A Collusion attack prevention (CAP) scheme for securing Mobile Adhoc Network

Madiha Zanab , Humaira Ashraf * , NZ Jhanjhi *

Posted Date: 22 December 2023

doi: 10.20944/preprints202312.1652.v1

Keywords: Collusion attack prevention; Wireless; Mobile

Article

A Collusion Attack Prevention (CAP) Scheme for Securing Mobile Adhoc Networks

Madiha Zanab, Humaira Ashraf * and NZ Jhanjhi [2,*]

[1] Department of Computer Science and Software Engineering, International Islamic University Islamabad 44000, Pakistan; humaira.ashraf@iiu.edu.pk, madihazanab@gmail.com

[2] School of Computer Science, SCS, Taylor's University, Malaysia {noorzaman.jhanjhi@taylors.edu.my}

* Correspondence: humaira.ashraf@iiu.edu.pk; noorzaman.jhanjhi@taylors.edu.my

Abstract: Due to the advancement and availability of internet in present age, device tend to become wireless as well. Mobile ad-hoc network is a wireless environment that consist of advanced agility of nodes and does not contain on any central administrative authority. As it does not contain any central administrative authority so being wireless environment, the network is vulnerable to security threats and suffers in performance as well. Security of MANET is the core issue in this era, meanwhile the data is sent over untrustworthy network. Several techniques were proposed to secure data over Mobile Adhoc Network though cryptography that is one of the most reliable techniques to protect data. In our proposed methodology a Secure Cryptographic technique for Mobile Adhoc Networks (SCTMA) we proposed A Collusion attack prevention (CAP) scheme with ElGamal key generator along with DNA encryption Algorithm is used to make it more secure. The proposed scheme protects the network against collusion attacks and improves the performance as well. Performance analysis will be measured on the basis of key generation time, response time, encryption time and decryption time. The proposed scheme also protects the network against collusion attacks.

Keywords: collusion attack prevention; wireless; mobile

1. Introduction

A mobile ad hoc network is a independent group of mobile devices (laptops, smart phones, sensors, etc.) that are unified with each other over wireless connections and collaborate in a scattered mode to perform the essential network functionalities in the absence of an immovable structure. In MANET mobile devices are connected to each other within their range and communicate to each other to exchange data and information between each other's.

Security is the major concern in the communication channel in MANET technology. Attacker attacks on the network with the intention to destroy information or to hack the information. It is a serious concern for big organizations, military departments and educational institutes that have private information about departments. To provide enough security in MANET Enhanced Adaptive Acknowledgement (EAACK) scheme was proposed [1] that further consists of three more schemes: ACK, SACK, and MRA. All techniques uses acknowledgement packets with data to provide more security while transmitting message over the network. All these schemes are acknowledgement packet based so it makes easy for the attacker to invade the security hence making the scheme vulnerable. In [2], to provide better security author proposed a Curve Based Cryptography scheme with CBSDV routing protocol for authentication of valid nodes. In CBSDV scheme, the data of every system ingoing a network or outgoing from the network are retained by the Credibility Check Table (CCT) and update automatically. CBSDV using curve-based cryptography scheme for encryption that is attacked by collusion attacks. An overview of collusion attack is shown in Figure 2:in this paper a secure encryption scheme with ElGamal key Generator is proposed to protect the MANET against collusion attack. To make it more secure we are used DNA encryption algorithm as well.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Figure 1. Shows an overview of MANET.

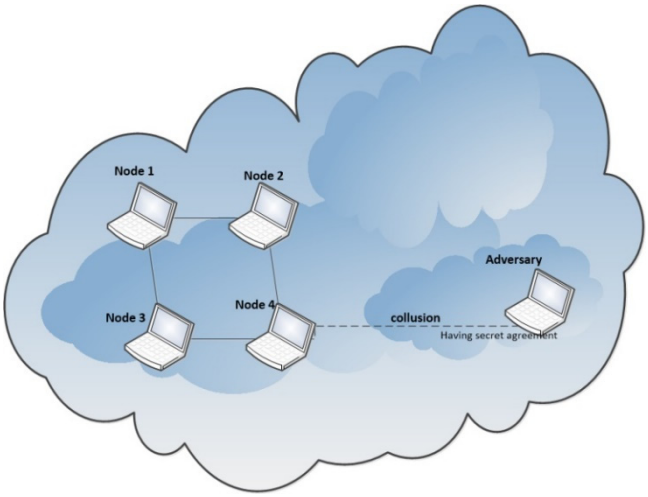


Figure 2. Overview of Collision Attack.

The proposed scheme protects the network against collusion attacks and provides better performance by reducing the encryption and decryption with key generation time.

1.1. Novelty of Work

- A much more interesting attack known as collision attack is prevented through a simple and efficient CAP algorithm.
- A secured CAP algorithm is simple and comfortable in terms of cost and time consumption.

1.2. Contribution of Work

- Proposed technique is tested over various input sizes to analyze security level.
- Multiple literature techniques are collected and compared with the proposed CAP algorithm in terms of time consumption.

1.3. Organization

The rest of the paper is organized as: unit 2 describes literature review, unit 3 describes proposed methodology, whereas unit 4 explains result analysis, and in unit 5 conclusion is provided.

2. Literature Review

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Data security is the main concern in Mobile Adhoc Networks. There are so many vulnerabilities to destroy the security of Mobile Adhoc networks. A detailed literature review is discussed here, where various techniques that have been studied explained. Figure 3 illustrates an overview of all techniques that will be discussed below:

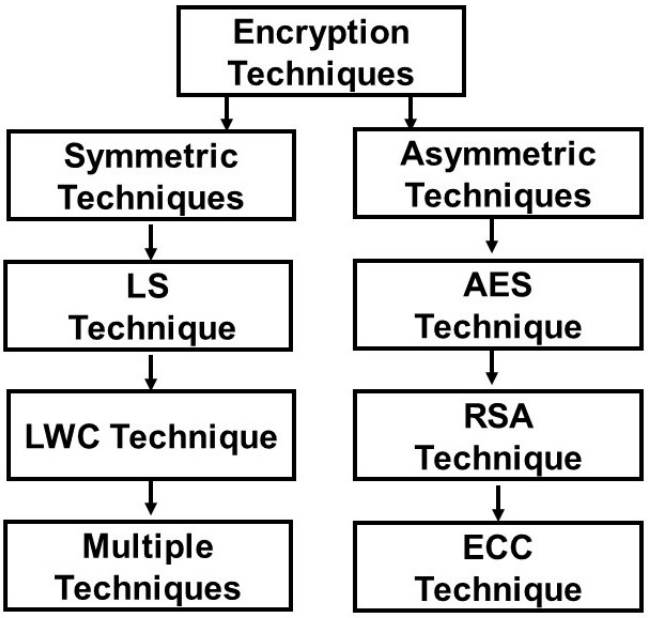


Figure 3. Overview of techniques.

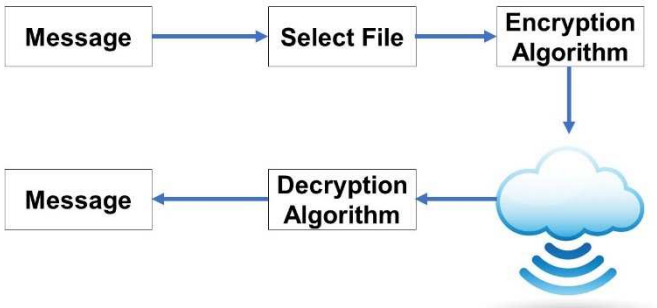
In this paper [1] researchers used hashing functions for secure encryption. In this research [2] the researcher proposed EAACK and it includes ACK, SACK and MAR schemes. It is concluded that collusion is not found in the network when hash functions are used [3]. SHA (Secure Hash Algorithm) shows that slide attacks occur on Hash function. In research [4], researchers proposed EAACK technique which is the combination of SHA and DSA and it is also vulnerable to slide attacks. In [5], an evaluation of Boolean function is used to prove that differential attack can occur if SHA-3 is used. In [6], the researchers proposed a methodology by using Chinese remainder theorem (CRT) based key generation that suffer from birthday attack and computation cost is also very high using CRT technique.. In [7], authors showed that the birthday attacks have easily occurred on CRT technique when the private and public key is very small. It has also shown that CRT can be broken down easily. In [8], the researchers proposed a technique by using CRT). Researcher briefly describes in [9] that Chinese remainder theorem based techniques suffer from vulnerabilities of computationally hiding commitments. In this research [10] researcher proposed a lightweight Elliptic curve based cryptography scheme for the security of nodes in MANET. ECC is an efficient technique for security issue. it is noticed that collision search attack possible to occur on the proposed procedure and study has verified to reduce the time of breaking ECC in [11]. In this research [12] researcher proposed Distributed Public key Infrastructure using Shamir Secret Sharing methodology which permits the nodes to share their private key among other nodes in MANET. Communication is done by using the Tiny Encryption Algorithm (TEA). The TEA can be infected by key equivalence attack [12]. This attack is done by using a known plain/cipher text pair of any unknown key (K). In the proposed methodology researchers also used the Diffie Hellman Key exchange algorithm which is less secured, because it has low-security performance that is verified/proven by the researchers in [13]. In paper [14], the researchers proposed a new technique, recognized as QOS secure encryption (QASEC), to reach better throughput by securing end-to-end communication in MANETs. In paper [15] researchers focused on secure intrusion detection system using RSA to provide security to physical devices in mobile ad hoc networks against attackers. However, RSA has some drawbacks[16]. RSA algorithm is attackable by some sort of mathematical attacks, small private key attacks, small public key attacks, implementation attacks, and elementary attack. In [17], researchers concentrate on some

 doi:10.20944/preprints202312.1652.v1

malicious activities in Manet. They proposed an Adaptive Approach Detection using KDS with a shuffling algorithm. This scheme minimizes the effect of key management-based authority certificates and minimizes acceptance level without disturbing the nodes. In this paper researchers proposed Cooperative Bait Detection Scheme (CBDS), which has some drawbacks. the drawbacks of CBSD technique were increased computational overhead and reduced efficiency [18]. In [19], researchers proposed a technique named as TRIM in which three nodes are referee nodes. Proposed methodology used hashing function. However, it is concluded that it is difficult to find collusion and slide attacks in the network while using hash function [3]. In [20], researchers proposed a new cryptography scheme that is Letter to Shape Encryption for providing security among nodes in the Manet. This method exchanges different shapes for letters in a message that will be transmitted. This scheme is harmless in contradiction of man in the middle attack. Researcher proved in [21], that this technique has too much simpler algorithm, the attacker can easily break the security. Data security in WSN is very difficult due to sensor nodes limited lifetime. An efficient approach for data security in WSN is given in [22]. This research approach gives a decent amount of data security, yet it does not reduce sensor node lifetime. [23] used an efficient genetic based security algorithm with ElGamal key generation method to secure data in WBAN. The Robust Cluster Based Routing Protocol (RCBRP) is described in this study [24] in order to pinpoint the routing paths that use the least amount of energy and so extend the life of the network. For the purpose of examining ow and communication, the design is provided in six phases. We suggest the following two algorithms: (i) an energy-efficient clustering and routing method (and (ii) a distance and energy consumption calculation technique. Clustering the smart devices allows the system to use less energy while balancing the load. With a focus on data security challenges across many clouds, this paper [25] suggests the Proficient Security over Distributed Storage (PSDS) technique. The data is separated into two categories by PSDS: normal and sensitive, with the latter category being further broken into two portions. While the typical data is uploaded on a single cloud in encrypted form, each component is encrypted and dispersed over multiple clouds. Sensitive data is combined from many clouds during the decryption stage. The PSDS has been put to the test against a number of attacks, and it has been determined that it is resistant to related key attacks, pollution attacks, chosen ciphertext attacks, and well-known plain text assaults. Building upon the foundational work laid out in [24-30], our proposed Collusion Attack Prevention (CAP) scheme for securing Mobile Adhoc Networks represents a significant advancement in the field. The techniques and methodologies introduced in [31-34] provide a solid basis for understanding the challenges in ad hoc networks, while the innovative approaches outlined in [35–59] inform and inspire our design choices for effective collusion attack prevention.

3. Methodology

Security is the major issue in mobile ad hoc network. The communication over mobile ad hoc network, suffer from difficulties against confidential data. Attackers attack on network to destroy data and information. For securing mobile ad hoc network various cryptographic schemes were provided in previous research work. In [2], the researcher proposed acknowledgement packet based scheme with hashing function for securing mobile ad hoc network and it is also proved by the researcher in [3], that while using hash function, it is difficult to find collusion attacks over Manet. Here, the proposed methodology provide security against collusion attacks. An overview of proposed methodology is explained below in Figure 4.



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Figure 4. Overview of Proposed Methodology.

3.1. Encryption Process

In the encryption process, initially data is converted into their ASCII values. Then ASCII values are converted into binary values by binary converter. Then compute the values from S-Box using the binary values as input, resultant values from S-Box are then combined with the generated key values using merge operation. Then applied DNA sequence coding algorithm and converted into cipher text. Figure 5 demonstrates the whole proposed key generation and encryption process, how key will be generated and then how DNA encryption algorithm will be worked to convert plaintext into cipher text.

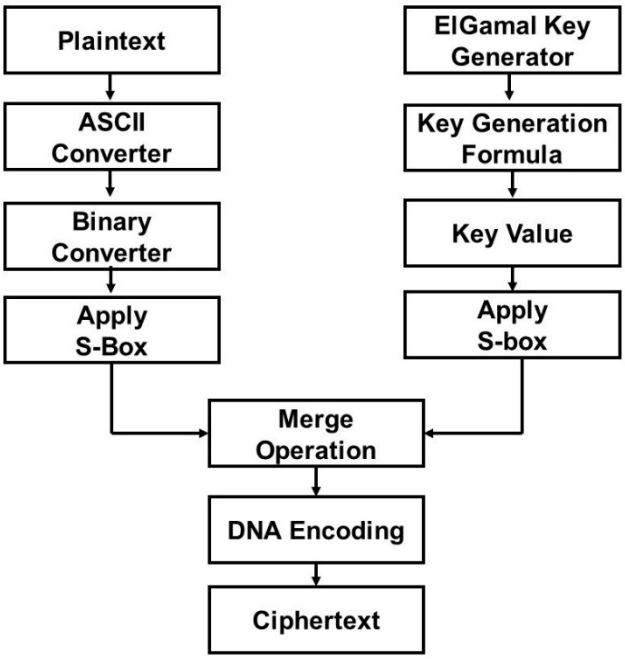


Figure 5. Overview of Proposed Encryption Technique.

3.2. Decryption Process

In the decryption process initially DNA sequence coding algorithm applied on cipher text in reverse. Then the resultant values from DNA will be divided into two halves', the first half's four bits are extracted from S-Box and then second half's bits will be extracted from S-Box. Then resultant eight bits will be converted to ASCII values and then converted into plaintext. Figure 6 Briefly describes decryption process of the proposed methodology that how cipher text will be converted into plaintext on the receiving side:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

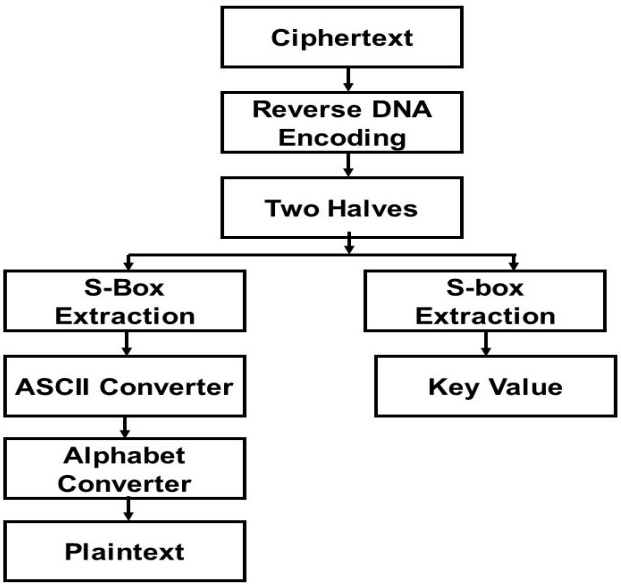


Figure 6. Overview of Proposed Decryption Technique.

3.3. ElGamal Key Generation Algorithm

There are two types of key generation algorithms, symmetric key generation algorithms and Asymmetric key generation algorithms. In symmetric key generation, only one key value is used for the both encryption side and decryption side. In Asymmetric key generation methods two keys are generated for encryption and decryption processes, one public key and second is private key. Here proposed scheme uses ElGamal key generation algorithm for encryption and decryption processes. ElGamal key generation algorithm is symmetric key generation algorithm. Table 11 consists of all steps of ElGamal key generation algorithm in detail. The algorithm works as it takes 3 public keys and 1 private key p, g an x respectively as prime numbers on the sender node. Node will have to choose values of p, g and x randomly then it will have to calculate the value of Y. The computation formula for y is given. The value of Y will be the key Value K.

TABLE I. ELGAMAL KEY GENERATION ALGORITHM

The Algorithm works as follows:

We have public keys (P, g, y)

1 private key X

We must choose the values of p, g and x randomly by the user,

but we must find out the value of key Y

For computation of Y the formula is:

$$Y = g^x \bmod p$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Table 2 consists of all steps of DNA digital coding encryption process. DNA takes 8-bit binary value and first divide them into pairs each consists of two bits 0 and 1. Then from DNA digital sequence table take an Alphabet for each pair and the receiving stream of alphabets called cipher text.

TABLE II. DNA BASED ENCRYPTION ALGORITHM

First take 8-bit input into binary form e.g., 01101101

Divide them into pairs, each pair consist of two bits

e.g., Input bits = 01101101

Pairs = 01 10 11 01

Then give each pair a value according to its digital sequence:

Binary Value	DNA digital sequence
00	A
01	C
10	G
11	T

Now convert paired bits into DNA digital sequence to make Cipher Text:

e.g., Paired bits = 01 10 11 01

Cipher Text = C G T C

End encryption process.

Substitution-Box is an elementary module of symmetric key algorithms which is used to perform substitution. In block ciphers, they are usually used to unintelligible the relationship between the key and the cipher text that is not understandable by the attacker. S-box takes some input bits, m, and transforms them into some output bits, n, where n is not essentially equal to m. The calculation of $m \times n$ S-box can be applied as a lookup table with 2^m words of every n bits. Table 13 shows an S-Box, which will be used by the proposed scheme:

TABLE III. NOTATION TABLE

Notations:	*Description:*
P	Denotes plaintext
K	For every alphabet or letter belongs to plaintext
N	Used to represent ASCII values
B	Denotes binary value
K_1	Denotes key value generated by ElGamal
V_1	Denotes first 4 bits of key value
V_1	Denotes last 4 bits of key value

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Z	Denotes merged values of V1 and V2
Y	Denotes values belong to Z
C_p	Denotes Cipher text

TABLE IV S-BOX

First 4 bits	Last 4 bits															
	1000	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**	**0000**	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**
0000	A1	B3	0A	C2	D3	DS	E3	J4	CM	O2	PP	LO	IR	HQ	MZ	QH
0001	Q1	B2	D5	0B	D2	8B	Q4	QS	K4	HR	P2	AR	DO	JS	RI	HO
0010	AB	RJ	C3	E6	0C	E2	PB	F3	TO	L4	CO	Q2	ZM	SJ	UR	QY
0011	BC	ZA	SK	D4	F7	0D	F2	NP	G3	MD	M4	KI	TK	VE	EV	RU
0100	DE	XB	JL	TL	E5	G8	OE	G2	GM	H3	DP	UL	7B	R2	3T	OY
0101	FG	YC	KI	E4	UM	F6	H9	OF	H2	MV	VM	5E	N4	6C	S2	LO
0110	HI	WD	L2	F4	9V	VN	G7	IA	0G	WN	I2	I3	7Z	O4	YO	T2
0111	JK	UE	M3	7O	G4	8X	WO	H8	XO	0H	N3	J2	J3	5N	P4	CV
1000	LM	SF	N4	4L	6B	H4	XP	YP	I9	JB	0I	O3	K2	K3	4W	Q4
1001	NO	QG	O5	4A	ST	3D	ZQ	YQ	OT	JA	KC	0J	P3	L2	L3	TV
1010	PQ	OH	P6	I4	QE	IR	0U	V3	ZR	OS	KB	LD	0K	Q3	M2	MP
1011	RS	MI	Q7	2M	2S	0V	U2	W3	X3	IS	OR	LC	ME	0L	S3	N2
1100	TU	KJ	R8	GT	0W	U4	FP	V2	Y3	Z3	2T	OQ	ON	NF	0M	R3
1101	VW	IK	4U	0X	T4	WZ	LT	PT	W2	XA	PO	3U	OP	NE	OG	0N
1110	XY	5V	0Y	S4	ZA	YX	V4	W4	BS	X2	Y4	T3	4V	0O	FT	PH

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

111 1	6W	0Z	R4	9L	Z4	Z W	MS	RP	9C	CS	Y2	U3	Z2	5W	6X	PG

Table 5 has detailed description of all encryption steps of the proposed 'A CAP (Collusion attack prevention) Cryptography Technique'. The methodology will be works as, it first takes 8-bit plaintext Pt, covert each character/letter into its ASCII value then convert these ASCII values into binary value refer as V. Then take 8-bit k key value generated by ElGamal key generator. System substitutes values of V and K from S-Box and then receiving two set of 4-bit values will be merge as a new 8-bit value. Then system will apply DNA encryption algorithm on the bits to form cipher text. The process will be stopped after this:

Algorithm: proposed encryption method
Input: plaintext **P**
Output: Cipher text **Cp**
Step 1. **for all** k € p **do**
convert **k** into equivalent **ASCII** values
end for
Step 2. **for all n € ASCII value do**
Convert **n** into equivalent Binary value **B**
end for
Step 3. **Take 8-bit key value K_1 generated by Elgamal Cryptosystem**
Step 4. **for all V_1 € K_1 do**
Apply **S-Box substitution** on k_1 values
end for
Step 5. **for all V_2**€ B **do**
Apply **S-Box Substitution** on **B** values
end for
Step 6. **Merge values of V_1 and V_2 to Z**
Step 7. **for all** Y € Z **do**
Apply **DNA** coding scheme on **Y**
end for

The Table 5 explain the algorithm of encryption.

Step 1: In first step, the system will take character by character from plaintext and then convert into their equivalent ASCII values.

Step 2: Then each ASCII values n converted into Binary values B

Step 3: In step 3 random 8-bit key value K1 is generated using ElGamal key generator.

Step 4: system will take first 4 bits from key value K1 and denotes it by V1 and then apply substitution Box on them.

Step 5: system will take last 4 bits from key value K1 and denotes it by V2 and then apply substitution Box on them.

Step 6: in step 6 the merge operation is applied to combine the values V1 and V2, received by system after Substitution process and give it name as Z

Step 7: In last step system will apply DNA digital coding scheme on values of Z and convert it into Cipher text.

Table 6 consists of decryption process of the proposed methodology. Decryption procedure will be works in reverse of encryption procedure.

Algorithm: proposed decryption method

Input: Cipher text **Cp**

Output: plaintext **P**

Step 1. **for all** Y € Cp **do**

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Apply reverse **DNA coding scheme** on **Y**

end for

Step 2. **Divide 8-bits value of plaintext Y into V_1 and V_2**

Step 3. **for all V_1€ Y do**

Extract values from **S-Box**

end for

Step 4. **for all V_2€ Y do**

Extract values from **S-Box**

end for

Step 5. **for all V_1 € B do**

// B=Binary values

Convert values of V into **ASCII** values

end for

Step 6. **for all K € ASCII values do**

Convert **ASCII** values into equivalent plaintext **P**

end for

Table 6 explains decryption process. In decryption process the system decrypts the cipher text into original plaintext step by step. Detailed process shown below:

Step 1: In the first step the reverse DNA digital coding scheme will apply on each character of Cipher text. The output will be in 8-bit value.

Step 2: In this step divide operation is applied and 8-bit value will be converted into two equivalent halves of 4-bits V1 and V2.

Step 3: In this step the system extracts values of V1 from S-Box. The output will be in binary numbers.

Step 4: In this step the system extracts values of V2 from S-Box. The output will be in binary numbers.

Step 5: In this step covert the resultant binary values, from step 4, into ASCII values.

Step 6: In last step system converts it into original plaintext and stop processing.

3.4. Math metical Modelling

P is the plaintext which sender wants to transmit over the network. AC denote ASCII converter, equation 1 presents original text conversion in ASCII code.

$$\boldsymbol{P \rightarrow AC} \quad \text{.....(1)}$$

Equation 2 shows that Y is temporarily generated variable that store and convert ASCII generated code **into** binary version.

$$\boldsymbol{Y = AC \rightarrow BC} \quad \text{.....(2)}$$

Y1 is the updated variable that applies S-box values over the binary converted data in equation 3.

$$\boldsymbol{Y1 = BC \rightarrow S\,box} \quad \text{.....(3)}$$

While equation 4, combine s-box generated bits with the key generated by the ElGamal key generation algorithm to make 8-bits of data and store it in Y2.

$$\boldsymbol{Y2 = (Sbox)\,U\,(K)} \quad \text{.....(4)}$$

$$\boldsymbol{Y3 = DNA} \quad \text{.....(5)}$$

$$\boldsymbol{Y4 = C} \quad \text{.....(6)}$$

Y3 store DNA encoding data which is ciphertext and is denoted with the C which is equal to Y4.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

4. Result and Analysis

This unit analyses the results on the bases of encryption time, decryption time, response time and communication time. Results are also studied for some security perspectives

Computational Time:

Computational time is the total amount of time taken by an algorithm to complete a specific amount of time. The table explains the time of key generation, response time, encryption time and decryption time for altered lengths and sizes of data:

File size (Bytes)	Encryption time (s)	Decryption time (s)	Key Generation time (s)
10	55	45	3
20	123	111	6.5
30	187	172	10
40	251	240	13.2
50	340	328	17
60	401	391	20.6
70	466	448	24

4.1 . Encryption Time Complexity

Encryption time means the time taken to convert plaintext into the cipher text during communication over the network. The encryption time consumed by the proposed scheme is shown in Figure 7 below for different length of data. The time is shown in seconds.

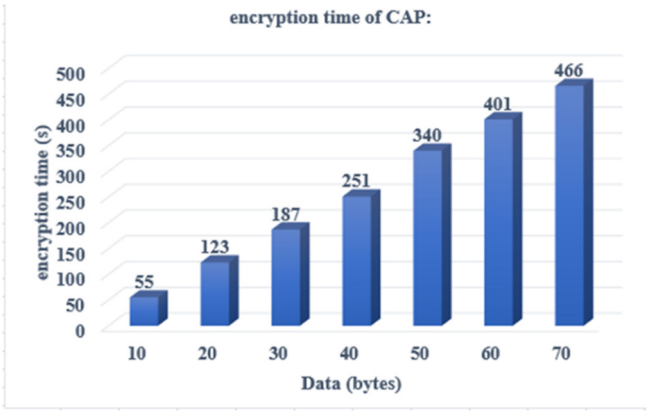


Figure 7. Shows an overview of Encryption Time.

4.2. Decryption Time Complexity

Decryption is the time required to convert cipher text into plain text. The encryption time taken by the proposed technique is shown in Figure 8 below for different data size. The time is shown in seconds.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

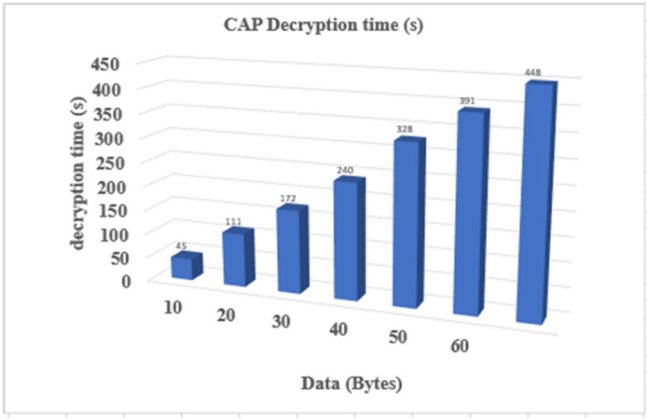


Figure 8. Shows an overview of Decryption Time.

4.3. *ElGamal Key Generation Algorithm*

The key generation time is the time which is taken by the algorithm for the generation of secret key while communication, on networks. The Figure 9 shows the key generation time of the proposed scheme:

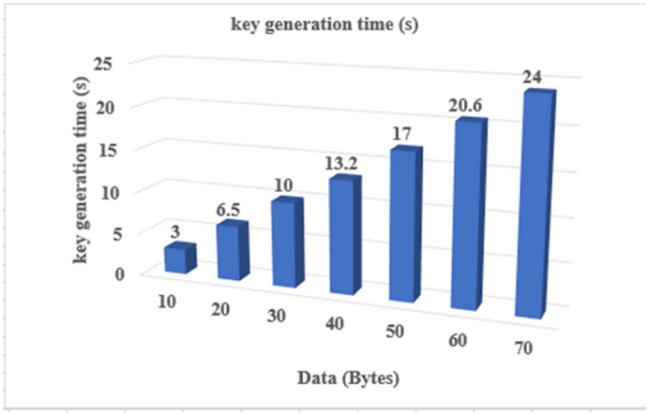
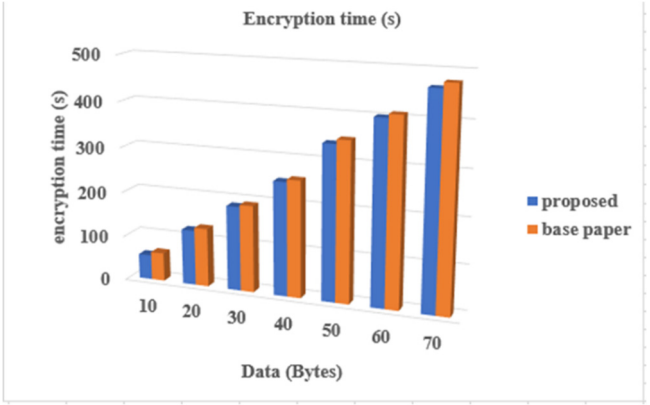


Figure 9. Shows an overview of Key Generation Time.

4.4. *Comparative Analysis*

The proposed CAP scheme is compared with existing Algorithms[1], [4], [15] on the basis of encryption and decryption time. The encryption time of the proposed scheme for the data file size of 10 bytes is 55 second and the decryption time is 45 seconds whereas existing algorithms[1], [4], [15], were taken 105 second for encryption of the file size of 10 bytes and 67 seconds are taken for decryption. This property will make proposed scheme less time consuming. The comparative results are shown in figures 10 and 11 below:



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

Figure 10. Shows Encryption Time Comparison Analysis.

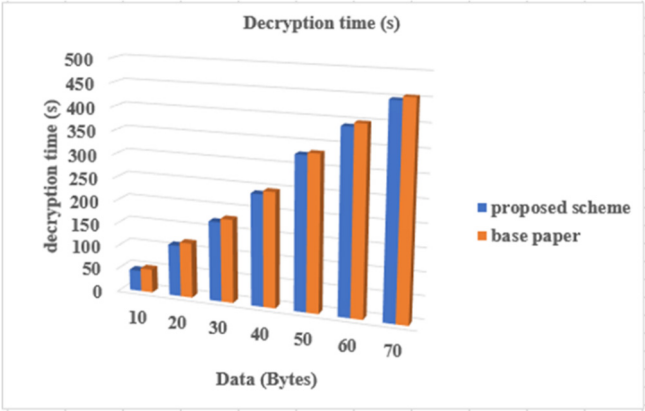


Figure 11. Shows Decryption Time Comparison Analysis.

4.5. Response Time

The response time is calculated to check how much time taken by the algorithm in communication over the network. In Figure 12, we provided response time of our proposed scheme. The response time increases as the amount of data increases. The values are calculated in seconds.

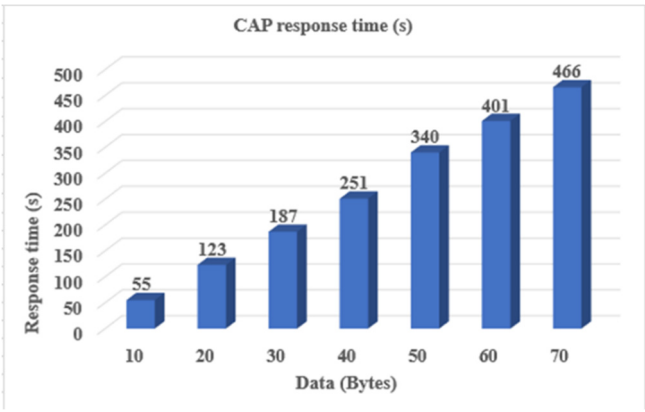


Figure 12. Shows an overview of CAP Response Time.

V. SECURITY

There are several parameters, calculated in order to check the protection of algorithm against multiple attacks. While performing cryptography, several attacks can destroy the network, which requires security mechanisms to protect the Network against these vulnerabilities. In [10], the researcher proposed Elliptic curve cryptography technique which enough security for manet but in another research article [11] the researcher proves that Elliptic curve cryptography technique can be attacked by collusion attack, so here our proposed cryptography technique provides security to manet against collusion attacks.

5.1. Collision Attack

The Collusion attack is kind of network attacks in which a node deliberately makes a private agreement with an attacker. The attacker can collect secret information from the system, and then attacks on the system in sophisticated ways by misusing wrong data inoculation through one or more cooperated node. The proposed CAP (Collusion attack prevention) scheme secures manet against collusion attacks. The situation of collusion attack presented in Figure 13:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 December 2023 doi:10.20944/preprints202312.1652.v1

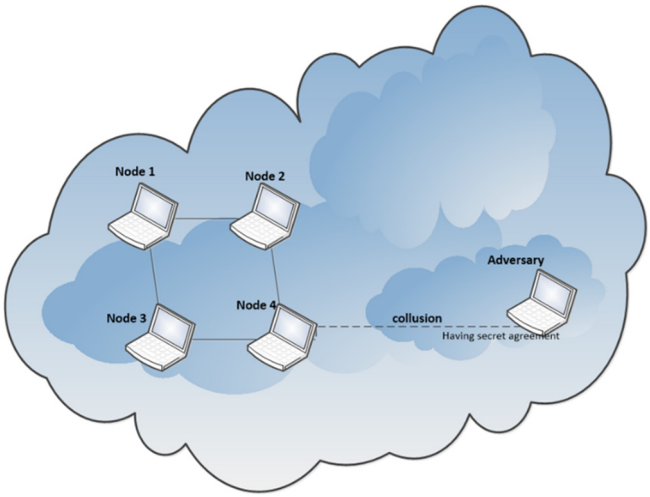


Figure 13. Shows an overview of Collison Attack.

5.2. *Man-In-Middle Attack*

Man-in-the-middle attack contains three actors. There is the attacker, the entity with which the attacker is trying to connect, and the "man in the middle," who is exploiting the victim's communications. In Figure 14, a clear picture of how this attack is not conceivable in proposed algorithm is given. Since man in the middle attack is conceivable, whenever the attacker recognized the private conversation between two connecting parties. The present situation is, if the attacker can collect the data being sent between the two parties, the acquired data will be encrypted. The encrypted data can only be decrypted if the key and the encryption algorithm is recognized. Meanwhile the private and the public key theory is used for the generation of keys, it is very tough to recognize the key because the private key is never sent over the network. If the key is not recognized, it becomes very challenging for an illegal person to recover the data. Symmetric key is shared over the network, where the attacker can find the key and can use it to recover the data. On the other side Asymmetric approach does not need the key to be sent above the network, which makes this strategy more protected against man in the middle attack.

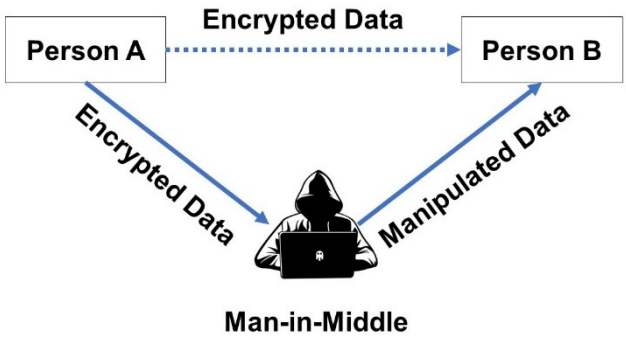


Figure 14. Shows an overview of MAN-in-MIDDLE Attack.

5. Conclusions

Previous security schemes are intelligent to identify several security attacks, but they did not analytically detect collusion attack. As proved with the authentic references, some sophisticated collusion attacks can occur in the presence of these schemes. This paper provides the CAP (collusion attack Prevention) technique for the protection of data in mobile ad hoc network. Proposed technique consists of ElGamal key generation scheme and DNA encryption algorithm. It provides 98% better encryption and decryption time as compared to the Base paper (RSA, CBSDV, ECC and

Acknowledgement packet based) techniques, also provides enough security for data over mobile ad hoc networks against collusion attacks.

References

1. B.Sowndarya, G.V.Suresh, O.SrinivasaReddy, and Dr.Sai Satyanarayana Reddy, "Enhanced Adaptive Acknowledgement for Mobile Ad Hoc Network," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5 (4), p. 4, 2014.
2. N. Sridevi1 and V. Nagarajan1, "A curve based cryptography for wireless security in MANET," *Clust. Comput.*, p. 9, Mar. 2018.
3. Markku-Juhani O. Saarinen, "Cryptanalysis of Block Ciphers Based on SHA-1 and MD5_," *_c Int. Assoc. Cryptologic Res.*, p. 9, 2003.
4. N. Sridevi, V. Nagarajan, and Senior Member, "Enhanced Secure Wireless Communication in MANETs," *Int. Conf. Commun. Signal Process.*, p. 6, Apr. 2017.
5. Yan Wang and Mohan Yang, "Higher Order Differential Cryptanalysis on the SHA-3 Cryptographic Hash Algorithm Competition Candidates," p. 9.
6. Ritu Aggarwal, "A Survey to Improve the Network Security with Less Mobility and Key Management in MANET," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. Volume 3, no. Issue 3, p. 7, Apr. 2018.
7. Santanu Sarkar and Subhamoy Maitra, "Side Channel Attack to Actual Cryptanalysis: Breaking CRT-RSA with Low Weight Decryption Exponents," *Int. Assoc. Cryptologic Res.*, p. 18, 2012.
8. Inderpreet Kaur, "A Framework to improve the Network Security with Less Mobility in MANET," *Int. J. Comput. Appl. 0975 – 8887*, vol. 167, p. 4, Jun. 2017.
9. Og˘ uzhan Ersoy, Thomas Brochmann Pedersen, Kamer Kaya, Ali Aydın Selçuk, and Emin Anarim2, "A CRT-based verifiable secret sharing scheme secure against unbounded adversaries," *Wiley Online Libr. Wileyonlinelibrarycom*, p. 9, Oct. 2016.
10. Rohit Kumar, Yashendra Shiv, Vimal Kumar, and Manoj Wairiya, "An Authentication Technique in Mobile Ad hoc Network using Elliptic Curve Cryptography," *2018 8th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu.*, p. 5, 2018.
11. Michael J. Wiener and Robert J. Zuccherato, "Faster Attacks on Elliptic Curve Cryptosystems," p. 11, 1999.
12. N Chaitanya Kumar, Abdul Basit, Priyadarshi Singh, and V. Ch. Venkaiah, "Lightweight Cryptography for Distributed PKI Based MANETS," *Int. J. Comput. Netw. Commun. IJCNC*, vol. Vol.10, No.2, p. 15, Mar. 2018.
13. David Adrian *et al.*, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," p. 13, 2015.
14. Muhammad Usman a, Mian Ahmad Jan b, Xiangjian He c, and Priyadarsi Nanda c, "QASEC: A secured data communication scheme for mobile Ad-hoc networks," *Future Gener. Comput. Syst.*, p. 7, May 2018.
15. Sankaranarayanan.S and Murugaboopathi.G, "SECURE INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORKS USING RSA ALGORITHM," *Int. Conf. Recent Trends Chall. Comput. Models*, p. 4, 2017.
16. Dr. Kartik Krishnan, "Attacks On the RSA Cryptosystem," p. 5, Apr. 2005.
17. V.Govindasaml, S.Sandosh, And C. Suraj Kumar, "kd2sa: key distribution scheme shuffling algorithm for heightened secure data transmission," *int. conf. comput. power energy inf. commun. iccpeic*, p. 6, 2016.
18. Jayanthi Chandrashekar and Arun Manoharan, "An Identity Based Key Management Technique for Secure Routing in MANET," p. 11, Jun. 2018.
19. T. R. Vedhavathy1 and M. S. K. Manikandan2, "Triple referee incentive mechanism for secure mobile adhoc networks," *Clust. Comput.*, p. 10, Jan. 2018.

A. Maheswary and Dr.S.Baskar, "Letter To Shape Encryption For Securing MANET Routing Protocols," *IEEE*, p. 4, 2016.

20. Mamta Martolia1, Priti Dimri2, and Nitin Arora3, "PIGPEN: A Novel Approach for Securing Data," vol. 80, p. 4, Oct. 2018.
21. Shahwar Ali, A Humaria, M Sher Ramzan, Imran Khan, and J Zakia, "An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. Vol. 16(6), p. 24, 2020.
22. T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band and A. Mosavi, "A Lightweight Genetic Based Algorithm for Data Security in Wireless Bosy Area Network," *IEEE Access*, vol. 8, pp. 1-10, 2020.

23. Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Jhanjhi, N., & Humayun, M. (2021). Robust cluster-based routing protocol for IoT-assisted smart devices in WSN. Computers, Materials & Continua, 67(3), 3505-3521.
24. Shahid, F., Ashraf, H., Ghani, A., Ghayyur, S. A. K., Shamshirband, S., & Salwana, E. (2020). PSDS–proficient security over distributed storage: a method for data transmission in cloud. IEEE Access, 8, 118285-118298.
25. Talwani, S., Singla, J., Mathur, G., Malik, N., Jhanjhi, N. Z., Masud, M., & Aljahdali, S. (2022). Machine-Learning-Based Approach for Virtual Machine Allocation and Migration. Electronics, 11(19), 3249.
26. Ramamoorthy, M., Qamar, S., Manikandan, R., Jhanjhi, N. Z., Masud, M., & AlZain, M. A. (2022, June). Earlier detection of brain tumor by pre-processing based on histogram equalization with neural network. In Healthcare (Vol. 10, No. 7, p. 1218). MDPI.
27. Khalil, M. I., Jhanjhi, N. Z., Humayun, M., Sivanesan, S., Masud, M., & Hossain, M. S. (2021). Hybrid smart grid with sustainable energy efficient resources for smart cities. sustainable energy technologies and assessments, 46, 101211.
28. Kok, S. H., Azween, A., & Jhanjhi, N. Z. (2020). Evaluation metric for crypto-ransomware detection using machine learning. Journal of Information Security and Applications, 55, 102646.
29. Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Jhanjhi, N. Z., & Humayun, M. (2021). Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN. Computers, Materials & Continua, 67(3).
30. Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022). AI-based wormhole attack detection techniques in wireless sensor networks. Electronics, 11(15), 2324.
31. Jabeen, T., Jabeen, I., Ashraf, H., Jhanjhi, N., Humayun, M., Masud, M., & Aljahdali, S. (2022). A monte carlo based COVID-19 detection framework for smart healthcare. Computers, Materials, & Continua, 70(2), 2365-2380.
32. Siddiqui, F. J., Ashraf, H., & Ullah, A. (2020). Dual server based security system for multimedia Services in Next Generation Networks. Multimedia Tools and Applications, 79, 7299-7318.
33. Ponnusamy, V. (Ed.). (2016). Biologically-Inspired Energy Harvesting through Wireless Sensor Technologies. IGI Global.
34. Ponnusamy, V., Jung, L. T., Ramachandran, T., & Zaman, N. (2017, April). Bio-inspired energy scavenging in wireless ad hoc network. In 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT) (pp. 1-5). IEEE.
35. Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Software-as-a-service security challenges and best practices: A multivocal literature review. Applied Sciences, 12(8), 3953.
36. S. Muzafar and N. Jhanjhi, "DDoS Attacks on Software Defined Network: Challenges and Issues," 2022 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2022, pp. 1-6, doi: 10.1109/ICBATS54253.2022.9780662.
37. Ilyas, Q. M., Ahmad, M., Zaman, N., Alshamari, M. A., & Ahmed, I. (2021). Localized text-free user interfaces. IEEE Access, 10, 2357-2371.
38. Kumar, K., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). A Survey of The Design and Security Mechanisms of The Wireless Networks and Mobile Ad-Hoc Networks. In IOP Conference Series: Materials Science and Engineering (Vol. 993, No. 1, p. 012063). IOP Publishing.
39. Hamid, B., Jhanjhi, N. Z., & Humayun, M. (2020). Digital Governance for Developing Countries Opportunities, Issues, and Challenges in Pakistan. In Employing Recent Technologies for Improved Digital Governance (pp. 36-58). IGI Global.
40. Alsaade, F., Zaman, N., Hassan, M. F., and Abdullah, A. 2014. "An Improved Software Development Process for Small and Medium Software Development Enterprises Based on Client's Perspective," Trends in Applied Sciences Research (9:5), pp. 254–261.
41. E. Ndashimye, N. I. Sarkar, and S. K. Ray, "A Multi-criteria based handover algorithm for vehicle-to-infrastructure communications," Computer Networks, vol. 185, no. 202152, Article ID 107652, 2020
42. Ray, S. K., Pawlikowski, K., & Sirisena, H. (2009). A fast MAC-layer handover for an IEEE 802.16 e-based WMAN. In AccessNets: Third International Conference on Access Networks, AccessNets 2008, Las Vegas, NV, USA, October 15-17, 2008. Revised Papers 3 (pp. 102-117). Springer Berlin Heidelberg.

43. Srivastava, R. K., Ray, S., Sanyal, S., & Sengupta, P. (2011). Mineralogical control on rheological inversion of a suite of deformed mafic dykes from parts of the Chottanagpur Granite Gneiss Complex of eastern India. Dyke Swarms: Keys for Geodynamic Interpretation: Keys for Geodynamic Interpretation, 263-276.
44. Ray, S. K., Sinha, R., & Ray, S. K. (2015, June). A smartphone-based post-disaster management mechanism using WiFi tethering. In 2015 IEEE 10th conference on industrial electronics and applications (ICIEA) (pp. 966-971). IEEE.
45. Chaudhuri A, Ray S (2015) Antiproliferative activity of phytochemicals present in aerial parts aqueous extract of Ampelocissus latifolia (Roxb.) planch. on apical meristem cells. Int J Pharm Bio Sci 6(2):99–108
46. Hossain, A., Ray, S. K., & Sinha, R. (2016, December). A smartphone-assisted post-disaster victim localization method. In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1173-1179). IEEE.
47. Airehrour, D., Gutierrez, J., & Ray, S. K. (2018). A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol. Journal of Telecommunications and the Digital Economy, 6(1), 41-49.
48. Ray, S. K., Ray, S. K., Pawlikowski, K., McInnes, A., & Sirisena, H. (2010, April). Self-tracking mobile station controls its fast handover in mobile WiMAX. In 2010 IEEE Wireless Communication and Networking Conference (pp. 1-6). IEEE.
49. Dey, K., Ray, S., Bhattacharyya, P. K., Gangopadhyay, A., Bhasin, K. K., & Verma, R. D. (1985). Salicyladehyde 4-methoxybenzoylhydrazone and diacetylbis (4-methoxybenzoylhydrazone) as ligands for tin, lead and zirconium. J. Indian Chem. Soc.;(India), 62(11).
50. Airehrour, D., Gutierrez, J., & Ray, S. K. (2017, November). A testbed implementation of a trust-aware RPL routing protocol. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE.
51. Ndashimye, E., Sarkar, N. I., & Ray, S. K. (2016, August). A novel network selection mechanism for vehicle-to-infrastructure communication. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 483-488). IEEE.
52. Ndashimye, E., Sarkar, N. I., & Ray, S. K. (2020). A network selection method for handover in vehicle-to-infrastructure communications in multi-tier networks. Wireless Networks, 26, 387-401.
53. Diwaker, C., Tomar, P., Solanki, A., Nayyar, A., Jhanjhi, N. Z., Abdullah, A., & Supramaniam, M. (2019). A new model for predicting component-based software reliability using soft computing. IEEE Access, 7, 147191-147203.
54. Hussain, S. J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N. Z., & Humayun, M. (2019, April). IMIAD: intelligent malware identification for android platform. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
55. Humayun, M., Alsaqer, M. S., & Jhanjhi, N. (2022). Energy optimization for smart cities using iot. Applied Artificial Intelligence, 36(1), 2037255.
56. Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.
57. Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In 2018 4th International conference on computer and information sciences (ICCOINS) (pp. 1-5). IEEE.
58. Wassan, S., Chen, X., Shen, T., Waqar, M., & Jhanjhi, N. Z. (2021). Amazon product sentiment analysis using machine learning techniques. Revista Argentina de Clínica Psicológica, 30(1), 695.

59. Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81
60. Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81.