JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Data reliability in Adhoc network for enhanced security using randomized bit interleaving

Ramya s pure
pureramya@gmail.com
Guru Nanak Dev Engineering College, Bidar.

Dr Dayanand J
jdayanand1@gmail.com
Guru Nanak Dev engineering College bidar

Abstract:

Security of data in Adhoc network is enhanced by a new randomize bit interleave coding for encryption process. The volatile nature of the Adhoc network has a constraint of security breaching resulting in non-reliable data exchange. The conventional approach of security provisioning using heuristic approach was developed in improving security provisioning. Recent method based on self-adaptive sail fish optimization (SA-SFO) is used in the security provisioning in real time data exchange. The optimization approach selects a suitable embedding location in data encoding using sail fish coding which improves the security level and data integrity. However, the approach does not focus on the security pattern applied and use a fixed key pattern in encryption process. This limits the security coding with higher probability of data breaching. To overcome the stated limitation in this paper, a new security key provision using randomized bit interleaving is proposed. The randomized key pattern offers a higher security measure and higher data accuracy.

Index term: Data security, Adhoc network, Randomized bit interleaving, Adaptive coding.

I. Introduction

Advancement in the communication approach has outcome into various new means of data exchange, in which Adhoc network has shown a great interfacing in wireless communication. The dynamic nature of data exchange in Adhoc network due to a self-creating property offers a high possibility in data exchange at remote places. In wireless ad hoc networks, reliability is the most critical consideration. As a result, in Adhoc network, determining trustworthiness has become critical. Routing techniques in many existing wireless networks presuppose the presence of dependable nodes. However, given the nature of wireless ad hoc networks, this is not a tenable premise. Also, because of the frequent topology changes, connection failures and node failures are possible. The stability of wireless networks has become a significant problem in the design, development, and implementation of wireless networks as the use of wireless networks grows. A wireless network's ability to supply the essential services must be quantified by establishing relevant quantifiable quantities. The reliability measurements of the network are the names given to these quantifiable values. Reliability of the data exchange is a major factor in the performance of Adhoc network. To improve reliable data exchange, various security coding were proposed in past. a comparative analysis of the two most often used methods of symmetric encryption, DES and AES is outlined in [1] for the selection of security coding in data exchange. High impact owing to one-bit change in plaintext while keeping the key constant, the memory required for implementation, and the simulation time necessary for encryption were observed and found optimal for AES approach. It is also observed that DES encryption scheme that had a disadvantage because of its large memory consumption.

In [2] the use of AES to encrypt messages exchanged between objects through unprotected channels is outlined. It is observed that AES is helpful for monetary transactions, as well as for experiments on other forms of data. [3,4] compared the most widely used symmetric encryption methods AES (Rijndael), DES, 3DES, and Blowfish in terms of power consumption. Comparison of the encryption methods employing various data kinds, such as text, image, audio, and video were outlined in [5]. The algorithms for encrypting data were implemented in Java. The software has been tested on a variety of file types and sizes. The encryption, decryption, and throughput times were measured. It is observed that AES has a superior performance than other commonly used encryption algorithms, according to the simulation findings presented. In [6] AES is outlined as a strong candidate for security due to the fact that the study presented & demonstrated no known security flaws. DES performed poorly because it demands a lot of computing resources. The AES encryption technique is the ideal choice for MANET nodes because battery

power is one of the primary limits. In [7,8] Symmetric key encryption methods such as DES, AES, and Blowfish were developed in NS-2 network simulator in order to compare their effectiveness with various data kinds such as text and image. A variety of file kinds, including text, image, and video, are encrypted by the algorithms in the tests. Measurements such as encryption and decryption times, power usage, remaining battery capacity, and data throughput were taken to determine performance. Analysis for Different packet sizes were used in [9] to create a symmetric encryption method, and the obtained simulation results revealed that AES is easy and better than the other developed algorithms in terms of residual battery & encryption time. In terms of throughput, Blowfish performed better, but it uses more battery power when compared to the other algorithms.

[10] studied how to improve wireless Ad hoc security by using an encryption technique and a specified transmission rate. The data was sent in one of two ways: encrypted or not. In the first case, data is sent in an unencrypted form. DES, AES, and Blowfish are the three encryption algorithms used in the second way of transmitting data. In [11] one key was utilized to encrypt and decode data during data exchange, which was kept large for higher security. The amount of time it takes to deliver data to the receiver and the amount of data that may be received is calculated based on the inputs of distance and size and for fast data delivery and high throughput, AES was observed suitable, while using Blowfish for bigger data transfers with a lower transmission rate. The video streaming properties of Ad hoc networks were studied in [12-15] using various cryptographic techniques. Ad hoc networks can benefit from secure video streaming. The network layer was protected by using a public key infrastructure (PKI).

Ad hoc networks based on Optimized Link State Routing (OLSR) might benefit from a fully distributed certifying authority. It took less than 1500ms to encrypt a 1-MB binary file using RC4, 3DES, AES-128, AES-256, Salsa20-128 and Salsa20-256. Interference detection system EAACK proposed by [16] is composed of ACK, Secure Acknowledgement (SACK), and Authentication of Misbehavior Reports (AMR). To avoid the use of fake acknowledgement packets, all of the recognition packets were signed and authenticated. Keys were developed and distributed ahead of time for signing or verifying acknowledgement packets.

In [17] a one-hop ACK is employed to increase detection rates of misbehavior. The proposed system included DHKE, which relies on the difficulty of computing algorithms and allows users to securely encrypt communications, to eliminate the demand for pre-distributed keys. In order to conduct a simulation, the NS-2simulator tool was employed, and findings revealed an increase in misbehavior detection rates, which leads to lower routing overhead than that of the existing Intrusion Detection Services (IDS). [18] proposed the HARD-KM key management and authentication technique, which uses hop-by-hop authentication and routing. Two pairs of keys were generated using an enhanced Elliptic Curve Diffie-Hellman (ECDH)protocol with authentications and stored in a cache until their expiration. Instead of placing some cluster heads or a central node in the network, HARD-KM employed an off-line digital certificate to sign credentials and disseminate authentication credentials matrix for all mobile nodes in the network.

The feasibility and efficiency of HARD-KM were evaluated with the use of an NS2 simulator. Key storage space was reduced while the HARD-KM key management system remained impervious to attackers. A shared secret key generation for symmetric key encryption over Ad hoc networks, which was proposed in[19]. New routing protocols for MANETs is developed using notion to ensure maximum security against every type of attacks. It is possible to create an encrypted data transmission protocol that has five stages, including: key generation and exchange; shared secret creation; and encrypted data transmission. Open-source e-learning program CrypTool [20] was used to model and evaluate the DH key agreement protocol, an open-source simulator for cryptographic algorithms. It is not just source and destination who can see the public parameters, because they were made publicly available. In CrypTool, the secret numbers of a source and destination are selected by pressing the button choose hidden that once public parameters have been defined. It is only then that each party receives a copy of the other's shared key. It's at this point that CrypTool generates a shared and secret session key for both the source and destination.

For a reliable coding in security measure recently in [21] a new method based on heuristic optimization approach using sailfish optimizer is proposed. This method combines the approach of sailfish behaviors and predator movement in the location of best position of data embedding for security coding. However, the volatile nature of the Adhoc network limits the security measure due to fixed key allocation. A security model that uses several techniques to encrypt and decrypt packets is proposed in this work using Randomized Bit Interleaving for Encryption and Decryption in Ad hoc Networks (RBI-ED-AN).

The key generation and selection model is performed randomly. The suggested methodology reduces the number of messages transferred between nodes during key establishment. The proposed model enhances the security levels of the ad hoc networks by encoding the data at sender using randomized bit interleaving model and the data decryption is performed at the destination side. To present the outlined approach this paper is presented in 6 sections, where the existing security approach is outlined in section 2. Section 3 outlined the approach of randomized bit allocation for security measure. In 4 the simulation result of the developed method is outlined. Section 5 present the conclusion of the presented work.

II. heuristic security coding in MANET

With the rise of internet and wireless communication, it's more important than ever to prioritize safety. Cryptosystems have been created in an effort to increase security. All cryptographic algorithms perform encryption and decryption. The art of cryptography is changing data into a form that cannot be deciphered by those whose data is meant. Crypt text is the name given to the data after it has been encrypted. In order to preserve the original data, the cipher text and the key are decoded one after the other. Only the intended recipients of the data can perform this decryption method. Among cryptographic algorithms, AES is one of the most widely used. An AES algorithm was requested by the National International Organization For standardization (NIST) in 1997 as a way to improve on 3DES' flaws. Over the course of five years, NIST received fifteen algorithms for evaluation. Ad hoc Networks (ANETs) have evolved as a significant next-generation wireless networking technology in the recent years. But security concerns on ANET are becoming a major issue. In contrast to wired networks, ANETs are more susceptible to assaults. There will always be attempts to exploit these flaws and interrupt ANET operations as a result. In addition to the problem of passive observation and masquerade, the wireless environment complicates the matter further. Confidentiality is one of the security services available to ensure data safety. Confidentiality refers to the practice of limiting who has access to private information. Because ANET makes use of an open medium, data can typically be accessed by any node within the transmission range. Using data encryption techniques is one method of keeping information private.

For the sake of saving space and transferring more data over the internet, compression is used to protect the data. Transferring data from a hard drive to a memory device becomes much faster. Confidentiality, Authentication, Integrity, and Non-repudiation are the four pillars of data security. Data security provides enterprise-wide data protection. IT firms of all sizes are increasingly concerned about the security of their data. More and more IT companies are turning to encryption to safeguard their sensitive data in response to this growing issue. Additional problems for IT businesses include the ever-increasing expenses of storage needed to ensure that there is sufficient storage capacity for the organization's present and future needs.

Reduced storage and communication costs are two of the advantages of data compression. As the name implies, it entails the transformation of data in one form the source message into data in another form the code word that is much smaller. It is well-known that data encryption is used to protect information from being eavesdropped. It uses an encryption key to transform data from one format to another called cypher text. As things stand right now, compression and encryption are handled independently. Early cryptography was effectively synonymous with encryption, the transformation of information from an easily readable state to an unintelligible one before the advent of digital encryption. As a result, today's encryption algorithms are built on computational hardness assumptions, making it extremely difficult for an adversary to crack them in practice. It is theoretically possible, but practically impossible, to break such a system.

On-demand IT services are hampered by security concerns, which pose the greatest challenge in ad hoc network environments. This has led to a great deal of research on the difficult problem of securing data on ad hoc networks against assault and other unforeseeable events.

The most effective and common solution to this problem is to use encryption methods in network servers. Ad hoc network settings require more than just a single cryptographic technique to provide data security and precise access control, especially when a user's permissions are removed. In order to prevent the user who has been revoked from accessing the encrypted data and produce reliable keys for legitimate users, a re-encryption scheme appears to be necessary. Responsibilities such as managing time, resource confidentiality, and access control must all be taken into consideration while implementing a re-encryption procedure. Because of this, efficient re-encryption management may improve the dependability and the level of security in ad hoc network situations.

In order to connect participating nodes in wireless networks, the wireless medium must always be available. Because of its openness, this medium is subject to a wide range of security risks. It is possible for anyone with a transceiver to listen in on wireless communications, send false information, or block the legitimate ones entirely. It is significantly more difficult to combat jamming attacks than it is to stop eavesdropping and message injection. By delivering a continuous signal or multiple short bursts of jamming, a jammer can disrupt communication. External threats have typically been used to represent jamming attacks, when the jammer is not a network node. Denial of service attacks are virtually always the result of jamming, and this is true for both the sender and the receiver. Users can jam wireless network connection simply by sending a constant stream of garbage data to the node that's already overloaded. If a jamming signal is active, the vast majority of individuals are unaware of it. There seems to be no service. This exploit prevents genuine users from accessing the network resource. If an attacker is present in the network, they can readily intercept every message transmitted by any node using broadcast communication. A Denial-of-Service attack is caused by an attacker who selectively jams only the messages sent by the target node.

Encryption is one of the best ways to protect sensitive data from attackers. The decryption process, also known as a key, is required to recover the data's original content after it has been encrypted. Security or protection from unauthorized access is the goal of the encryption procedure. A substitute technique, a shifting methodology, or mathematical operations can all be used to implement encryption. In the last year, a number of new symmetric key reference algorithms

have been created. Encryption and decryption systems are mostly used for privacy concerns. Access to data transmitted via the Internet can be gained by other parties that are not authorized. Decryption is the process of transforming encoded or encrypted text or other data back into text that can be read and understood by you or the computer. Un-encrypting data manually or using the correct codes or keys is referred to as decryption in this context. Plaintext data is converted into something seems to be random and useless through the process of encryption. To put it simply: decryption is the process of deciphering cipher text.

Even if the encryption algorithms are not encrypted and stored on the compromised nodes, the system's confidentiality could be jeopardized. The problem of key management is yet another obstacle to effective ANET security. Because hostile nodes can join networks if they are not authenticated, it is necessary to do so. For ANETs, a low weight and space efficient key management strategy is important because of their limited energy consumption and computational capabilities.

In optimizing the security method current security coding are upgrading with new heuristic methods. In recent a self-adaptive sailfish optimization approach is presented for security enhancement in MANET [22]. The sailfish optimizer is used to develop an enhancement in the security measure to retain the message quality bit. In the process of SFO develop a fitness function is used in the determination of embedding location of the secrete keys into the original information. The optimization approach is developed with the objective of retaining the quality of the proposed approach with the payload maintaining. In developing the embedding process, the fitness function used is defined as,

$$Ft(n) = \frac{Ac(n) \times Sq(n)}{\sum_n Lc} \times Rv \qquad (1)$$

Where,

$Ac(n)$ is the ASCII converted characters

$Sq(n)$ set of letters in sequence

Lc letter's locations

Rv random values with values 0 to 1.

The encryption process is developed for the key pattern given for processing. The embedding is developed by replacing the original data with the encrypted data. The SFO method selects the location of the embedding. The process iterates for the best fitting value where the position of the sailfish is updated given by,

$$p_n^{m+1} = p_n^{m+1} - \varphi_m \times (\beta \times p_e^m + y_n^{m+1})/2) - p_n^m \qquad (2)$$

Where,

p_n^{m+1} is the new updation position of sailfish

p_n^m is the current location of the sailfish

β is a random number of value 0 to 1

p_e^m is the current changing position of the sailfish

y_n^{m+1} is the position of injured sardine

φ_m is the generated coefficient at each iteration

The updation parameter φ_m is given as,

$$\varphi_m = (2 \times \beta \times De) - De \qquad (3)$$

Where,

β is a randomly varying value between 0 and 1

De is the current density of the prey.

The value of density of prey De is given as a ratio of numbers of sailfish and sardines in current observation which is given as,

$$De = 1 - (Csf/(Csd + Csf) \qquad (4)$$

Where,

Csf is the count of sailfish in observation and,

Csd is the count of sardine in the observation.

The updation process is iterated for the fitness function eqn. 1 convergence, where the location of the sailfish is updated using eqn. 2. The best location of the embedding is located and applied key is embedded for encryption. Here, the location prediction gives a significance of better security provisioning, however the key applied constraint its robustness. To improve the security measure, a new bit interleaved key is proposed which offers a higher security and data quality for location predicted and updated security approach.

III. Randomized bit interleaved coding for MANET

It is possible for an adversary to add fake data or a harmful script to encrypted data packets, even if they are protected by encryption algorithms and safe keys. Information packets may be corrupted by a malicious node that adds junk or alters the data. Modified data cannot be used by the network and may impair communication over the network. As a result, data integrity ensures that any sent data has not been tampered with. The proposed model maintains integrity in data transmission to the end users. The freshness of data is just as important for network transmission as it is for maintaining data secrecy and integrity. Older data should not be used, and newer data should be used instead. The cryptographic keys need to be renewed,

refreshed, and altered over time for them to be effective. Replay attacks can be thwarted if the data is kept up-to-date. These problems can be addressed by utilising timestamps.

Communication security relies heavily on the ability to authenticate each other. This feature ensures that every data is from a reliable source. It is important for the sending node to verify that it is the network's genuine node and that any data it sends is valid. In other nodes, verify that the data or communication you are receiving is verified and trustworthy. The proposed model authenticates the nodes before providing the keys for encryption and decryption. Using node encryption to protect data collecting can be beneficial. However, for the intermediate nodes, it is necessary to decrypt and encrypt a lot. In order to handle all node content in the connection path, it is too complicated and expensive. In order to collect data, the entire procedure must be open to the public, which increases the risk of obtaining private information.

Using the bit operation, the plaintext of the information gathered for privacy purposes is encrypted. Increased plaintext of confidentiality will reduce encryption performance due to a large number of repetitions. Iterative sequences with different beginning values are generated for each block of plaintext. It is possible to overcome this issue by using encryption. The major goal of the proposed security architecture is to improve existing data security techniques for ANETs in order to accommodate technological advancements and to examine the performance of the network. A random pattern will emerge when responses are evaluated, making it impossible to determine either the algorithms or the keys. A common set cryptographic algorithm is utilised by both the sender and receiver to encrypt and decrypt the data packets. A suitable synchronisation function is selected to appropriately coordinate the decoding on the other end. A security model that uses several techniques to encrypt and decrypt packets is proposed in this work using Randomized Bit Interleaving for Encryption and Decryption in Ad hoc Networks (RBI-ED-AN). The key generation and selection model is performed randomly.

Algorithm RBI-ED-AN

{

Input: Nodes in Network, Threshold Th value

Output: Encrypted and Decrypted data

Step-1: The nodes need to involve in the data communication process has to register the identity. The nodes registration and identity generation is performed as,

$$NR(n) = \sum_{n=1}^{P} nodeID(n) + TI + Th + \bigcup_{n=1} maxcomp(n) + \bigcup_{n=1} maxener(n) \quad (4)$$

Here nodeID is the default node identity value, TI is the time instant, Th is the threshold value, maxcomp(.) is used for identifying the maximum computational capabilities and maxener() is used to calculate the maximum energy level of a node.

Step-2: The key generation model is performed and the keys are used for encryption and decryption of data that provides security for the data. The key generation is performed as

$$p = getvalue(n)$$

$$v = getvalue(n) > p$$

$$r = getrand(p, v)$$

$$T_1 = p \ll 2 \oplus v + r \quad (5)$$

$$T_2 = V\&2 \oplus p \quad (6)$$

$$K1 = T_1 \ll 2v + r \quad (7)$$

$$K2 = T_1 + T_2 + \ll \left(\frac{r}{2}\right) + p - v \quad (8)$$

$$Keyset\{v1: v2\} = \{K1\&r|p + Th: K2\&r|q + Th\} \quad (9)$$

Step-3: The randomized bit interleaving process for a 42 bit value is performed that is used in the encryption and decryption process that uses complex model for providing the security.

RL = RL & 0x3fffffffff (10)

RL = (RL | RL& p<< 64) & 0x3ff00000000000000ffffffffL (11)

RL = (RL | RL⊕ q<< 32) & 0x3ff00000000ffff00000000ffffL (12)

RL = (RL | RL | r<< 16) & 0x30000ff0000ff0000ff0000ff0000ffL (13)

RL = (RL | RL | p<< 8) & 0x300f00f00f00f00f00f00f00f00f00fL (14)

RL = (RL | RL& q << 4) & 0x30c30c30c30c30c30c30c30c30c30c3L (15)

RL = (RL | RL⊕ r<< 2) & 0x9249249249249249249249249249L (16)

RBInV=RL⊕K1&K2 (17)

Step-4: The node authentication is performed to permit for the encryption process. The nodes which are authenticated only will be provided with a key for encryption.

$$AuthenN(n) = \sum_{n=1} getnodeID(n) + TI + NR(n)\varepsilon NetworkNodes \quad (18)$$

If(AuthenN(n)>0)

Node(n)=VALID

Else

Node(n)=INVALID

Step-5: The encryption process is performed on the data that needs to be transferred to destination. The encryption is performed on the normal message NM resulting in cipher text. The encryption is performed as

$$MT = NM^{v1} mod(p) \quad (19)$$

$$CT = MT|RL + p - q \oplus \text{K1} \quad (20)$$

$$CT = \text{RBInV} \oplus \mathbf{r} - \boldsymbol{T_2} \quad (21)$$

Step-6: The node authentication is performed to permit for the decryption process. The nodes which are authenticated only will be provided with a key for decryption.

$$AuthenN(n) = \sum_{n=1} getnodeID(n) + TI + NR(n) \varepsilon NetworkNodes \quad (22)$$

If(AuthenN(n)>0)

Node(n)=VALID

Else

Node(n)=INVALID

Step-7: The decryption is performed to access the original data at the destination side. The decryption on cipher text results in normal message by the destination. The generated cipher text CT is considered to perform decryption operation. The decryption is performed as

$$MT = CT^{v2} mod(q) \quad (23)$$

$$NM = MT|RL - p + q \oplus \text{K1} \quad (24)$$

$$NM = \text{RBInV} \oplus \mathbf{r} + \boldsymbol{T_1} \quad (25)$$

Step-8: The data loss rate of the model is calculated for identification of the lost data that can be retransmitted.

$$DL = \sum_{n=1}^{M} PDR(n) + maxPack(n) - PD(n) + \bigcup_{n=1} TotPackets(Network) \quad (26)$$

Here PDR is the packet delivery rate, PD is the packets delivered successfully and totpackets is the total packets generated in the network.

}

IV. Simulation result

To determine whether a specific group of nodes will be able to communicate with one another for a specific amount of time is a common problem in network dependability. A security model that uses several techniques to encrypt and decrypt packets is proposed in this work using Randomized Bit Interleaving for Encryption and Decryption in Ad hoc Networks (RBI-ED-AN). The proposed model is compared with the traditional Self Adaptive Sail Fish Optimization (SA-SFO) model. The proposed model exhibits better results when compared to traditional model in terms of Node Authentication Accuracy Levels, Key Generation Time Levels, Randomized Bit Generation Time Levels, Encryption Time Levels, Decryption Time Levels, Data Reliability Maintenance Levels and Data Security Levels.

The technique of Node Authentication is used to ensure safe communication between the controlling server and data collectors. The Data Sources all operate in a secure manner when dealing with Node Authentication. Authentication is perhaps the most effective and efficient method of securing a network. For more secure connection through that node, authenticating it is a good idea. It can be concluded that some attacks alter sensor network nodes in order to introduce hostile new nodes. Other normal nodes can accept these new nodes that have been introduced. Because these bogus nodes are a problem, an authentication method is essential. The node authentication accuracy levels of the proposed and traditional models are shown in Figure 1.

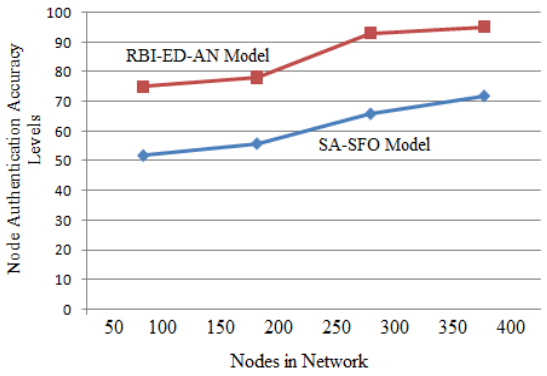

Fig 1: Node Authentication Accuracy Levels

In cryptography, key generation is indeed the process of creating new keys. Symmetric-key algorithms and public-key algorithms are two of the most common types of modern cryptography. One shared key is required to keep data private in symmetric-key methods. A public key as well as a private key are used in public-key algorithms. Anyone can access the public key. When a sender uses the recipient's public key to encrypt data, only the recipient's private key may decrypt it. The key generation time levels of the proposed and traditional models are shown in Figure 2.

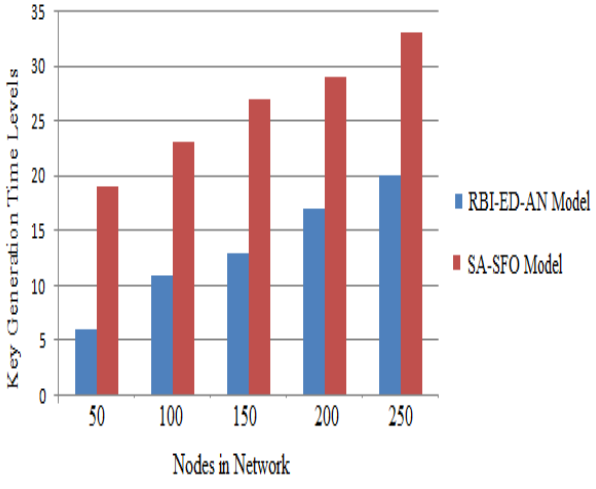

Fig 2: Key Generation Time Levels

Reordering data to be communicated in order to distribute successive bits of data over a broader data sequence to lessen the impact of errors is called interleaving. Non-contiguous data is interleaved in order to speed up and improve a systems performance and reliability. It aids with the organisation of data and the detection of mistakes. The ability of error prevention codes to adjust for errors is substantially enhanced by the use of interleaving. After going through the interleaving block, which is essentially a bit interleaving, the data bits are in the correct order as transmitted. The randomized bit generation time levels of the proposed model are less than the traditional model. The randomized bit generation time levels of the existing and proposed models are shown in Figure 3.

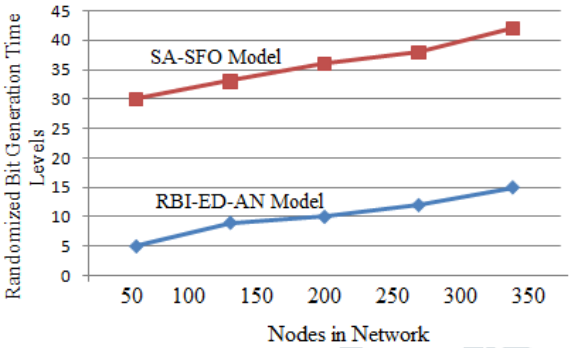

Fig 3: Randomized Bit Generation Time Levels

As a means of protecting digital information, encryption uses one or maybe more mathematical techniques, as well as a key or password that can encrypt the data. Encryption is the process of transforming data into a form that cannot be decoded by humans. The encryption time levels of the existing and the proposed models are depicted in Figure 4.

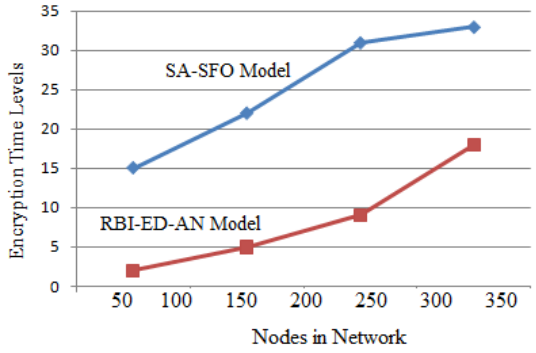

Fig 4: Encryption Time Levels

Decryption refers to the process of restoring encrypted data to its unaltered state. Most of the time, it is the opposite of what is performed in encryption method. Decryption necessitates a secret key or password, so only authorised users can access the encrypted data. The decryption time levels are represented in the Figure 5.

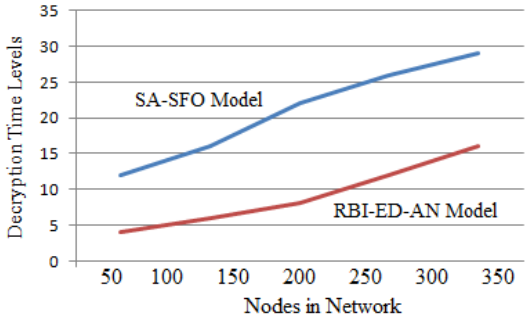

Fig 5: Decryption Time Levels

Data accuracy and completeness are essential prerequisites for establishing a culture of data trust within an organisation. In addition to ensuring data security, quality, and regulatory compliance, one of the primary goals of data integrity initiatives is to ensure data reliability. The data reliability maintenance levels of the proposed and existing models are shown in Figure 6.

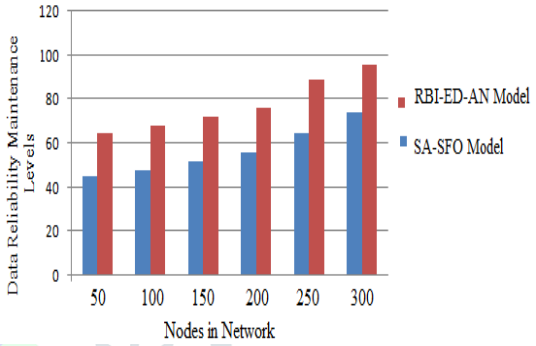

Fig 6: Data Reliability Maintenance Levels

When it comes to data security, it is all about safeguarding user's information against unwanted access and corruption at every stage of its lifespan. There are a number of techniques that can be used to protect data, including data encryption, hashing, tokenization, and key management. The data security levels of the existing and current proposed model is shown in Figure 7.

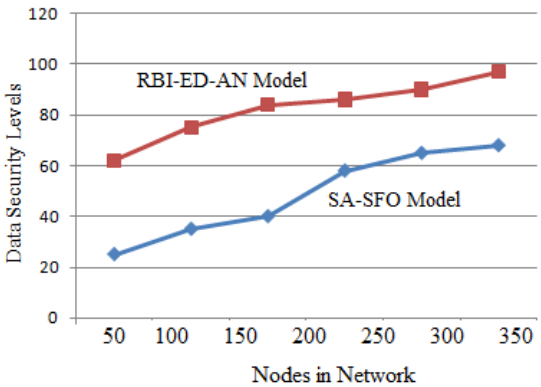

Fig 7: Data Security Levels

V. conclusion

Data is encrypted and other users' identities are verified using cryptography, which safeguards the privacy of its users. More data can be saved because of it. When it comes to transmitting sensitive information, cryptography is a useful approach. Using random algorithm selection, we have come up with a new way for protecting data in wireless ad hoc networks. The proposed approach was tested on AODV traffic with CBR to see how it performed. Data security was examined first, and then we compared the protocol's performance both with encryption and decryption. In comparison to data provided without encryption, the suggested security solution boosts the delivery ratio to 96%. There is a very less delay induced by the encryption procedure, but the control overhead does not increase significantly as the network traffic increases. We conclude that the suggested randomised bit interleaving scheme provides best security for the data in the ad hoc networks, and that it works well for networks with high movement and heavy traffic. In future, the encryption model complexity can be reduced to avoid delay in encryption process that improves the network performance.

VI. References

[1]. Khatri, Yogesh, Rachit Chhabra, Naman Gupta, Ashish Khanna, and Deepak Gupta. "Secure modified aes algorithm for static and mobile networks." In International Conference on Innovative Computing and Communications, pp. 389-399. Springer, Singapore, 2020.

[2]. Rao, Kavikondala Praveen Kumar, and Tamilarasan Senthil Murugan. "Energy efficient clustering technique using k-means and AODV-ACO Routing with Secured AES Cryptography in MANET." International Journal of Intelligent Engineering and Systems 12, no. 3 (2018): 292-302.

[3]. Bulla, Suneetha. "A Comprehensive Survey on Cryptography Evaluation in Mobile (MANETs)." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 2 (2021): 3406-3416.

[4]. Kapoor, Jitaksh, and Divyansh Thakur. "Analysis of Symmetric and Asymmetric Key Algorithms." In ICT Analysis and Applications, pp. 133-143. Springer, Singapore, 2022.

[5]. Sudha, S., V. Madhu Viswanatham, K. Brindha, L. Agilandeeswari, and G. Ramya. "Implementation of Enhanced Data Encryption Standard on MANET with less energy consumption through limited computation." Proceeding of International Journal of Engineering Research and Development 2, no. 4 (2012): 46-52.

[6]. Srividya, R., and B. Ramesh. "A COMPARATIVE ANALYSIS OF DES AND BAES FOR MANET." Technology 11, no. 6 (2020): 816-825.

[7]. Ahmad, Amal, and Shereen Ismail. "User selective encryption method for securing MANETs." International Journal of Electrical and Computer Engineering (IJECE) 8, no. 5 (2018): 3103-3111.

[8]. Bulla, Suneetha. "A Comprehensive Survey on Cryptography Evaluation in Mobile (MANETs)." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 2 (2021): 3406-3416.

[9]. Vinayagam, Jaikumar, C. H. Balaswamy, and K. Soundararajan. "Certain investigation on MANET security with routing and blackhole attacks detection." Procedia Computer Science 165 (2019): 196-208.

[10]. 10 Ismail, Zahian, and Rosilah Hassan. "Effects of packet size on AODV routing protocol implementation in homogeneous and heterogeneous MANET." In 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, pp. 351-356. IEEE, 2011.

[11]. Sarao, Pushpender. "Performance Analysis of MANET under Security Attacks." J. Commun. 17, no. 3 (2022): 194-202.

[12]. Sharma, Ravi Shanker, Bright Keswani, and Dinesh Goyal. "Analysis of routing and security issues in OLSR protocol for video streaming over MANET." Journal of Discrete Mathematical Sciences and Cryptography 25, no. 4 (2022): 1203-1211.

[13]. Nourildean, Shayma Wail, Yousra Abd Mohammed, and Abdulkreem Mohammed Salih. "Mobile Ad Hoc Network Improvement against Jammers for Video Applications Using Riverbed Modeler (v17. 5)." Webology 19, no. 1 (2022).

[14]. Patil, Vrinda R., and S. V. Sandhya. "QoS aware MANET routing protocol for multimedia traffic in an adaptive cross layer architecture." IRJET 6, no. 06 (2019).

[15]. Ahmed, Diaa Eldin Mustafa. "Enhanced Scheme for Video Transmission over Mobile Ad hoc Networks based on Optimized Link State Routing Protocol." PhD diss., Sudan University of Science and Technology, 2020.

[16]. 16 Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." IEEE Transactions on industrial electronics 60, no. 3 (2012): 1089-1098.

[17]. Dhende, Sandeep, and Suresh Shirbahadurkar. "MACO-DHKE Based Secure Data Transmission in MANETs." International Journal of Electrical and Computer Engineering Systems 13, no. 4 (2022): 245-252.

[18]. Sharma, Apoorva, and Gitika Kushwaha. "Comparative Analysis of Different Encryption Techniques in Mobile Ad-Hoc Networks (MANETs)." IITM Journal of Management and IT 10, no. 1 (2019): 55-64.

[19]. Sirajuddin, Mohammad, Ch Rupa, Surbhi Bhatia, R. N. Thakur, and Arwa Mashat. "Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-Healthcare System." Wireless Communications and Mobile Computing 2022 (2022).

[20]. Bairwa, Amit Kumar, and Sandeep Joshi. "Mutual authentication of nodes using session token with fingerprint and MAC address validation." Egyptian Informatics Journal 22, no. 4 (2021): 479-491.

[21]. Mercy, S. Sudha, J. M. Mathana, and J. S. Jasmine. "An Energy-Efficient Optimal multi-dimensional location, Key and Trust Management Based Secure Routing Protocol for Wireless Sensor Network." KSII Transactions on Internet and Information Systems (TIIS) 15, no. 10 (2021): 3834-3857.

[22]. Abdulhammed, Omar Younis. "SFO for enhancing steganogrphy by exploiting exact resemblance between cover and secure text." Acta Scientiarum. Technology 44 (2022): e57581-e57581.