette score

Figure 6 depicts the graphical representation regarding clustering time and silhouette score. Here, the proposed DB-DBSCAN obtained a low clustering time of 17358ms and a high silhouette score of 0.91253. But, conventional techniques like DBSCAN, Fuzzy C-Means (FCM), K-Means, and Clustering Large Applications (CLARA) obtained high clustering time and low silhouette scores.

Table 2: Entropy estimation

Techniques	Entropy
Proposed NI-SSS	32.89
SSS	29.56
BSS	26.23
VSS	19.87
ASS	14.23

The entropy estimation of the proposed and conventional methods is displayed in Table 2. Here, the proposed NI-SSS achieved a high entropy of 32.89, whereas the conventional SSS, Blakley's Secret Sharing (BSS), Verifiable Secret Sharing (VSS), and Additive Secret Sharing (ASS) attained low mean entropy of 22.47.

4.3 Comparative Analysis

The comparative analysis is done to demonstrate the proposed model's effectiveness.

Table 3: Comparative analysis

Author's name	Objective	Methodology	Advantages	Downsides
Proposed model	Distributed MAC security implementation in SN	BMP-MACSEC	Provided enhanced MAC security in SN	However, more energy was wasted during the data transmission in SN.
(Sarang et al., 2020)	Quality of Service (QoS) MAC protocol for Wireless Sensor Networks (WSN)	Asynchronous QoS-MAC (AQSen-MAC)	Improved the packet delivery ratio	But, the research had high complexity.
(Girdler &Vassilakis, 2021)	Defending against blacklisted MAC addresses	Software Defined Networking (SDN) based Intrusion Detection and Prevention System (IDPS)	Proficiently protected against network intrusions	Due to the single network segment, the packet transition was hard to detect.
(Bairwa & Joshi, 2021)	Mutual authentication of nodes	SHA	Improved the reliability and security of the network	Yet, it failed to provide security to the users of the node.
(Singh et al., 2019)	Authentication scheme for WSN	MAC	Preserved key secrecy and confidentiality	Furthermore, the model had scalability issues.
(Armknecht et al., 2020)	Continuous authentication of message streams	Progressive MACs (ProMACs)	Increased the security of subsequent messages	But, it had high computational overhead.

Table 3 depicts the comparative analysis of the proposed model and related works. Here, the proposed model provided enhanced MAC security in SN by using BMP-MACSEC. However, the related works had high complexity, computational overhead, and scalability issues. Therefore, the proposed research is better than the existing models.

5. CONCLUSION

This paper presented distributed MAC security implementation in SN using BMP-MACSEC. Here, the CIC-IDS2017 dataset was employed for IDS. The blockchain-based MAC address maintenance was created to avoid MAC address flooding attacks and MAC table overflow. Here, the proposed BMP-MACSEC provided a high-security level of 98.68%. Likewise, the proposed BP-Skein attained a low hash verification time of 3014ms. The proposed VDCLU-RNN obtained a high accuracy, precision, and recall of 98.42%, 98.75%, and 98.89%, respectively. Thus, the proposed model effectively improved the distributed MAC security in SN. However, more energy was wasted during the data transmission in SN.

Future work

In the future, advanced techniques will be developed to improve the energy efficiency of nodes in SN.

REFERENCES

Dataset link:https://www.unb.ca/cic/datasets/ids-2017.html

1. Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks. IEEE Access, 8, 44459–44469. https://doi.org/10.1109/ACCESS.2020.2978303
2. Almaslukh, B. (2020). An Efficient and Effective Approach for Flooding Attack Detection in Optical Burst Switching Networks. Security and Communication Networks, 2020, 1–11. https://doi.org/10.1155/2020/8840058
3. Alzahrani, A. O., &Alenazi, M. J. F. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5), 1–18. https://doi.org/10.3390/fi13050111
4. Anathi, M., & Vijayakumar, K. (2020). An intelligent approach for dynamic network traffic restriction using MAC address verification. Computer Communications, 154, 559–564. https://doi.org/10.1016/j.comcom.2020.02.021
5. Armknecht, F., Walther, P., Tsudik, G., Beck, M., &Strufe, T. (2020). ProMACs: Progressive and Resynchronizing MACs for Continuous Efficient Authentication of Message Streams. Proceedings of the ACM Conference on Computer and Communications Security, 211–223. https://doi.org/10.1145/3372297.3423349
6. Bairwa, A. K., & Joshi, S. (2021). Mutual authentication of nodes using session token with fingerprint and MAC address validation. Egyptian Informatics Journal, 22(4), 479–491. https://doi.org/10.1016/j.eij.2021.03.003
7. Bhola, J., Soni, S., & Kakarla, J. (2019). A scalable and energy-efficient MAC protocol for sensor and actor networks. International Journal of Communication Systems, 32(13), 1–16. https://doi.org/10.1002/dac.4057
8. Fan, C. I., Shih, Y. T., Huang, J. J., & Chiu, W. R. (2021). Cross-Network-Slice Authentication Scheme for the 5th Generation Mobile Communication System. IEEE Transactions on Network and Service Management, 18(1), 701–712. https://doi.org/10.1109/TNSM.2021.3052208

9. Farhana, K., Rahman, M., &Tofael Ahmed, M. (2020). An intrusion detection system for packet and flow based networks using deep neural network approach. International Journal of Electrical and Computer Engineering, 10(5), 5514–5525. https://doi.org/10.11591/IJECE.V10I5.PP5514-5525
10. Fathurrahmad, Yusuf, S., Iqbal, T., & Salam, A. (2020). Virtual private network (Vpn) network design for multiprotocol label switching (Mpls) networks. International Journal of Scientific and Technology Research, 9(1), 105–108.
11. Girdler, T., &Vassilakis, V. G. (2021). Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses. Computers and Electrical Engineering, 90(January 2021), 1–12. https://doi.org/10.1016/j.compeleceng.2021.106990
12. Groma, M., Boros, T., &Helebrandt, P. (2019). Scalable cache-based address resolution protocol handling in software-defined networks. ICAT 2019 - 27th International Conference on Information, Communication and Automation Technologies, Proceedings, 1–6. https://doi.org/10.1109/icat47117.2019.8938849
13. Jouma Ali AlMohamad, J. A. A. (2021). Build Encrypted Interconnection Networks by application of IP Security and Mac Address Filtering Authentication Methods. JurnalMantik, 5(3), 66–56. https://doi.org/10.26389/ajsrp.m280321
14. Kesar, P., & Sandhu, M. K. (2019). Security Issues and the Energy Consumption in the Optical Burst Switched Networks. International Journal of Trend in Scientific Research and Development, Volume-3(4), 881–885. https://doi.org/10.31142/ijtsrd23934
15. Krupski, J., Graniszewski, W., &Iwanowski, M. (2021). Data transformation schemes for cnn-based network traffic analysis: A survey. Electronics (Switzerland), 10(16), 1–35. https://doi.org/10.3390/electronics10162042
16. Liu, S., Liao, X., & Shi, H. (2021). A pso-svm for burst header packet flooding attacks detection in optical burst switching networks. Photonics, 8(12), 1–14. https://doi.org/10.3390/photonics8120555
17. Mebawondu, J. O., Alowolodu, O. D., Mebawondu, J. O., &Adetunmbi, A. O. (2020). Network intrusion detection system using supervised learning paradigm. Scientific African, 9, 1–11. https://doi.org/10.1016/j.sciaf.2020.e00497
18. Sahoo, P. K., Pattanaik, S. R., & Wu, S. L. (2019). A novel synchronous MAC protocol for wireless sensor networks with performance analysis. Sensors (Switzerland), 19(24), 1–25. https://doi.org/10.3390/s19245394
19. Sarang, S., Stojanović, G. M., Stankovski, S., Trpovski, Ž., &Drieberg, M. (2020). Energy-Efficient Asynchronous QoS MAC Protocol for Wireless Sensor Networks. Wireless Communications and Mobile Computing, 2020, 1–13. https://doi.org/10.1155/2020/8860371
20. Singh, D., Kumar, B., Singh, S., & Chand, S. (2019). SMAC-AS: MAC Based Secure Authentication Scheme for Wireless Sensor Network. Wireless Personal Communications, 107(2), 1289–1308. https://doi.org/10.1007/s11277-019-06336-8