International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 14 Issue 1 ǁ January 2026 ǁ PP. 161-172

An Efficient and Lightweight Chaotic Function with Key Exchange Protection for Man in the Middle Attack in Mobile Ad-hoc Networks (MANET)

Ashish Kumar Soni[1], Rajendra Gupta[2], AnkurKhare[3]

[1] *Department of Computer Science, Rabindranath Tagore University, Raisen, 464993, Madhya Pradesh, India.*
[2] *Department of Computer Science, Rabindranath Tagore University, Raisen, 464993, Madhya Pradesh, India.*
[3] *Department of Computer Science, Rabindranath Tagore University, Raisen, 464993, Madhya Pradesh, India.*

ABSTRACT
Independent communication in Mobile Ad-hoc Networks is widely recommended in Ad-hoc Networks to easily transmit data in undefined situations and make strong connections between sensors directly without any extra infrastructure. The MANET network's security issues are explored and solved by using high-security features by chaotic function. The chaotic cryptographic security can make help by generating highly complex pseudo-random numbers. The complexity is the first feature of the chaotic cryptosystem to get high-level security applications for the MANETs communication. In this paper, the Diffie-Hellman key exchange protection is used to establish the identification of user access links, and a chaotic function is added to generate highly complex situations for attackers to read the encrypted information. The lightweight speed of chaotic functions can also prevent protection without giving time to attackers. So both security features are combined as an Efficient and Lightweight Chaotic function with Key Exchange Protection (EL-CKP). The Efficient protection and lightweight speed of EL-CKP are analyzed better than existing AES and RSA security algorithms by comparative analysis of encryption time and the avalanche effect.

Keywords: *Chaotic Security, Key Exchange Protection, Avalanche Effect, Man in the middle attack.*

Date of Submission: 13-01-2026 Date of acceptance: 29-01-2026

I. INTRODUCTION

The Hybrid improved methods are solving a required essential role in building a lightweight setup in the whole world. In recent years, Hybrid solutions are enhanced and solved existing problems of security and privacy but many weak points are searched by the attackers day to day. These security and privacy weaknesses are pointed out by researchers for new improvements in security protection. The presented weaknesses are opened different prevention schemes of security for removing further security weaknesses. The MANETs have the special feature of self-configuration network protocols for establishing a connection with the wireless connection of PAN or LAN or WAN [1]. The available networks are worked for moving random connections in independent form without any extra protocols. The wireless MANETs are generating new security challenges in communication which are known as man-in-the-middle attacks [2].

The improved result is summarized to generate prevention by Diffie-Hellman key exchange for improving secure communication in Mobile Ad hoc Networks [3]. And two-way securities organized by Ping-Pong and LM05 QKD methods to prevent man-in-the-middle attacks [4]. The MANETs communication can be secure but if our organized protocols are achieved features (confidentially, availability, authentication, integrity, non-repudiation & access control). Then the communication can be guaranteed in a protected environment. The security goals are preceded by categorized algorithms cryptography, steganography, and watermarking. In digital media text, image, audio, and video are used as combined security features

The algorithms are presented with limited features only encryption or identification. The encryption features are used in [6, 10, 15, 16, and 17] but not used in any other security and some researchers work only on identifications in [12, and 14]. But some research is introduced combined features in [8, and 13].

So this paper is introduced combines features of security first identification achieved by the Diffie-Hellman key exchange method and second lightweight complex encryption and decryption achieved by chaotic function. Both security goals are designed for multiple features against attacks.

This paper is pieced as follows: Part 2 describes the literature work. Part 3 explores the proposed methodology in four subparts first steps of EL-CKP, the second chaotic key generation method, the third encryption method, and the fourth decryption method. Part 4 defines the result and analysis in three subparts first key sensitivity analysis, second cryptanalysis result, and third analysis for EL-CKP. Part 5 describes comparative analysis. Part 6 defines the conclusion and future work.

II. Literature Review

The many existing research is defined in this literature research to understand presented security goals. There are much research is done to find the solution to attacks and hide data with different security models to achieve the best results. Image cryptography is widely spread as a security application in digital media. The advanced solution hash table-based initial keys are used with the hyper-chaotic model to improve bit-level operations applied for secure image transmission [5]. Double encryption can generate double protection layers with the help of chaotic functions for key generation and encryption process [6].

The mapping can be one or multiple-dimensional but the image encryption scheme is an organized new concept of a one-dimensional fractional chaotic mapping mathematical model combined sine map and fraction procedures [7]. The Biometric authentication model is applied in many industrial areas and the Internet of Things. The combined security model with advanced encryption model AES and Chaotic function is used in different multiple objects, smart homes, and other areas [8].

A Deep learning and efficient communication can make a protection for medical sensitive images or data in unsafe wireless or wired network media. The loss function is applied to generate end-to-end encryption and decryption process for reliable recovered output [9]. The piecewise chaotic map is combined in 1D and 2D models to generate pseudo numbers and the XOR operation helped to generate shuffling in the image to protect against different attacks [10]. The aihara neural chaotic network pattern is optimized and compared after optimization to find a better pattern of security against attacks [11].

The key exchange protocols are studied and defined as all authentication protocols which is proposed by Diffie Hellman [12]. The proposed key exchange protocols can be more helpful for medical information to make authentication and AES security can achieve a better result in combined mode [13].

A reliable communication will have to establish identification protocols to manage unauthorized access. The absolute Diffie-Hellman protocol is introduced and generated strongly modified keys [14]. The lightweight speed and avalanche effect protocols can test the result of security of existing methods like DES protocols improved as triple DES protocols to make strong encryption results which analyzed in different key points of avalanche effect [15]. Same as the AES algorithm is too fast and gives a good encryption protocol but modified AES is proposed with analyzed good effect which is strictly compared with straight AES protocols [16].

The S-Box method is used to make more strong security of the AES method [17]. MANETs have many specialties to connect with the node in easy mode but many changes are accepted with MANETs with this easy specialty like multiple routers, distributed process, physical security, and other existing problems except this MANETs added in many areas like all emergency fields, education, sensors, home industry, and other modern required networks [18].

A comparative study can help to select better protocols to solve MANETs attacks. The DES and BAES security protocols for MANET are compared with used memory, process time, and avalanche result to select the best protocols in MANETs security [19]. There are many cryptography protocols and users must be confused about selecting the best cryptography scheme for personal data sharing in the MANETs network system. So the combined comparison is presented in different parameters and attacks also compared between RSA, 3DES, DES, AES, Two Fish, and blowfish security methods that compared results can be more helpful for various existing attacks because cryptographic methods are reliable but used in different security problems which are extremely explored [20]. Cloud services can help with memory utilization and connect to the centralized network system for less memory, less computation speed, less energy, and other application issues. Digital violation is increasing rapidly in cloud services like cybercrime hacking, attacks, and any different form of words, hear day to day in the whole world in all digital areas especially healthcare, home automation, banking, etc. In modern days users' data

are saved in the cloud to make easy access anywhere to think independent access in wild areas with demanding high-security parameters but many challenges are increased in cloud sectors. So the homomorphic cryptography can be helpful to manage these problems by generating strong security and a shielded environment in cloud services for every distributed user. The investigation of homomorphic cryptography method is analyzed and proven to find better security goals [21].

III. Proposed Methodology EL-CKP

This part describes EL-CKP by identification, chaotic key generation, encryption, and decryption method. The security method extends with the key exchange method and chaotic function for secure communication in MANETs against MITM attacks. The keys are calculated by chaotic functions in complex terms. The security method EL-CKP is figured in Fig 1.

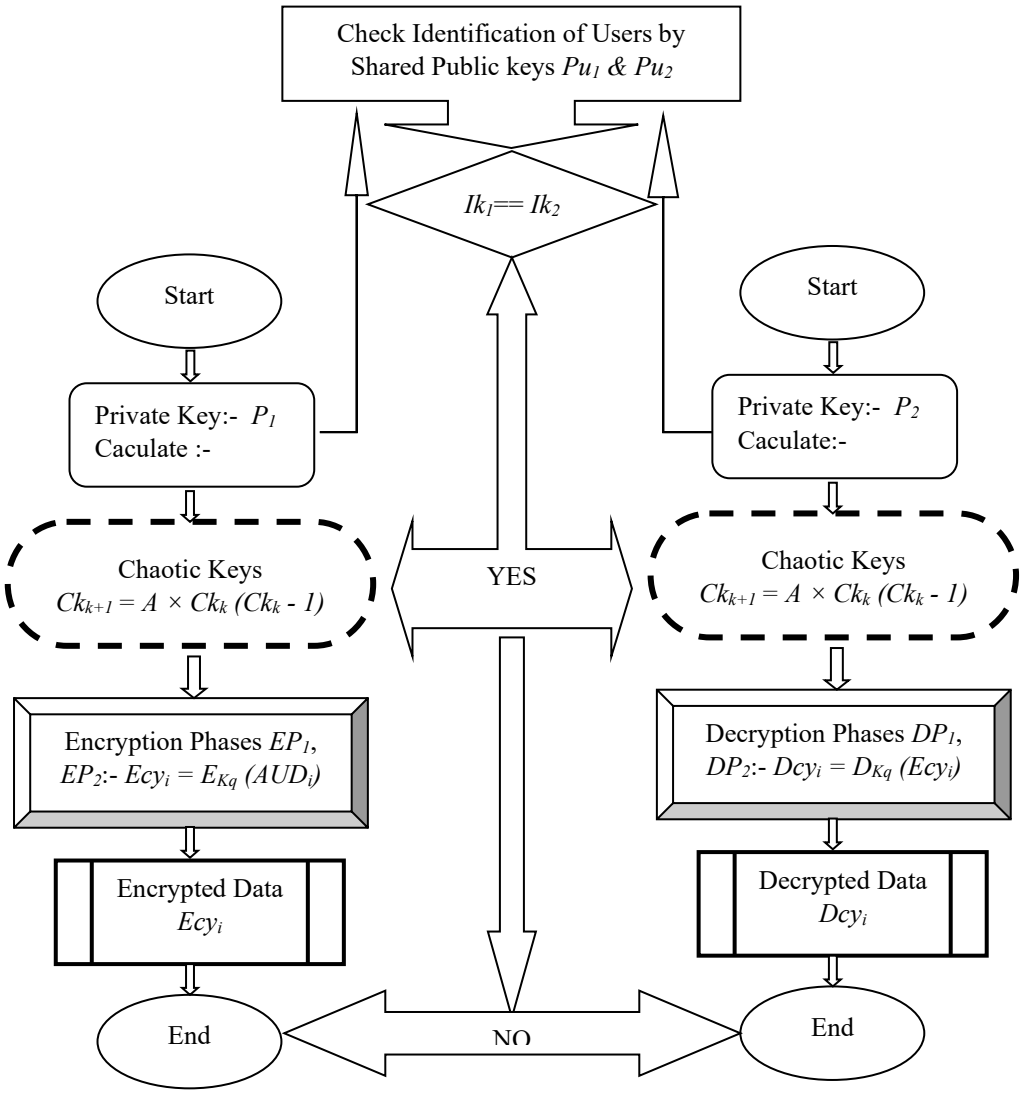

Fig 1 Proposed Methodology EL-CKP

a. Steps of EL-CKP

i. Sender steps

a. In the first step, the user decides on two global prime values G_1 and G_2. (G_1 and G_2 = prime numbers)
b. Sender decides any secret private key P_1.
c. Calculate public key Pu_1 for sharing globally by method $Pu_1 = mod(power(alpha, P_1), G_2)$. ($P_1 < G_2$, $alpha < G_2$, and $alpha$ = primitive root of G_2)

d. Check the right users by generating the identification key Ik_1. The identification key is generated by method $Ik_1 = mod(power(Pu_2, P_1))$. ($Pu_2$ = shared public key by the receiver)
e. If identification keys are equal on both sides sender and receiver then the next steps will execute otherwise the system will stop for the next step.
f. In the next step, the sender inputs user data UD_i and finds the ASCII value (AUD_i) of user data UD_i, AUD_i = ASCII (UD_i).
g. Calculate chaotic six Ck_{k+1} keys by method $Ck_{k+1} = A \times Ck_k (Ck_k - 1);$ *If* $(Ck_k > 255)$ *then* $Ck_k = Ck_k \bmod 256;$ (A= any integer value like 1,2,3,4…, Ck_k = intial value of chaotic method, and $q = 6$)
h. In the next encryption phases process in two-step EP_{1n} and EP_{2n}.
   I. First encryption step EP_{1n} run by method $EP_{1n} = Ck_k$ XOR Co_n. (Co_n = is a counter value of the system used for EL-CKP in terms $Co_n = (Co_n * A) + Ik_1$)
   II. The second encryption step EP_{2n} run by method $EP_{2n} = EP_{1n}$ XOR AUD_i.
i. Finally, get cipher ASCII data EP_{2n} to generate a cipher data Ecy_i, Ecy_i = ASCII (EP_{2n}).

ii. Receiver steps

a. In the first step, the user decided on two global prime values G_1 and G_2. (G_1 and G_2 = prime numbers)
b. The receiver decides on any secret private key P_2.
c. Calculate public key Pu_2 for sharing globally by method $Pu_2 = mod(power(alpha, P_2), G_2)$. ($P_2 < G_2$, $alpha < G_2$, and $alpha$ = primitive root of G_2)
d. Check the right users by generating the identification key Ik_2. The identification key is generated by method $Ik_2 = mod(power(Pu_1, P_2))$. ($Pu_1$ = shared public key by the receiver)
e. If identification keys are equal on both sides sender and receiver then the next steps will execute otherwise the system will stop for the next step.
f. In the next step receiver input encrypted data Ecy_i, and find the ASCII value ($AEcy_i$) of encrypted data Ecy_i, $AEcy_i$ = ASCII (Ecy_i).
g. Calculate chaotic six Ck_{k+1} keys by method $Ck_{k+1} = A \times Ck_k (Ck_k - 1);$ *If* $(Ck_k > 255)$ *then* $Ck_k = Ck_k \bmod 256;$ (A= any integer value like 1,2,3,4…, Ck_k = intial value of chaotic method, and $q = 6$)
h. In the next decryption phase process in two steps DP_{1n} and DP_{2n}.
   I. First decryption step DP_{1n} run by method $DP_{1n} = Ck_k$ XOR Co_n. (Co_n = is a counter value of the system used for EL-CKP in terms $Co_n = (Co_n * A) + Ik_2$)
   II. The second decryption step DP_{2n} run by method $DP_{2n} = DP_{1n}$ XOR $AEcy_i$.
i. Finally get decrypted ASCII data DP_{2n} generate a plain user data Dcy_i, Dcy_i = ASCII (DP_{2n}).

b. Identification Scheme with Diffie -Hellman Protocols

a. First, decide on two Global Prime Values G_1 and G_2.
b. Sender decides Private Key P_1 and generates Public Key Pu_1 by method $mod(power(alpha, P_1), G_2)$ in terms $P_1 < G_2$ and $alpha < G_2$ ($alpha$ is a primitive root of G_2). The same process is used for the receiver by deciding Private Key P_2 and generating Public Key Pu_2 by method $mod(power(alpha, P_2), G_2)$ in terms $P_2 < G_2$ and $alpha < G_2$.
c. Now calculate Indentification Key values Ik_1 and Ik_2 in both side by algorithm $Ik_1 = mod(power(Pu_2, P_1), G_2)$ and $Ik_2 = mod(power(Pu_1, P_2), G_2)$.
d. If calculated identification key values Ik_1 and Ik_2 are going on successfully or equal then the system processes the next step otherwise system must be off for the next process.

c. Chaotic Key Generation Method

a. The Chaotic Keys depend on Chaotic Function than chaotic keys $Ck_{k+1} \in \{A, Ck_k\}$.
   For 1 to q:

$$Ck_{k+1} = A \times Ck_k\ (Ck_k - 1);\quad If\ (Ck_k > 255)\ then\ Ck_k = Ck_k\ mod\ 256;$$

b. Add all the given parameters to generate pseudo-random keys which are created Ck_k to generate the keys $Ck_1, Ck_2 \ldots\ldots\ldots\ldots Ck_q$.

d. Encryption Method

a. The encryption method is processed by following the step $Ecy_i = E_{Kq}\ (UD_i)$. The data encoding process $E_{Kq}\ (UD_i)$ is processed by bitwise XOR operation in two phases EP_{1n} and EP_{2n} on user ASCII data AUD_i. The encryption phases are processed by following steps:
   I. First phase $EP_{1n} = Ck_k$ XOR Co_n.
   II. Second phase $EP_{2n} = EP_{1n}$ XOR AUD_i.

b. And, Finally, ASCII data EP_{2n} generates a cipher text data Ecy_i.

e. Decryption Method

a. The decryption method is processed by following the step $Dcy_i = D_{Kq}\ (Ecy_i)$.

b. The data decoding process $D_{Kq}\ (Ec_{yi})$ is processed by bitwise XOR operation in two phases of decryption DP_{1n} and DP_{2n} on encrypted ASCII data AEc_{yi}. The decryption phases are processed by following steps:
   I. Frist phase $D_{P1n} = C_{kk}$ XOR C_{on}.
   II. Second phase $D_{P2n} = D_{P1n}$ XOR AEc_{yi}.

c. And, Finally, ASCII data DP_{2n} generates a plain user data Dcy_i.

IV. Result and analysis

The performance result is introduced with complex chaotic six keys with the EL-CKP method. The performance result is applied in Conversion/Encryption Time and Avalanche Effects. The analysis result environment is performed by using Intel® Core(TM) i3-6006U CPU @ 2.GHz processor speed with x64- based processor, 4 GB RAM.

a. Key Sensitivity Analysis

The chaotic keys are too complex to search or calculate according to the chaotic terms. The chaotic keys are explored hard noticeable parts in the key parameters ($Ck_{k+1} \in \{A, Ck_k\}$):

$$Ck_{k+1} = A \times Ck_k\ (Ck_k - 1);\quad If\ (Ck_k > 255)\ then\ Ck_k = Ck_k\ mod\ 256;$$

Original Data:– “MM Kalam Sahab”. Key Parameters $\{A, Ck_k\}$ with Keys $\{Ck_1, Ck_2 \ldots\ldots\ldots\ldots Ck_q\}$ and key values A = chaotic value ;

i. Sensitivity of Calculated Condition Ck_k

It is analyzed that if any one minor changes are transforming in the given condition Ck_k like several numbers then the encrypted data are entirely transformed into a different form for the original data. All the transformation for $\boldsymbol{Ck_k}$ by changing a little bit of text to calculate different encrypted values is displayed in Table 1.

Table 1 *Sensitivity of Calculated Condition Ck_k*

Ck_k	A	Ck_{k+1}	Chaotic Keys (Ck_{k+1})	Encrypted Value
6	3	90,222,242,118,202,206	90,222,242,118,202,206,90, 222,242,118,202,206,90,222	□□-_°&/¶>_¨&+¶1
7	3	126,146,22,106,110,130	126,146,22,106,110,130,126, 146,22,106,110,130,126,146	¾R»¬□c□r»´□g□}
8	3	168,200,104,136,40,72	168,200,104,136,40,72,168, 200,104,136,40,72,168,200	ÅNÄ©D(ÅVÄ-D'
9	3	216,56,24,120,88,184	216,56,24,120,88,184,216,	øµ¾´Y4Øµ¦´]4×

			56,24,120,88,184,216,56	
10	3	14,34,38,122,254,18	14,34,38,122,254,18,14, 34,38,122,254,18,14,34	Îâ‹¼óâÂ‹¤÷âÍ
11	3	74,78,98,102,186,62	74,78,98,102,186,62,74, 78,98,102,186,62,74,78	□□Ï Vß¦®Ï¸VÛ¦¡

ii. Sensitivity of Initial Condition A

The sensitivity of initial condition *A* for the initial number is analyzed in Table 2 by using little changes in *A* initial condition then these modifications generate full changes in encrypted data. The given All the used changes can make different encryption and decryption output. So the sensitivity of the *A* initial condition is accepted without change in the process of key calculation, encryption, and decryption process.

Table 2 *Sensitivity of Initial Condition A*

Ck_k	*A*	Ck_{k+1}	Chaotic Keys (Ck_{k+1})	Encrypted Value
6	1	30,102,62,198,94,38	30,102,62,198,94,38, 30, 102,62,198,94,38,30,102	|1¢eP$1ºaP+
6	2	60,168,48,160,192,128	60,168,48,160,192,128,60, 168,48,160,192,128,60,168	/»Nµÿ²›N-ÿ¶”
6	3	90,222,242,118,202,206	90,222,242,118,202,206,90, 222,242,118,202,206,90,222	□□-_°&/¶>_¨&+¶1
6	4	120,32,128,0,0,0	120,32,128,0,0,0,120, 32,128,0,0,0,120,32	□Ñ□÷ÝÐ¥ñ□ïÝÔ¥þ
6	5	150,134,22,6,150,134	150,134,22,6,150,134,150, 134,22,6,150,134,150,134	0 Ý¦□□ Ý¾□□
6	6	180,40,144,160,64,128	180,40,144,160,64,128,180, 40,144,160,64,128,180,40	æſ]DZĻĦŭĮş]ǩĻDzǏŐ

b. Cryptanalysis Result

The security scheme can prove the security features of the method with the help of cryptanalysis protocols. The cryptanalysis protocols are analyzed by breaking the secret code of the organized scheme and uncovering the used possible encryption keys and original data as well.

i. Secret Data Only Attack

Parameters: $q = 6$, $A = 3$, $Ck_k = 6$, $Co_n = 31$.

Chaotic Keys: Ck_{k+1} {90, 222, 242,118, 202, 206}.

Given: Encryption Phases: EP_1, EP_2:- $Ecy_1 = E_{Ck}(UD_1)$, $Ecy_2 = E_{Ck\ 2}(UD_2)$,……., $Ecy_i = E_{Ck\ q}(UD_i)$ where q=1 to 6, $E_{Kq} = EP_1, EP_2(Ck_q)$.

Deduce:- Either UD_1, UD_2, UD_3, UD_4,…… UD_i.

$Ck_1, Ck_2, Ck_3, Ck_4, Ck_5, Ck_6$.

Example:

UD_1 = C then	$Ecy_1 = E_{Ck\ 1}(UD_1) = E_{90}$	C = D
UD_2 = CC then	$Ecy_2 = E_{Ck\ 1,2}(UD_2) = E_{90,\ 222}$	CC = DÀ
UD_3 = CCC then	$Ecy_3 = E_{Ck\ 1,2,3}(UD_3) = E_{90,\ 222,\ 242}$	CCC = DÀì
UD_4 = CCCC then	$Ecy_4 = E_{Ck\ 1,2,3,4}(UD_4) = E_{90,\ 222,\ 242,\ 118}$	CCCC = DÀìh
UD_5 = CCCCC then	$Ecy_5 = E_{Ck\ 1,2,3,4,5}(UD_5) = E_{90,\ 222,\ 242,\ 118,\ 202}$	CCCCC = DÀìhÔ
UD_6 = CCCCCC then	$Ecy_6 = E_{Ck\ 1,2,3,4,5,6}(UD_6) = E_{90,\ 222,\ 242,\ 118,\ 202,\ 206}$	CCCCCC = DÀìhÔÐ

The presented result is explaining that if any value of data is repeated one or more times in the original data, the encrypted data is changed in a different form for the repeated data C. The Encrypted data of text C resulting as the 1st text value is unrelated to C resulting in N time text value in the original data.

ii. Known Plain Data Attack

Parameters: $q = 6$, $A = 3$, $Ck_k = 6$, $Co_n = 31$.
Chaotic Keys: Ck_{k+1} {90, 222, 242,118, 202, 206}.
Given: Encryption Phases: EP_1, EP_2: UD_1, $Ecy_1 = E_{Ck1}(UD_1)$, UD_2, $Ecy_2 = E_{Ck2}(UD_2)$,……., UD_i, $Ecy_i = E_{Ckq}(UD_i)$ where q=1 to 6, $E_{Ckq} = EP_1, EP_2 (Ck_q)$.
Deduce:- Either Ck_1, Ck_2, Ck_3, Ck_4, Ck_5, Ck_6.

Example:

UD_1 = I then	$Ecy_1 = E_{Ck1}(UD_1) = E_{90}$	I = N
UD_2 = II then	$Ecy_2 = E_{Ck1,2}(UD_2) = E_{90, 222}$	II = NÊ
UD_3 = III then	$Ecy_3 = E_{Ck1,2,3}(UD_3) = E_{90, 222, 242}$	III = NÊæ
UD_4 = IIII then	$Ecy_4 = E_{Ck1,2,3,4}(UD_4) = E_{90, 222, 242, 118}$	IIII = NÊæb
UD_5 = IIIII then	$Ecy_5 = E_{Ck1,2,3,4,5}(UD_5) = E_{90, 222, 242, 118, 202}$	IIIII = NÊæbÞ
UD_6 = IIIIII then	$Ecy_6 = E_{Ck1,2,3,4,5,6}(UD_6) = E_{90, 222, 242, 118, 202, 206}$	IIIIII = NÊæbÞÚ

The analyzed result of the given example is shown many repeated data values with their related encrypted data. It is made too complex for breaking the key or the security scheme which is added for the encryption phase of the original data value for decryption. The calculated complex keys are produced in rare complex terms and strong barriers. The encrypted data of user data value I set up as the 1st data value is unrelated data value text I set up as the N time data value in the original data.

iii. Chosen Plain data Attack

Parameters: $q = 6$, $A = 3$, $Ck_k = 6$, $Co_n = 31$.
Chaotic Keys: Ck_{k+1} {90, 222, 242,118, 202, 206}.
Given: Encryption Phases: EP_1, EP_2: UD_1, $Ecy_1 = E_{Ck1}(UD_1)$, UD_2, $Ecy_2 = E_{Ck2}(UD_2)$,……., UD_i, $Ecy_i = E_{Ckq}(UD_i)$ where q=1 to 6, $E_{Ckq} = EP_1, EP_2 (Ck_q)$.
Where the cryptanalysis obtain to determine UD_1, UD_2, UD_3,…. UD_q; and q=1 to 6.
Deduce Either UD_1, UD_2, UD_3,…..... UD_q;

Example : UD_1 = OP then Encrypted data $Ecy_1 = E_{Ck1,2}(UD_1) = E_{16,20}$(OP) = HÓ
UD_2 = PO then Encrypted data $Ecy_2 = E_{Ck1,2}(UD_2) = E_{16,20}$(PO) = WÌ

It is made too complex a security scheme to decrypt the encrypted secret data. That is encrypted with similar keys, so finding keys is making too complex.

iv. Chosen Secret Data Attack

Parameters: $q = 6$, $A = 3$, $Ck_k = 6$, $Co_n = 31$.
Chaotic Keys: Ck_{k+1} {90, 222, 242,118, 202, 206}.
Given: Two step Encryption EP_1, EP_2:- Ecy_1, $UD_1 = D_{Ck1}(Ecy_1, Ecy_2, UD_2 = D_{Ck2}(Ecy_2),$,……., Ecy_q, $UD_q = D_{Ckq}(Ecy_q)$, where q=1 to 6, $D_{Ckq} = DP_1, DP_2(Ck_q)$
Deduce Either Ck_1, Ck_2, ... Ck_q.

Example : Ecy_1 = HÓ then Encrypted Data $UD_1 = D_{Ck1,2}(Ecy_1) = D_{16,20}$(HÓ) = OP
Ecy_2 = WÌ then Encrypted Data $UD_2 = D_{Ck1,2}(Ecy_2) = D_{16,20}$(WÌ) = PO

The chaotic keys are calculated with given parameters A, and Ck_{k+1}. The given keys are too sensitive and different to each parameter, so this concept is making complicated to deduce the keys by transforming the encrypted data and its decrypted original data.

c. Analysis for EL-CKP

The security method as an Efficient and Lightweight Chaotic function with Key Exchange Protection (EL-CKP) is measured with some existing security methods. The performance result is tested by speed and the avalanche effect. The EL-CKP is situated to make a very strong shield to cover sensitive data. The presented result is gratified with the given existing terms of security features by experimental result.

i. Conversion/Encryption Time

The conversion/encryption time of the EL-CKP method is located on the computation time. That is performed the key length, the complication of the EL-CKP security method, and the plain data size to be encrypted with different patterned encryption protocols. The result is given with different sizes of data files 6kb to 30 kb in 8 different sizes of data files and conversion/encryption time collected linearly from small to big size of data files in Fig 2.

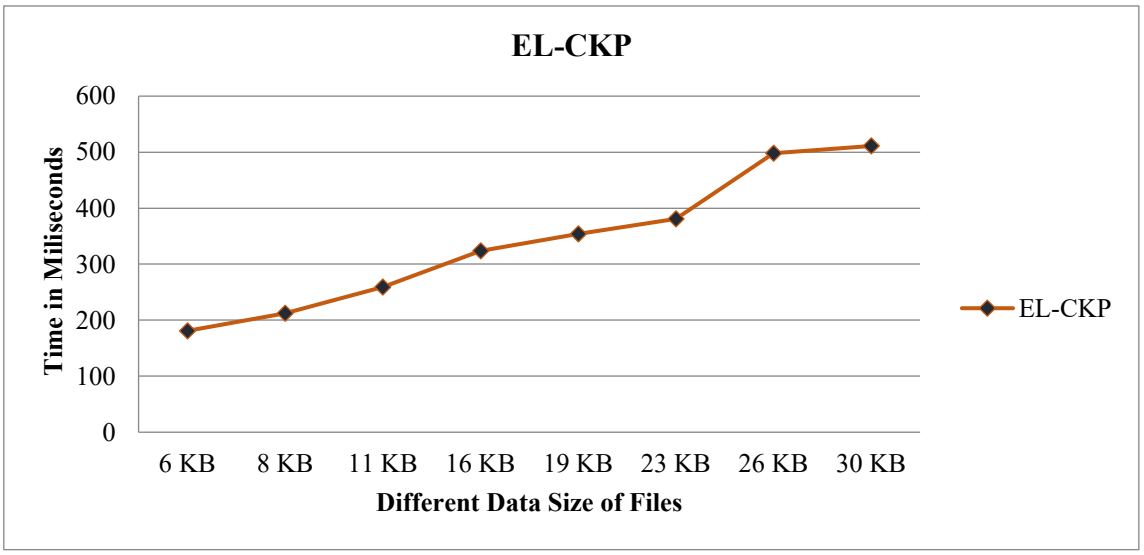

Fig 2 Different Data Size of Files VS Conversion/Encryption Time

ii. Protocol of Avalanche Effect

The Avalanche protocol is identified in [15] [16] [19] and resulted to make strong conversion of data at least 50% in the security scheme. The avalanche effect of the EL-CKP security method is the result of using the method:

$$A_f = \text{(changed total bits / present total bits in converted data)} \times 100\%;$$

Where the changed total bits = count the total number of bits converted; present total bits in converted data = count total bits in encrypted data:

The protocol of the avalanche effect is calculated by using XOR bit-wise operation between the encrypted data and the changed one-bit encrypted data. The bit-wise XOR operator can be helpful to count the number of 1's bit.

iii. The Avalanche Effect by Given Minor Data

The Minor data "MM Kalam Sahab" with their decimal values "77, 77, 32, 75, 97, 108, 97, 109, 32, 83, 97, 104, 97, 98" is engaged to calculate the result of avalanche effect with similar six keys "90, 222, 242, 118, 202, 206" for both minor data distorted a one single bit value "MM Kalam SahaB" with their decimal values "77, 77, 32, 75, 97, 108, 97, 109, 32, 83, 97, 104, 97, 66". Both minor data are converted with the same keys at both times.

Table 3 The Result of the avalanche effect by given minor data

Protocol	Ck_{k+1}	UD_n	UD_n In decimal	Ecy_i in decimal	Avalanche Effect
EL-CKP	90, 222, 242, 118, 202, 206	MM Kalam Sahab	77,77,32,75,97, 108,97,109,32, 83,97,104,97,98	74,206,143,96,246,2 55,102,238,143,120, 246,251,102,225	69/112 = 61.60 %
		MM Kalam SahaB	77,77,32,75,97, 108,97,109,32, 83,97,104,97,66	119,243,178,93,203, 194,91,211,178,69, 203,198,91,252	

The result of the avalanche protocol for the EL-CKP security method is shown in Table 3. The analyzed result of the avalanche effect after shifting one single bit in the minor data value is calculated at 61.60 %. That is a achieving good avalanche effect of the organized security method to make a guarantee to generate dissimilar encrypted data if any modifications are performed in the original data then the conversion of data must be dissimilar.

iv. The Avalanche Effect with different files by flipping one bit

The plain data file is added with data "MM Kalam Sahab" with their decimal values "77, 77, 32, 75, 97, 108, 97, 109, 32, 83, 97, 104, 97, 98" and their binary form "01001101 01001101 00100000 01001011 01100001 01101100 01100001 01101101 00100000 01010011 01100001 01101000 01100001 01100010" is engaged to calculate the result of avalanche effect with similar keys "90, 222, 242, 118, 202, 206" and their binary form "01111000 10001111 10010111 11110000 0011010 01011010" for distorted one single bit in diverse 11 data files. All the diverse one-bit of data files are produced with similar keys to convert encrypted data.

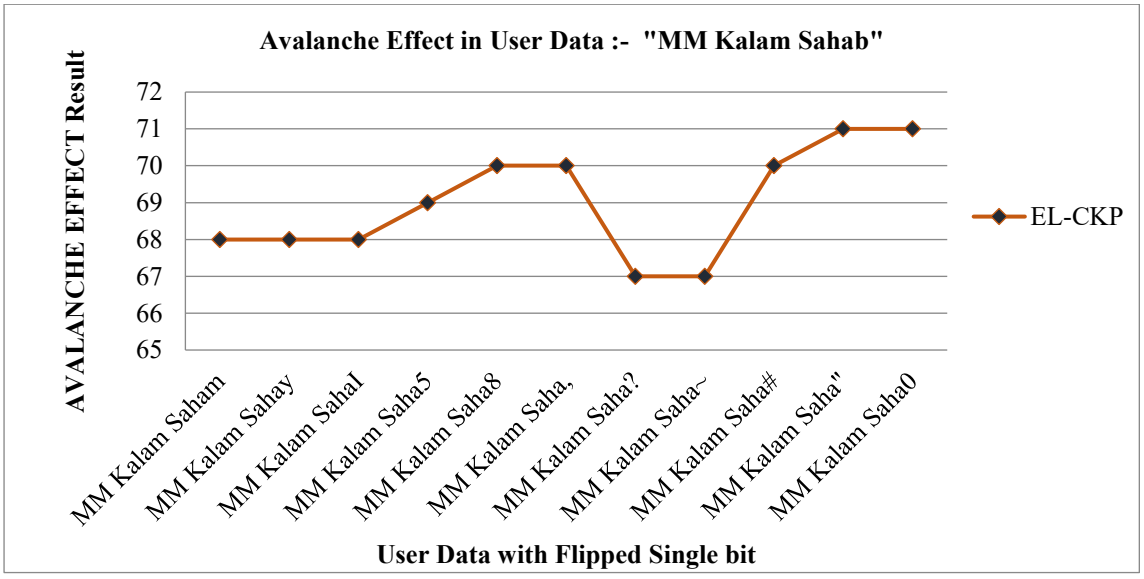

Fig 3 Avalanche Effect of EL-CKP Security method with different codes

The analyzed result is displayed in Fig 3 graphically to make the better avalanche effect by using similar keys in all 11 diverse data files. The security method is getting results above 50% by diverting a single bit of data files. The realized result is generating high-level security features for protecting data with better results of the EL-CKP security method to protect against unwanted users and man-in-the-middle attacks also.

V. Comparative Analysis

The analyzed result is shown with compared output based on different test protocols of the organized security method EL-CKP and compared with existing top security methods AES and RSA.

a. The Avalanche effect

The analyzed result is compared with the well-known security method AES to proven a better result of the given avalanche effect for finding another parameter of the encryption effect. So the analyzed result of compared result is analyzed between AES and the EL-CKP security method. Let the data "MMMrKalamSahabJi" of 16 Bytes with their decimal values "77, 77, 77, 114, 75, 97, 108, 97, 109, 83, 97, 104, 97, 98, 74, 105" and used similar keys in all 11 different data files.

The analyzed result of the avalanche effect is produced between AES and EL-CKP with 11 different data files by producing a minor distortion of a single bit in all 11 data files and the given result of encrypted data is displayed graphically in Fig 4. The displayed result of the avalanche effect is giving better results in comparison AES security method of EL-CKP with maximum avalanche effect to achieve better hybrid security of shielding data based on man-in-the-middle attack.

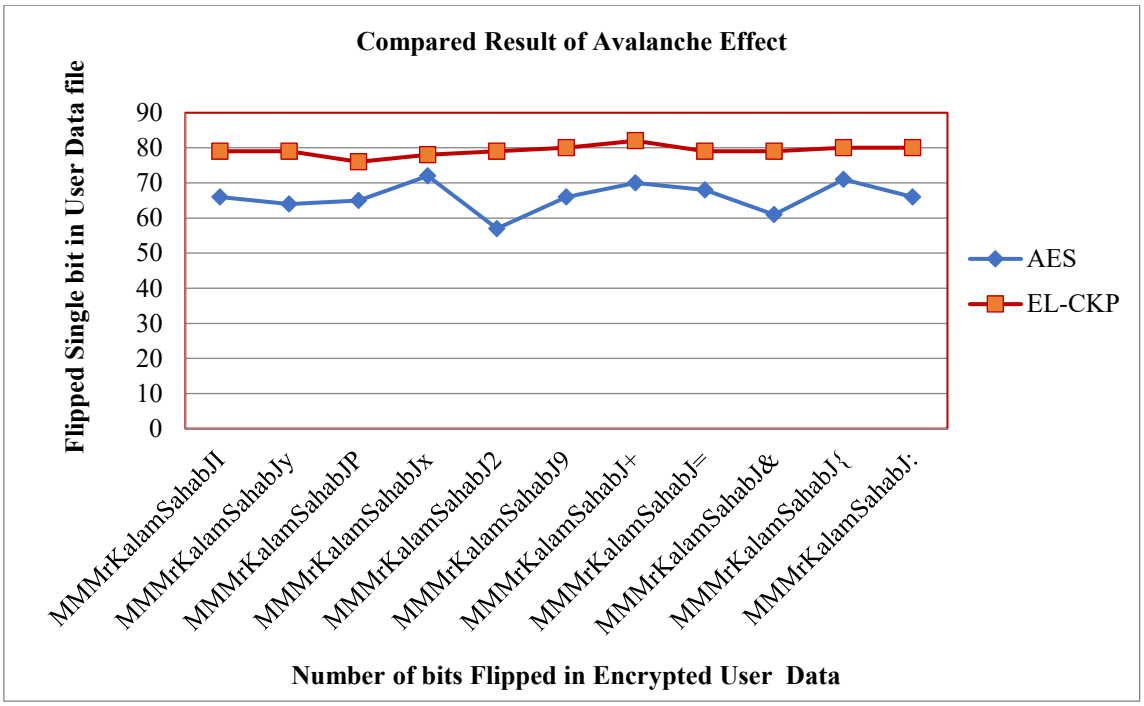

Fig 4 The analyzed result of the Avalanche Effect between AES and EL-CKP

b. The Analyzed Result of Process Time

The security method EL-CKP is compared with existing security methods AES and RSA by using plain data "MMMrKalamSahabJi" to calculate time in two section encryption time and algorithm running time between AES, RSA, and EL-CKP.

Table 4 Calculated Time between AES, RSA, and EL-CKP

Sn	Algorithm	UD_n User Data	UD_n in Decimal	Encrypted UD_n in Decimal	Encryption Time in second	Algorithm Runtime in second
1	AES	MMMrKalamSahabJi	77, 77, 77, 114, 75, 97, 108, 97, 109, 83, 97, 104,	164,180,27,159,15,52, 199,11,175,12,141, 255,148,176,155,105	0.069450	0.088456
2	RSA			121,121,121,229,124, 102,25,102,175,7,102, 26,102,32,171,150	0.098965	0.171537

3	EL-CKP		97, 98, 74, 105	245,2,26,66,145,251, 212,46,58,99,187, 242,217,45,29,89	0.006789	0.032375

The lightweight speed is presented in Table 4 of the EL-CKP security method with better fast results in comparison to AES and RSA security methods. The EL-CKP scheme is producing steps at light-weight speed to protect data with complex chaotic protocols. So the given result is finding the better speed of the proposed scheme EL-CKP.

VI. Conclusion and Future Work

A Mobile Ad-hoc Networks are used to find better connectivity in Ad-hoc networks most of the time in a distinct area with low cast steps. The chaotic function is producing complex values to find pseudo-random numbers for generating complex keys and not detectable parameters with key exchange protocol Diffie-Hellman for identification of required users during transmission in unsafe MANETs networks in the whole world. Both algorithms are used together to make efficient and lightweight speed in complex terms of encryption-decryption with better identification for the right users. All the parameters are too sensitive during the process of EL-CKP security method with a hybrid solution against MITM attacks in MANETs network.

The analyzed cryptanalysis attacks are tested for better responses to security applications. All the key sensitivity is tested with related concepts of security to generate sensitive keys. The Comparative analysis and tested results are awarding the better result of security features identification, lightweight chaotic keys, and encryption steps by the proposed methodology EL-CKP. The EL-CKP is compared with other most used security methods AES and RSA to present better results of the Avalanche effect and lightweight speed.

The MANET have security concerns and they need to combine security features. A single feature cannot manage new attacks. The combined security features are too helpful but at a lightweight speed. So the multiple security applications could be achieved by watermarking techniques in future research.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] N. Raza, M. U. Aftab, M. Q. Akbar, O. Ashraf, and M. Irfan, "Mobile Ad-Hoc Networks Applications and Its Challenges," Communication and Network, vol. 08, no. 03, pp. 1–6, 2016, doi: 10.4236/cn.2016.83013.

[2] A. Malik, A. Ahsan, M. M. Z. Shahdat and J. C. Tsou," Man-In-The-Middle-Attack: Understanding In Simple Words", International Journal Of Data And Network Science, pp.1-16, 2019. doi: 10.5267/j.ijdns.2019.1.001.

[3] J. Pan, C. Qian and M. Rigerud, "Signed (Group) Diffie-Hellman Key Exchange with Tight Security", Journal Of Cryptography, vol. 35, no. 4, pp.1-42, 2022. https://doi.org/10.1007/s00145-022-09438-y

[4] M. Pavicic, "How Secure Are Two- Way Ping-Pong and LM05 QKD Protocols under a Man-in-the-Middle Attack?", Entropy, vol. 23, no. 2, pp.1-10, 2021. https://doi.org/10.3390/e23020163

[5] X. Wang, X. Zhang, M. Gao, Y. Tian, C. Wang, and H. H. C. Iu, "A Color Image Encryption Algorithm Based on Hash Table, Hilbert Curve and Hyper-Chaotic Synchronization", Mathematics, vol. 11, no. 3, pp. 1-18, 2023. https://doi.org/10.3390/math11030567

[6] H. Mahalingam, T. Veeramalai, A. R. Menon, Subashanthini S., and R. Amirtharajan, ". Dual-Domain Image Encryption in Unsecure Medium—A Secure Communication Perspective", Mathematics, vol. 11, no. 2, pp. 1-23, 2023. https://doi.org/10.3390/math11020457

[7] S. Zhu, X. Deng, W. Zhang, and C. Zhu, ". Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding", Mathematics, vol. 11, no. 1, pp. 1-22, 2023. https://doi.org/10.3390/math11010231

[8] A. Altameem, P. P, Senthilnathan T, R. C. Poonia, and A. K. J. Saudagar, "A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0", Systems, vol. 11, no. 1, pp. 1-20, 2023. https://doi.org/10.3390/systems11010028

[9] K. Panwar, A. Singh, S. Kukreja, K. K. Singh, N. Shakhovska, and A. Boichuk, "Encipher GAN: An End-to-End Color Image Encryption System Using a Deep Generative Model", Systems, vol. 11, no. 1, pp. 1-15, 2023. https://doi.org/10.3390/systems11010036

[10] S. Askar, A. Alshamrani, A. Elghandour, and A. Karawia, "An Image-Encipherment Algorithm Using a Combination of a One-Dimensional Chaotic Map and a Three-Dimensional Piecewise Chaotic Map", Mathematics, vol. 11, no. 2, pp. 1-19, 2023. https://doi.org/10.3390/math11020352

[11] C. Liang, Q. hang, J. Ma, and K. Li, "Research On Neural Network Chaotic Encryption Algorithm In Wireless Network Security Communication", EURASIP Journal on Wireless Communications and Networking, pp. 1-10, 2019. https://doi.org/10.1186/s13638-019-1476-3

[12] M. R. Mishra and J. Kar, "A Study on Diffie-Hellman Key Exchange Protocols". International Journal of Pure and Applied Mathematics, pp. 1-12, 2019. doi: 10.12732/ijpam.v114i2.2

[13] Ermatita, Y. B. Prastyo, I. W. W. Pradnyana and M. Adrezo, "Diffie-Hellman Algorithm for Securing Medical Record Data Encryption keys", International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), IEEE, pp. 1-5, 2020. doi: 10.1109/ICIMCIS51567.2020.9354297.

[14] Aryan, C. Kumar and D. R. Vincent P M, "Enhanced Diffie-Hellman Algorithm for Reliable Key Exchange", ICSET IOP Conf. Series: Materials Science and Engineering, pp. 1-8, 2017. doi:10.1088/1757-899X/263/4/042015

[15] M. Chen, "Accounting Data Encryption Processing Based on Data Encryption," Complexity, pp. 1-12, 2021. https://doi.org/10.1155/2021/7212688.

[16] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande and E. O. Asani, "Modified Advanced Encryption Standard Algorithm for Information Security", Symmetry, pp. 1–16, 2019. http://dx.doi.org/10.3390/sym11121484.

[17] M., N. Kashyap, A. Aggarawal and T. Choudhary, "Security techniques using Enhancement of AES Encryption", IEEE International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), pp. 1-5, 2018.

[18] P. chitra and T. Ranganayaki, "A Study on Manet: Applications, Challenges and Issues", International Journal of Engineering Research & Technology (IJERT), vol. 8, no. 03, pp. 1-4, 2020.

[19] Srividya R and Ramesh B, "A Comparative Analysis of DES and BAES for MANET", International Journal of Advanced Research in Engineering and Technology, vol. 11, no. 6, pp. 1-10, 2020. doi:10.34218/IJARET.11.6.2020.073.

[20] Kumar K and Dr. K. Sasikala, "Comparative Study of Cryptographic Algorithms", International Journal of Engineering Research & Technology (IJERT), vol. 9, pp. 1-6, 2020.

[21] Devi P, Sathyalakshmi S, and V. Subramanian D, "A Comparative Study On Homomorphic Encryption Algorithms For Data Security In Cloud Environment", International Journal of Electrical Engineering & Technology, vol. 11, no. 2, pp. 1-10, 2020.