A NOVEL INTEGRITY BASED MESH DATA ENCRYPTION AND DECRYPTION ALGORITHM FOR DYNAMIC WMNs

Dr. Marepalli Radha,
Associate Professor, CVR College of Engineering, Mangalpalli, Ibrahimpatnam, RR district, Telangana - 501510
marepalli.radha@gmail.com

Dr. Mulagundla Sridevi,
Associate Professor, CVR College of Engineering, Mangalpalli, Ibrahimpatnam, RR district, Telangana - 501510
sreetech99@gmail.com

Abstract:

Wireless mesh networks (WMNs) play a vital role in the dynamic network topology and group data communication for large complex networks. Due to the increase in data size and mesh clients in the dynamic WMNs, it is difficult to secure the communication data against the attacks. Also, traditional encryption algorithms are independent of mesh client authentication and data security due to large data size and changes in mesh node properties. To overcome these problems in the dynamic WMNs, an integrated mesh node authentication and data security framework is developed. This model is efficient on the large WMNs and provides strong data security during the mesh client authentication process. In this framework, a novel integrity-based encryption algorithm is designed and implemented on the mesh client data for strong security. Experimental results illustrate that the proposed security model is efficient than the traditional models in terms of data encryption runtime(ms), data storage space, and integrity sensitivity.

Keywords*: Wireless mesh networks, data security, integrity, attributes-based policies.*

1. Introduction

The wireless mesh network can be defined as a special group of mesh clients (MCs), mesh routers (MRs), and gateways. Again, a wireless mesh network can be said as a special multi-hop technology that has many similarities with mobile ad-hoc networks, but it is assumed as a perfect superset of mobile ad-hoc networks. Basically, wireless mesh networks contain mesh routers that are interconnected with each other. These mesh routers are connected to the internet through mesh gateways. Each connection of wireless mesh networks is wireless in nature. The mesh routers are also known as routing devices or access points. Mesh routers are stationary in nature, and these are responsible for building the backbone of the network. The mesh clients can be either mobile or stationary. Some examples of mesh clients are: - laptops, mobile phones, and various kinds of wireless devices. It has the prime objective to connect with the network. Another important feature of this wireless mesh network is to relay the information those are transmitted from different nodes. By this, the network coverage can be enhanced. Both above-mentioned nodes can be differentiated by two important characteristics, those are: - mobility and energy consumption constraints. Mesh clients have a restricted amount of energy than that mesh routers. Hence, all the functionalities that need a large amount of computational time, bandwidth, and memory are usually issues of mesh routers.

Mobility, flexibility, and very high robustness can be achieved with the help of wireless mesh networks. Apart from this, the network coverage can also be enhanced with high scalability. There are vast numbers of applications of wireless mesh networks in the field of healthcare, enterprise networking, security surveillance, and so on. There has been an extensive amount of research works carried out to ensure the security of wireless mesh networks. There are several different efficient approaches by implementing which many attacks can be identified. Below are the severe issues that are found in the above-mentioned research works.

1. Excessive packets are eliminated and those are not at all processed. Again, lower priority packets are also eliminated which may result in packet loss.
2. The security protocol results in huge control overhead because of cryptographic extension and acquisition delay.
3. These systems are not at all efficient and effective for huge numbers of nodes. It also results in a huge execution time.
4. Initial packet loss can be noticed because of the probable selection of wormhole nodes.
5. In each case, these approaches result in noticeable identification inaccuracy.

Passive as well as active attacks are found in wireless mesh networks through wireless multi-hop communication. In the case of wireless mesh networks, passive attacks may violate confidentiality. On the other hand, active attacks may violate authentication, integrity, and non-repudiation. It is very much important to develop an efficient and effective security scheme to exchange information. The traditional approaches are inefficient due to storage, energy, and bandwidth restrictions. Therefore, there is a necessity for an advanced authentication technique in order to overcome all the issues of wireless mesh networks. It also involves high-speed wireless approaches, and it has a wide range. There are two major reasons for this authentication, those are: -

1. Each mesh domain is required to authenticate every individual user in order to avoid fraudulent use of network resources.
2. Usually, the authentication protocol is time-consuming and infeasible in terms of costs. It involves the users, his home domain, and his foreign domain also. On increasing the user base, the authentication signalling overhead is also increasing.
3. A new bilateral service level agreement is included among every pair of wireless mesh network domains to allow the process of user roaming.

Among all benefits of the above method, self-organization, minimum installation expenses, large-scale deployment, and fault-tolerance are significant ones. The above-mentioned features are responsible to connect anywhere and anytime. Both mesh routers and mesh clients result in poor security due to constrained computing and power supply.

Prior to the network access, every individual client is required to be authenticated with the help of a mesh access point. During the roaming of mesh access points, the client is required to be re-authenticated to access uninterrupted network services. To operate real-time applications and offer improved service, the handover latency must not be greater than 50ms. The latest wireless mesh networking standard IEEE 802.16m requires 1000ms in order to process Extensible Authentication Protocol (EAP) in case of a round trip between the client and the server. Many enhancements are required. To decrease the latency at the time of roaming, several different handover authentication protocols are introduced. The security issues are more complex in the case of wireless mesh networks as compared to traditional wired and wireless networks.

2. Related Works

C. Zhang introduced a new security architecture in order to achieve anonymity and traceability for WMNs [1]. Anonymity has become the prime concern of researchers because of the users' awareness of their privacy. The process of anonymity adds protection for users to access network services without being visible.

Y. Shih emphasized fast handoff in the case of secure IEEE 802.11s mesh networks [4]. The concept of mesh networking has become more popular nowadays and the applications of mesh networks are also increasing day by day. Research has focused on a fast handoff in the case of a secure mesh environment. Besides these, this research work includes the means related to IEEE 802.11s. It will no doubt treat a particular mesh portal just like an IEEE 802.1X authenticator to decrease the extra expenses of IEEE 802.1X authentication processes at the time of handoff. This technique is introduced to include all the constraints of IEEE 802.11s and 802.11i. Again, this technique can be implemented in generic multi-hop wireless networks.

X. Shen, introduced an advanced encryption-based authentication architecture for wireless mesh networks [3]. User authentication process has significant importance in the case of service-oriented communication networks. These systems have the responsibility to detect and discard all kinds of unauthorized network access. A secure wireless network must have an appropriate authentication mechanism, authorization, and accounting framework.

N. Guo introduced an anonymous authentication technique that completely depends upon the identity-based encryption model [2]. Access security is considered as the major challenge during the population of the wireless mesh network. In this piece of research work, the researchers introduced a new proxy group signature technique that completely depends upon the identity. This technique is integrated with proxy group signature and identity-based group signature technique. They have considered the hierarchical proxy architecture of wireless mesh networks. The above-proposed technique is basically an anonymous mutual authentication method. This method has the responsibility to simplify the complicated management of PKI. Apart from this, it plays a significant role during the anonymous authentication process.

A. Levi and E. Savas proposed a secure and efficient distributed key establishment protocol for wireless mesh networks [4]. In the above-presented research paper, they have introduced an effective and efficient security establishment protocol that can be implemented in the case of wireless mesh networks. The above-mentioned protocol completely depends upon identity-based key establishment. On increasing the threshold value, the resiliency of the network also increases. Apart from this, the latency and success percentage decreases significantly.

K. Yim presented an advanced localized efficient authentication technique in the case of multi-operator wireless mesh networks along with an identity-based proxy signature scheme [5]. They have included the basic concepts of an identity-based proxy signature scheme. Fast authentication in the case of various roaming environments is supported with the help of HMAC operations. Key agreements between network entities can be applied in order to protect both communication and authentication.

D. P. Agrawal introduced a polynomial-based technique in order to establish each and every authentic association in the case of wireless mesh networks [6]. Different degrees of mobility of mesh clients provide higher flexibility. Again, it also helps during the construction of an authentic association of different entities. In this piece of research work, they developed a polynomial-based technique that is responsible for providing pairwise connectivity, low communication, average storage overhead, and higher scalability. This technique is mostly resilient against traffic analysis as well as node capture attacks. In most wireless mesh

networks, challenges can be detected for mesh clients.

G. Xi presented traffic- agnostic intrusion detection system for resource-constrained wireless mesh networks [7]. Because of the increasing interest in the case of wireless mesh networks, the associated security challenges are also increasing day by day. Intrusion detection is considered the most common and vital security mechanism in the case of wireless mesh networks. This may lead to high false-negative rates because a small number of intrusion detection system functions can be activated inside the monitoring nodes. All the previously existing solutions result in very high communication overhead along with detection delay in case of high traffic load. In this piece of research work, a practical traffic-aware detection system is introduced for resource-constrained wireless mesh networks.

J. Chen proposed a linear multi-secret sharing technique in order to carry out group communications within a particular wireless mesh network [8]. Presently, wireless mesh networks are considered the most important technology that includes low-cost community wireless services.

C. Lee and C. Ku developed a new ticket-based authentication technique in order to achieve fast handoff in the case of wireless mesh networks [9]. Because of the increasing popularity of mobile devices, the requirements of large-scale wireless network infrastructure development are also increasing. A mobile device owner can become online in place of a wireless network access point. A particular wireless network access point has the responsibility to cover a restricted area. In some cases, if the handover protocol is inefficient, the internet connection can be disconnected.

S. Parka emphasized the design and implementation of an advanced data protection technique of energy IoT with the help of OTP within a wireless network [10]. The one-time password is the most used authentication technique. This technique uses a randomly produced nonce. The prime objective of this method is to resolve the security issues which usually occur when the same password is used for all the transactions. In this proposed method, a nonce is used as an encryption key during the process of encryption.

N. Huda proposed an efficient authentication technique in the case of wireless mesh networks [11]. They have introduced an advanced security protocol in order to support fast handover in the case of IEEE 802.11 based wireless mesh networks. In this security model, the authentication server is not involved during the handover authentication process.

Y. Zhang introduced a new privacy-preserving security model for WMNs [12]. Both security and privacy are considered as the major factor behind the efficiency of mesh networks. Presently, there are numbers of service-oriented applications which can be supported by deploying wireless mesh networks. There is no significant amount of research works has been carried out during the process of privacy preservation in the case of wireless mesh networks. This approach is known as PEACE (privacy-enhanced yet accountable security framework). This method enforces sophisticated user access control in order to manage the gap between free-riders sends malicious users. Apart from this, this technique provides an advanced user privacy protection scheme that is beneficial for all network entities. This technique is a perfect combination of strong authentication and key agreement protocols to carry out the complete process of short group signature variation.

X. Yang, introduced an enhanced handover authentication scheme and key

pre-distribution in the case of wireless mesh networks [13]. A ticket-based encryption mechanism is considered a complex technology to provide security to wireless mesh networks. This technique enables the communication between laptops, mobile phones, and various other kinds of wireless devices. In this piece of research work, they presented a new handoff authentication in the case of wireless mesh networks. This technique has the responsibility to decrease the handoff delay. They tried to improve the traditional key pre-distribution method during the process of handoff authentication. They implemented a new attribute-based authentication scheme in order to encrypt every individual key pre-distribution message. The complete process of key pre-distribution involves fixed computation expenses and communication expenses.

3. Proposed Model

In the proposed framework, each mesh client is initialized with a unique mesh id as an attribute in the dynamic WMN. Here, MC-1,MC-2…MC-n is the mesh client nodes in the WMN. These mesh nodes are used to initialize the mesh id and mesh data. Here, the attribute list defines the names of the mesh identities for policies construction. A policy list is used to check the constraints on the attributes for the data encryption and decryption process. In the proposed framework, a non-linear chaotic map is used to generate the randomization keys for the encryption and decryption process as shown in figure1. In this work, a dynamic chaotic key-based ciphertext policy attribute-based encryption(CP-ABE) model is implemented to secure the communication data in the dynamic WMNs.

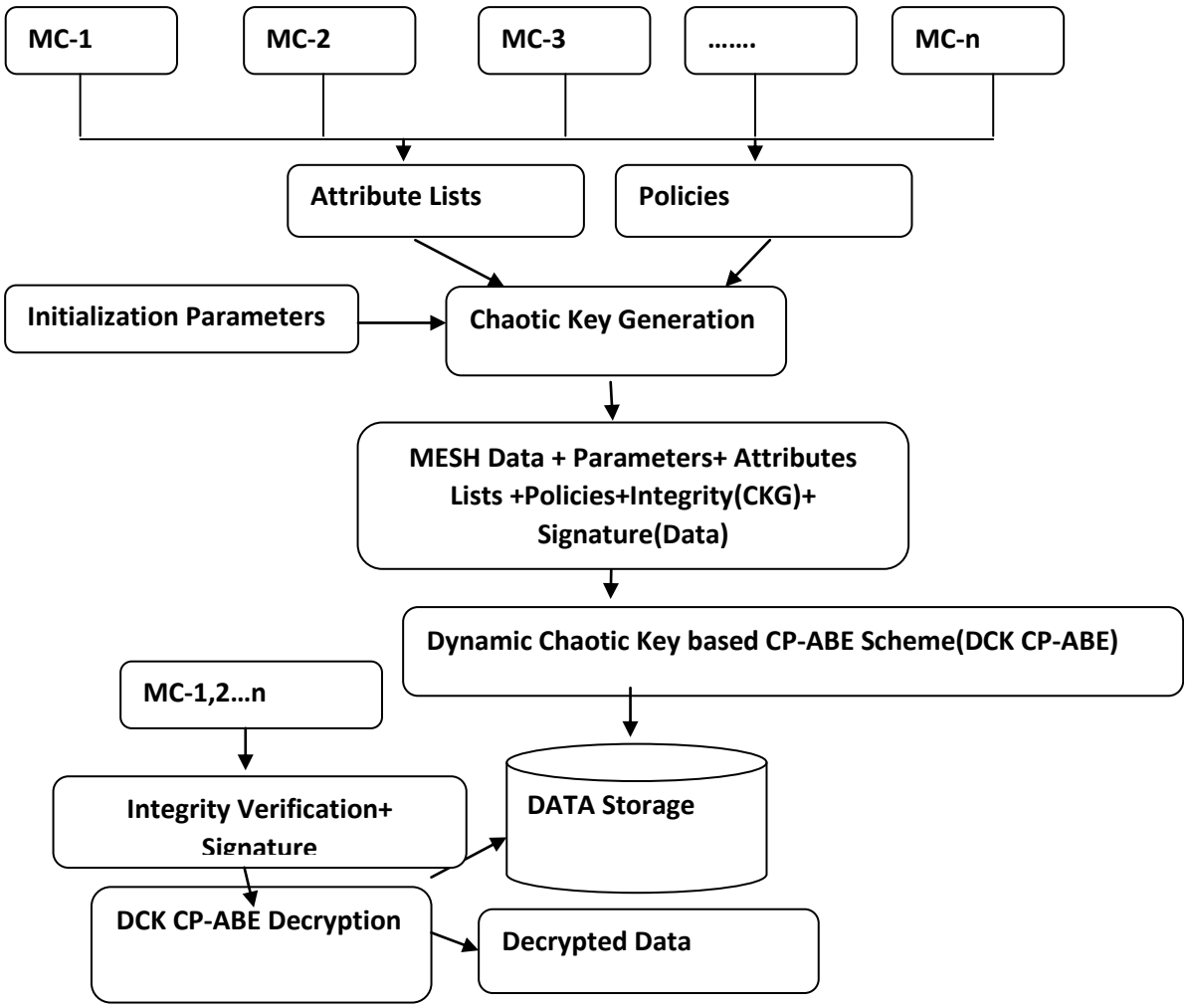
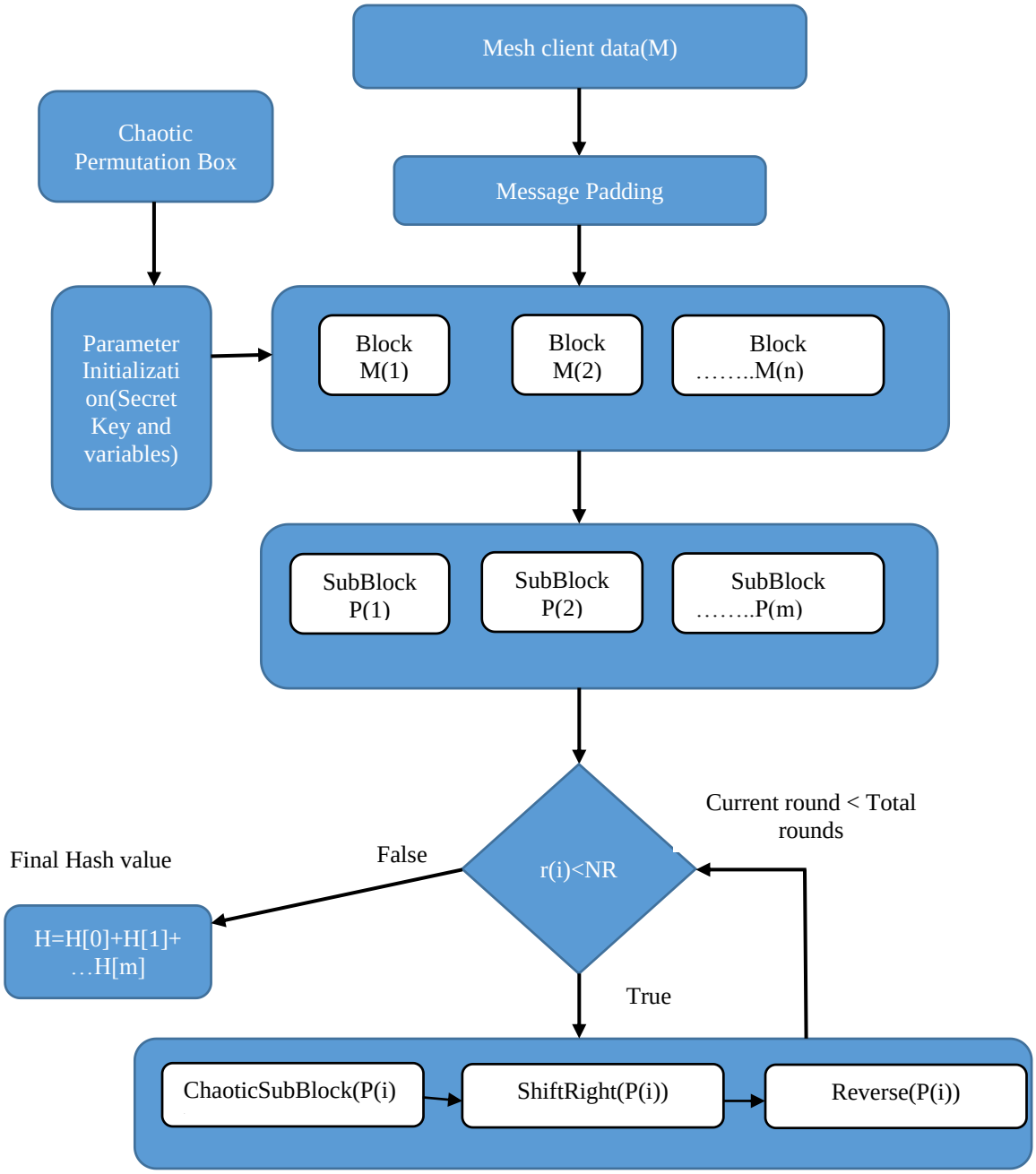


Figure 1: Proposed Model

Here, a dynamic chaotic key is used to find the integrity of the data owner during the data encryption and decryption process. After the data encryption, the ciphertext of the mesh data is stored in the data storage. The reverse process of encryption is the decryption process. Each mesh client decrypts the data from the mesh server using the policies that are defined in the mesh cipher data for the decryption process.

Proposed Algorithm 2: Chaotic Integrity Computation Algorithm



In the proposed model, a novel chaotic integrity verification algorithm is proposed to improve the performance of the wireless mesh clients in the dynamic WMNs. Figure 2, represents the proposed model architecture for integrity computational of the mesh clients. As shown in the figure, initially, each mesh client details and its data are taken as input to proposed integrity computation. If the size of the input message exceeds its hash size, then the message is padded with 1 followed by zeros. Here, input message M is

partitioned into blocks and then subblocks of size 32-bits each.

Computing Q using Secret Key matrix SK.
SK=[k1,k2..kn]
Using QR decomposition formula we have
SK=QR
$Q=SK.R^{-1}$
Where $Q=[v_1,v_2.....v_r]$ and

$$R=\begin{pmatrix} k_1.v_1 & K & k_1.v_r \\ M & O & M \\ 0 & L & k_r.v_r \end{pmatrix}$$

Chaotic Key Generation =

$$<CS>=<\begin{matrix} X_{n+1}=Y_{n+1}.X_n(1-X_n) \\ Y_{n+1}=p.\cos(2.\cos^{-1}Y_n) \end{matrix}>$$

Here, the chaotic key generation is used to generate the sequence of high randomized values. These sequences of randomized chaotic values are used to initialize the permutation box and secret key in the integrity computation model.

Step 1: Input Mesh Client details M_ID and Data D, Hash Size S, NR:Number of rounds.
Step 2: Message M=M_ID+D;
Step 3: Generate Secret key SK using the dynamic chaotic permutation Box generated using the set of chaotic key generation.
Step 4: Divide the message M into S/8 blocks.
Step 5:while(|M|>S/8)
Do
Message Padding;
BlockProcess(M[S/8]);// step 6
Done

Step 6: BlockProcess
Partition the block into S/32 subblocks of 4 bytes each;
P[]=ParitionBlocks[S/32];
For i=0 to |P|
Do
for each round r in NR-1
Do
ProcessSubblock(P[i]) // step 7
Done
Done
Step 7: ProcessSubblock
For each byte in P[i]
Do

$U_1 = SK^T$. [Q. Rank(SK), (CauchyLowerBound(Poly(SK))]

$$U_2=(\frac{[Q.\text{trace}(SK),\ (\text{CauchyLowerBound}(\text{Poly}(SK))]}{(\sum SK[i])/\max\{\text{solve}(\text{Poly}(SK))\}})$$

$U_3 = \sum \text{Solve}(\text{Poly}(Q.R))$ **// sum of roots of polynomial equation**

$H[i]= U_1 \oplus U_2 \oplus U_3$

Done
Step 8: H=H[1]+H[2]+….H[NR]

In the proposed integrity computational algorithm, an improvement in the chaotic key generation and sub-block processing are performed on the input mesh data. This algorithm is used to improve the high randomization and less computational time compared to the previous integrity verification algorithm.

Dynamic Chaotic CP-ABE Encryption Model:
The proposed integrity-based encryption algorithm consists of four phases i.e., Mesh Setup, mesh Encryption, mesh Chaotic Key generation, mesh decryption. Each phase and its mathematical formations are described below.
Phase1: Mesh setup: In this mesh setup phase, each mesh node initializes its own cyclic group parameters and chaotic In this phase, mesh public key and the master key is generated. Mesh public key is used to encrypt the source mesh node data to the nearest connected mesh node. The Mesh master key is used to generate the secret key in the mesh key generation phase.

Let G_1, G_2, Z_p are cyclic group pairing elements

$$Pubk = \{H_{4096}(G_1), H_{4096}(G_2), g^{H_{4096}(Z_r)}\}$$

$$Mk = \{H_{4096}(Z_r), g^{H_{4096}(Z_r)}\}$$

```
Element alpha  = pairing.getZr().newElement().setFromHash(bt, 0, 5);
PK.g           = pairing.getG1().newElement().setFromHash(bt, 0, 5);
PK.gp          = pairing.getG2().newElement().setFromHash(bt, 0, 5);
MK.beta        = pairing.getZr().newElement().setFromHash(bt, 0, 5);
MK.g_alpha     = PK.gp.duplicate().powZn(alpha);
PK.h           = PK.g.duplicate().powZn(MK.beta);
PK.g_hat_alpha = pairing.pairing(PK.g, MK.g_alpha);
```

Phase 2: Mesh data encryption: This phase takes a mesh attributes, mesh data as input and generates ciphertext as output using the mesh public key and mesh integrity values.
Let p1,p2 be the two cyclic prime factors taken from G such that

P=p1*p2; Q=log(P*P);

Choose a chaotic random number R_n from

Chaotic Key Generation =<CS>=<

$$X_{n+1} = Y_{n+1}.X_n(1-X_n)$$

$$Y_{n+1} = P.\sin(2.\sin^{-1} Y_n) >$$

$$\phi = \frac{p1.p2}{(P^{(p1)} \bmod(R_n)^{(p2)} \bmod(H(R_n))}$$

$$k = \phi^{\gcd(P.\max(p1,p2),R_n)}$$

Ciphertext CB[i]={Atree,

$$R_n^{PB[i]}(\bmod(s).R^P \bmod(e^Q)).\bmod(e^Q)\}$$

Mesh Key Generation Phase: In this phase, the mesh master key is used to generate the secret key. This secret is embedded with mesh integrity value for node authentication verification. The secret key is generated using the following formula.

$$Sk = \{Attlist, g, g.H_{4096}(meshdata), g^{H_{4096}(Z_r)}\}$$

Mesh key Decryption: In this phase, attribute list, ciphertext, and mesh integrity value are taken as input in order to decrypt the mesh data using the access tree structure.

$$h_1 = R_n^{\phi} \bmod(e^Q) - (\frac{\phi}{P})^{-1} \bmod(P)$$

$$D[]=\{CB[i]^{\phi} \bmod(e^Q) - \frac{\phi}{P}.h_1 \bmod(P),$$

Atree}

4. Experimental Results

Experimental results are executed in Netbeans IDE tool using Java environment. In this experimental study, different initialization parameters such as a number of mesh clients, malicious attack nodes, and a number of iterations are taken as input for network setup.

WMN Setup:

In the mesh network setup, the simulation view is designed using the SWING library. Third-party libraries such as Jama, JForm, Apache math, JSimulation are used to implement the proposed network topology. The basic parameters used to set up the wireless mesh network is shown in table 1.

Parameter Name	Purpose
Mesh –ID	Mesh node identity
Data	Mesh node communication data
Nodes	Number of mesh nodes to setup in the wireless mesh topology
Malicious nodes	Number of malicious nodes initialized in the mesh network

WMN Initialization:

In the proposed algorithm, different color nodes are initialized randomly in the WMNs as shown in Figure 3.

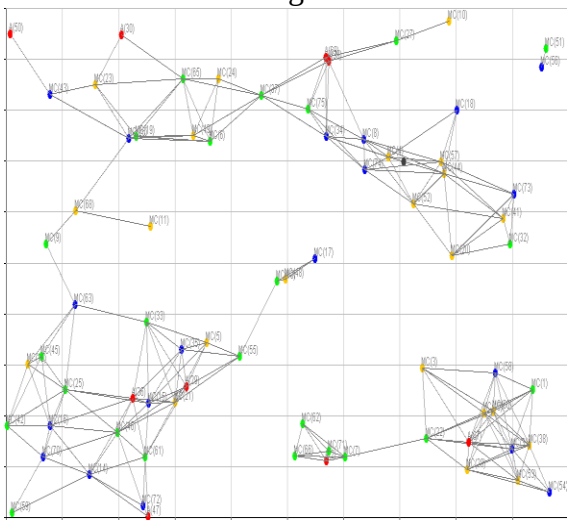


Figure 3: WMN initialization

The mesh network is initialized with mesh clients and malicious attack nodes. In the simulation, malicious attack nodes are represented in red colour and authorized mesh clients are represented in blue, green and yellow colours. For an efficient diffusion property, there should be a 50percent bit change in the hash value. The computed hash of the mesh node integrity is taken as a binary form to check the change bits.

Figure 4: Mesh generated sample master key:

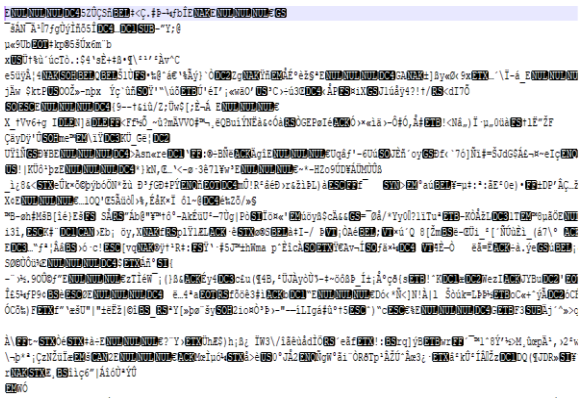
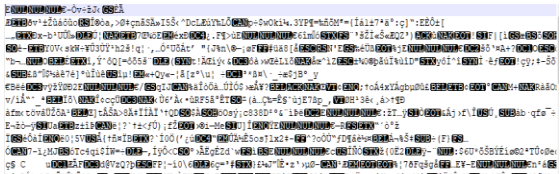


Figure 5: Mesh generated sample public key



Encrypted Sample Data:

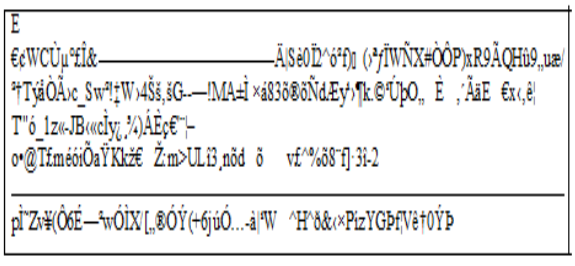


Table 2: Comparative analysis of the proposed model to traditional integrity algorithms on mesh data.

Model	Integrity Sensitivity	Integrity runtime(ms)
MD5	115	4353
SHA512	119	3975
whirpool	121	3684
NL-integrity	131	3254
ProposedIntegrity	133	2974

Table 2, describes the comparison of the proposed optimized integrity algorithm sensitivity and runtime to the existing algorithms on large mesh data. From the table, it is noted that the present algorithm has high sensitivity and less runtime than the existing algorithms.

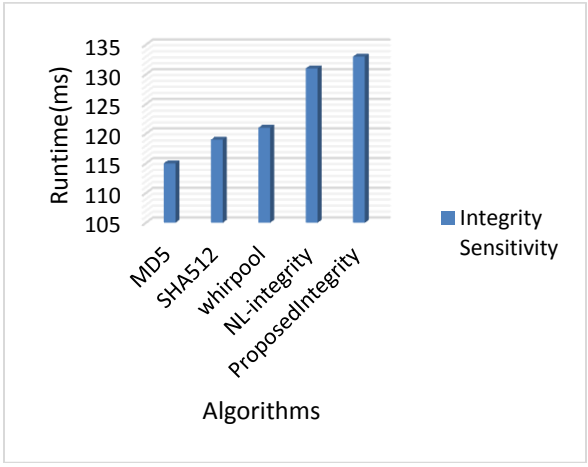


Figure 6: Comparative analysis of proposed model to traditional integrity algorithms on mesh data.

Figure 6, describes the comparison of the proposed optimized integrity algorithm sensitivity to the existing algorithms on large mesh data. From the figure, it is noted that the present algorithm has high sensitivity and less runtime than the existing algorithms.

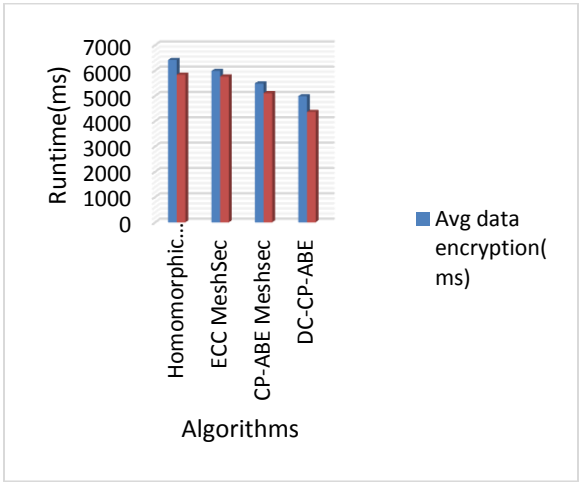


Figure 6: Comparative analysis of proposed model to traditional encryption algorithms on mesh data.

5. Conclusion

In most of the traditional malicious attack detection models, as the size of the network increases, these models become difficult to detect the malicious clients due to high computational time, data, and memory. Also, traditional encryption algorithms are independent of mesh client authentication and data security due to large data size and changes in mesh node properties. To overcome these problems in the dynamic WMNs, an integrated mesh node authentication and data security framework is developed. This model is efficient on the large WMNs and provides strong data security during the mesh client authentication process. In this framework, a novel integrity-based encryption algorithm is designed and implemented on the mesh client data for strong security. Experimental results illustrate that the proposed security model is efficient than the traditional models in terms of data encryption runtime (ms), data storage space, and integrity sensitivity.

References

[1] C. Zhang, "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks", "IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011", pp. 295-308.

[2] N. Guo, Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network, Journal on Wireless Communications and Networking (2016) 2016:193.

[3] X. Shen, ,TUA: A Novel Compromise-Resilient Authentication Architecture for Wireless Mesh Networks,IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 4, APRIL 2008, pp. 295-308 389-1400.

[4] A. Levi ,DKEM: Secure and EfÞcient Distributed Key Establishment Protocol for Wireless Mesh Networks, Ad Hoc Networks.,

[5] K. Yim, LEAS: Localized efficient authentication scheme for multi-operator wireless mesh network with identity-based proxy signature, Mathematical and computer modelling.

[6] D. P. Agrawal, Polynomial based scheme (PBS) for establishing Authentic Associations in Wireless Mesh Networks, J. Parallel Distrib. Comput. 70 (2010), pp. 338-343.

[7] G. Xi, RAPID: Traffic-agnostic intrusion detection for resource-constrained wireless mesh networks, Computer and security (2017), pp. 1 -17.

[8] J. Chen, A novel linear multi-secret sharing scheme for group communication in wireless mesh networks, Journal of Network and Computer Applications 34(2011), pp. 464–468.

[9] C. Lee and C. Ku, A New Ticket-Based Authentication Mechanism for Fast Handover in Mesh Network.

[10] L. Parka, and S. Parka, Design and Implementation for Data Protection of Energy IoT utilizing OTP in the Wireless Mesh Network, 4th International Conference on Power and Energy Systems Engineering, CPESE 2017, 25-29, September 2017, Berlin, Germany.

[11] N. Huda , Efficient Authentication for Fast Handover in Wireless Mesh Networks, Computer and security.

[12] Y. Zhang, PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks, PEACE: A Novel Privacy-Enhanced YetAccountable Security Framework for Metropolitan Wireless Mesh Networks, pp. 203-216.

[13] X. Yang, X. Huang, J. Han and C. Su, Improved handover authentication and key pre-distribution forwireless mesh networks, Concurrency Computat.: Pract. Exper.2016; 28:2978–2990.