IMPROVED AES FOR KEY GENERATION IN STREAM CIPHER FOR MANET SECURITY APPLICATION

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of

MASTER OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted By

MANSI SHARMA

801561017

Under Supervision of

Dr. Alpana Agarwal

Associate Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY, PATIALA, PUNJAB

JUNE, 2017

DECLARATION

I, Mansi Sharma hereby declare that the work presented in this thesis entitled "Improved AES for key generation in stream cipher for MANET security application" in partial fulfillment of the requirement for the award of degree of Master of Engineering submitted at Electronics and Communication Engineering, Thapar University, Patiala is an authentic record of work carried out under supervision of Dr. Alpana Agarwal, Associate Professor and Head, ECED, Thapar University, from January 2017 to June 2017. The matter presented in this thesis has not been submitted either in part or full to any other university or institute for the award of any other degree.

Mansi

Date: August 10, 2017.

Mansi Sharma
801561017

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

Alpana

Date: Aug. 10, 2017

Dr. Alpana Agarwal
Associate Professor

ii

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to Dr. Alpana Agarwal, Associate Professor and Head of Department, Electronics & Communication Engineering Department, Thapar University, Patiala for her patient guidance and support throughout the Literature Survey. I am truly very fortunate to have the opportunity to work with her. I found this guidance to be extremely valuable. I am also thankful to PG coordinator Dr. Hemdutt Joshi, Associate Professor, Electronics and Communication Engineering Department. I would like to thank entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encouragement and I admire their determination and sacrifice.

Mansi Sharma

ABSTRACT

Mobile ad hoc network comprise of network of nodes which are basically either mobile devices which communicate or routers used for forwarding data to these nodes. MANETs are deployed in many applications such as military services, in collaborative tasks in business environment, localized communication, even in case of emergency situations of disaster relief and rescue operations where infrastructure based networks fails to work or get damaged. However, MANETSs are also vulnerable to various attacks such as Black hole attack, replay attack *etc.* since there is no boundary predefined for the network and absence of central authority requires each node to participate and manage the network. So, Security of each node and encrypting data transferred through these nodes is the major requirement today's network. To secure secret information, cryptography comes into the picture where both stream and block ciphers algorithms are preferred. Work related to key generation and various encryption algorithms has been studied.

The proposed work includes the improved and optimized (in terms of memory) encrypting algorithm which is derived from AES algorithm. In the improved AES algorithm, on the basis of using Rijndaels substitution box and dynamic shifting principle security is achieved as equivalent to AES. To analyse the security of AES and improved AES, performance analysis is done on the basis of Correlation and Avalanche Effect properties.

Also, AES and Improved AES algorithm is used as an application for key generation with some improvements by reducing complexity and producing equivalent randomness for stream cipher because MANETs transmits packets of continuous streams. In the stream cipher overall security depends on randomness of key and Input parameters. So, for each packet random IV is generated and secret key derived from IV using non-linear function to produce randomness in the pseudo ransom number generation procedure for key generation. Moreover, comparative analysis is done with existing A5/1 stream cipher for key stream generation by pseudo random number generator using NIST key generation statistical analysis .The results show that improved AES algorithm provides equivalent security as compared to AES algorithm with less memory and execution time consumable. Also, its application for key generation also passed NIST statistical key generation test.

TABLE OF CONTENTS

Sr. No **Name of Chapters** **Page No**

Declaration……ii

Acknowledgement……iii

Abstract……iv

List of figures……vii

List of tables……viii

Chapter1 Introduction……1

*1.1*Overview of Wireless Network……1

1.2 Overview of MANETs……2

1.3 Characteristics of MANETs……3

1.4 Advantages of MANETs……4

1.5 Security Issues in MANETs……4

1.6 Security Goals of MANETs……7

1.7 Overview of Cryptography……8

1.7.1 Design Constraints in Cryptography……9

1.7.2 Block Diagram of Encryption and Decryption in Cryptography……9

1.7.3 Types of Cryptography……10

1.7.4 Symmetric Key Cryptography……10

1.7.4.1 Block Cipher……10

1.7.4.2 Stream cipher……11

1.8 Overview of Key Generation in Stream Cipher ……13

1.9 Overview of Cryptography in MANETs ……14

1.10 Random Number Generator……15

1.11 Outline of Thesis……16

Chapter 2 Literature Survey……18

2.1 Survey on Key Generation……18

2.2 Survey on Encryption Algorithm……19

Chapter 3 Problem Formation and Objective……21

3.1 Gaps from Literature Survey……21

3.2 Objectives……22

3.3 Methodology……22

Chapter 4 Simulation of Proposed Algorithm and Performance Analysis……..*24*

4.1 Overview of AES…….…….....*24*

4.2 Mathematical modelling of AES……...*26*

4.3 Improved AES for MANETs……....*27*

4.3.1 Analysis of Correlation and Avalanche test on AES and Improved AES……..*28*

4.4 AES as application in Key Generation Mechanism……..*34*

4.4.1 Statistical Tests for Key Generation……....*35*

4.4.2 Analysis of Randomness of Key Generated……....*36*

Chapter 5 Conclusion…….……..*37*

Reference……..……..*38*

List of Publications…….…….....*41*

LISTS OF TABLES

Sr. No	Table Details	Page No
Table 1.1	*Comparison of Infrastructure and Infrastructure less Network……..*	*2*
Table 1.2	*Comparative Analysis of Block And Stream Cipher……*	*13*
Table 4.1	*Parameters for AES-128, AES-192, AES-256…….*	*26*
Table 4.2	*Comparative Analysis of Correlation and Avalanche effect of AES and Improved AES…….*	*30*
Table 4.3	*Statistical Test for randomness of Key Generation Techniques……*	*36*

LISTS OF FIGURES

Sr. No	Figure Details	Page No
Figure 1.1	*Infrastructure based Network* ……	*1*
Figure 1.2	*Infrastructure less Network*……	*2*
Figure 1.3	*Classification of Attacks on MANETs* ……	*5*
Figure 1.4	*Black hole Attack*……	*6*
Figure 1.5	*Wormhole Attack*……	*6*
Figure 1.6	*Replay attack*……	*7*
Figure 1.7	*Block diagram of Encryption and Decryption*……	*9*
Figure 1.8	*Synchronous stream cipher*……	*12*
Figure 1.9	*Self-synchronous stream cipher*……	*12*
Figure 1.10	*Block diagram for different phases of stream cipher* ……	*14*
Figure 1.11	*Encryption Module of Data Stream in MANETs* ……	*15*
Figure 1.12	*Pseudo-Random Number Generators*……	*16*
Figure 3.1	*Flow chart of design methodology of proposed work*……	*23*
Figure 4.1	*AES (Advanced Encryption Standard) process*……	*25*
Figure 4.2	*Pseudo code of AES and Improved AES*……	*27*
Figure 4.3	*Block Diagram of Improved AES*……	*28*
Figure 4.4	*Correlation Test of AES and Improved AES*…….....	*33*
Figure 4.5	*Avalanche Test for AES and Improved AES*…….....	*33*
Figure 4.6	*Key generation Mechanism by PRNG*……	*34*
Figure 4.7	*Statistical Test for Key Generation Techniques*……	*36*

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF WIRELESS NETWORK

With hike in the demand of connecting the mobile devices in the corporate world and due to heavy internet traffic to be transmitted, wireless network is an attractive way of data communication. Even for automation coming up in homes, military services, wireless networks are preferred for increasing the efficiency of network access [1]. A large number of nodes gather together to form a wireless network for transmission of useful information through wireless media. Wireless networks are collection of self- organized nodes which are mainly classified as

- Infrastructure based Network: Infrastructure based network supporting a central authority is more vulnerable to denial of service attack as attack at a single point can disrupt the working network as shown in Figure 1.1.

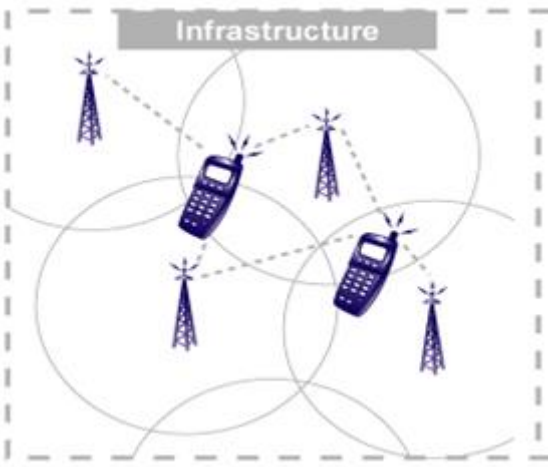

Figure 1.1 Infrastructure based Network

- Infrastructure-less Network: In Figure 1.2 shows an infrastructure-less network are the ones where there is no centralized node such as MANETs (Mobile Ad-hoc networks) which is temporarily designed network with no previously designated infrastructure [2]. The comparative analysis between infrastructure and infrastructure-less network is done in Table 1.1which shows infrastructure less network are more versatile because of decentralised node and each node works as host and router.

Figure 1.2 Infrastructures-less Network

Table1.1 Comparison of Infrastructure and Infrastructure-less Network

.

Infrastructure based Network	**Infrastructure-less Network**
Require a centralized node for devices to communicate with each other.	Decentralized network *i.e.* devices directly connect to each other.
Expensive since require a central access point.	Less Expensive as cost of access point is reduced.
Non-scalable as nodes are already authenticated to be part of a network and no further nodes can be added once the infrastructure is designed.	Scalable since can add more nodes if desired.
Large no of users are can be connected.	Beneficial when handful devices are to be connected.
Less resource requirement as fixed amount resources to be used are already assigned to infrastructure based network.	More resources desired as network layout change when devices move around.

1.2 OVERVIEW OF MANETS

MANETs is an autonomous system that lies in the category of infrastructure less network, which does not include a central authority mechanism to aid the communication between mobile nodes. MANETs provide device portability, as the infrastructure is small in size and low cost is required to maintain, it is also more convenient and powerful to aid devices with high mobility. So, MANETs can provide seamless connectivity in between devices which are either embedded in automobiles or for smart phones, smart sensors, and hand-held computers [2].

MANETs form a simple infrastructure consisting of mobile nodes that exchange data or packets using radio channels. MANETs can be characterized by types of ad-hoc network routing protocols that decides how to route the data packets between two communicating devices with no familiarity with the network topology:

- **Pro-active routing:** Proactive routing periodically creates a routing table for destination node and updates nearby nodes that provides route to the destination.
- **Reactive routing:** Reactive routing sends the request message for route on the network to find the routes which can creates high latency and excessive burden on the network.
- **Hybrid routing:** Hybrid routing initially establishes some active routes and further on demand develops more routes by reactive flooding [3].

1.3 CHARACTERISTICS OF MANETS

In wireless network, MANETs require following characteristics:

- **Network Infrastructure:** Mobile ad-hoc network has no previously defined infrastructure and nodes play the major role in management of network including transmission of information using direct or indirect contact of sender and receiver, providing security to information to be transmitted. Mobile ad-hoc network is an amorphous network where nodes can join and leave the network and nodes cooperate with other nodes to communicate in order to perform functions such as routing and providing security.
- **Network Topology:** Nodes form a dynamic and temporarily linked topology in MANETS where they are free to move with different speeds and establish their own network. Mobile ad-hoc network has an unstable topology which is unpredictable since nodes are mobile and unrestricted.
- **Self–organization:** To avoid an attack at a single point, MANETs do not depend on central control authority. They form a self-designed network where each independent node can behave as both a router and a host.
- **Limited resources**: In comparison to the wired network, MANETs have limited memory, computational and energy resource. Nodes in MANETs are mobile, they are operated by battery, and small CPU is used to satisfy low cost requirement. Thus, MANETS can easily substitute large wired network in case of power failure.
- **Poor Physical Security:** There is high probability of adversary compromising any node in the network since these nodes are mobile and can be easily stolen or lost. Analysis can be easily done on theses nodes to identify any secret information [4].

1.4 ADVANTAGES OF MANETS

- Variable size network.
- An easy connection to internet is available since wireless router is not required so MANETs are more affordable than conventional networks.
- Low cost for maintenance since cost for infrastructure is eliminated.
- Device portability.
- Provide services to high mobility devices.
- MANETs are scalable networks as more nodes can be added to the network when desired.
- Independent from central authority as nodes can themselves act as routers.[5]

1.5 SECURITY ISSUES IN MANETS

In MANETs, nodes use intermediate nodes to transmit packets which are not in direct contact by wireless transmission, which can make mobile ad-hoc networks vulnerable to passive attack and active attack. Passive attacks are where attacker does not manipulate the data being transmitted but acquire all the secret information needed by unauthorized listening which is not easily detected. These can be eavesdropping and analysis and monitoring of traffic which can further exploit network by other attacks. On the other hand, in active attack data being transmitted is modified or destroyed or network is disturbed by some intruded signal. These can be further defined as internal or external attacks. Threats occurring from internal nodes are not much easily detected since these nodes are authorized to participate in the network causing black-hole, replay, wormhole, jellyfish attack as these nodes behave such as [3]

- Failed nodes affect the ad-hoc network as they are unable to perform an operation, due to some environmental affects or power failure. Due to these failed operations, information about the broken links is not forwarded and cause a lot of data loss.
- Badly failed nodes perform incorrect operations causing false data injection into the network, which follows correct format but incorrect data and affect the integrity of the network.
- Malicious nodes purposely attack the network by disturbing the data.
- Selfish nodes attack the network by exploiting the routing mechanism for their own good by either packet dropping or by partial dropping which is difficult to detect and prevent [2].

External attacks occur because of nodes which are not authenticated for a particular network and are outside the range of a particular network. E.g. flooding or spoofing attack [1].

Securing the mobile ad-hoc network from various attacks and providing protection to the information transmitted is one of the major concerns. An attacker can disrupt the network traffic malicious nodes inject themselves in the path between the source and destination and thus control the network traffic flow. Some of the attacks classified as shown in Figure 1.3 are discussed below:

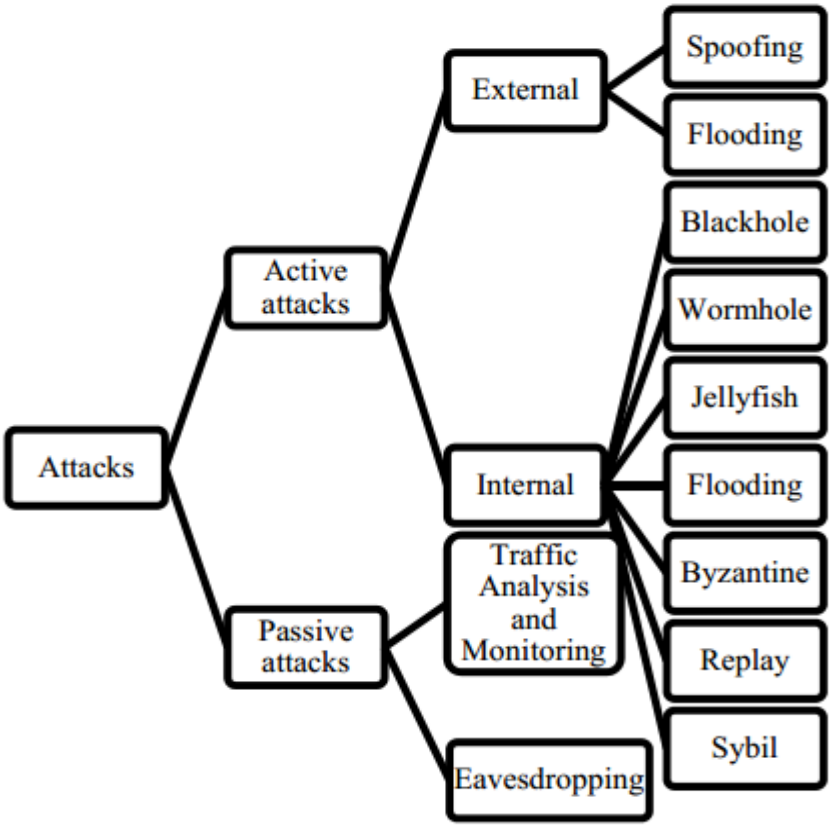

Figure 1.3 Classifications of Attacks on MANETS

- **Black hole Attack:** Black Hole attack as shown in Figure 1.4 is an internal attack where malicious nodes advertise that it can provide secure and shortest path to destination node. It claims to have an optimum route to destination with minimum hop count and highest destination sequence number. When S node desires to transmit data to D node, it requires a route discovery method. When M malicious node receive the request message ,it immediately responds and if the reply reaches the source node S before any other response, it ignores other responses send packet through M node which shows its malicious behaviour and drops all the packets instead of forwarding them.

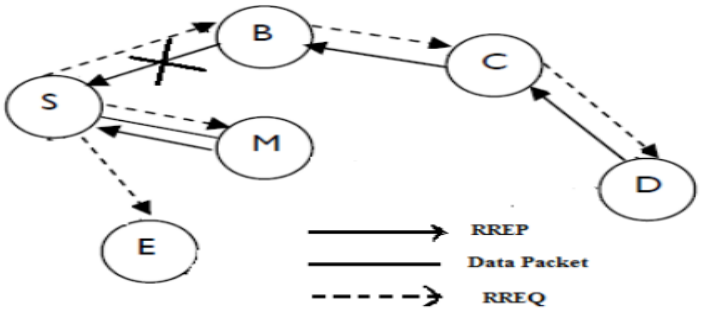

Figure 1.4 Black hole Attack

- **Wormhole Attack:** In this attack as shown in Figure 1.5, a malicious node make contact with other malicious node and form a tunnel between them which is known as wormhole. Any data packet received is tunnelled to other malicious node immediately for example, malicious node X and Y form tunnel in the network. When source node S sends the RREQ request message on the network to find optimum rote for destination node D , X node with Y node because of high speed tunnelled path give immediate response to source node, thereby causing source node to select <S-A-X-Y-B-D> route as an optimal route for transmission and invalidates the other route <S-C-H-E-F-G-D>. This will cause all the data packets to get lost in wormhole tunnel.

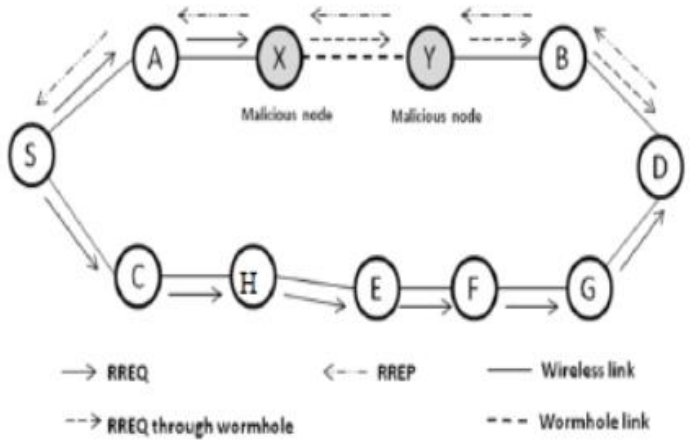

Figure 1.5 Wormhole Attack

- **Replay attack:** In replay attack, the attacker retransmits the message packets again and again which are already received and are invalid for every user, only to increase the network traffic. Other nodes start updating their routing table because of these invalid packets transmission requests, which damages the complete routing process in network as shown in Figure 1.6.

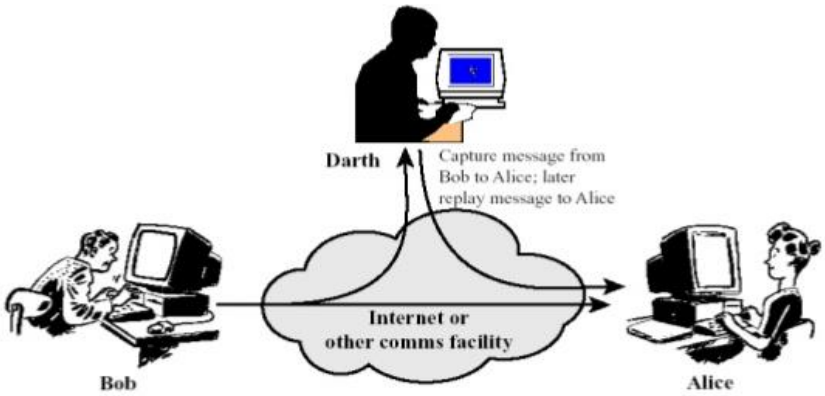

Figure 1.6 Replay attack

- **Flooding attack:** Malicious node inject false data packets with wrong information of destination address or request for non-existing addresses in the network to consume maximum resources and bandwidth available in this transmission. Since MANETs is a resource constraint network, during this attack, legitimate users are unable to use resources such as memory and battery.
- **Jellyfish Attack:** Jellyfish attack is similar to black hole attack only it is difficult to detect since the attacker behave following the rules of routing protocol. In this attack ,malicious node authenticates itself as a sober node and become part of network, then it modifies the sequence of the message packets and inject jitter in the network and produces delay in sending packets or either drop them which affects the throughput of the network.
- **Sybil Attack:** In Sybil attack, malicious nodes either create multiple identities of a single node, known as Sybil nodes. These multiple identities can be easily used by malicious node to have fake identity of a legitimate node and can cause other attacks using this sober impression of legitimate node in the network. The packets are easily received using this identity and then disturbing the communication in the network [1].

1.6 SECURITY GOALS OF MANETS

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network requirement.

- **Confidentiality:** Confidentiality assures protection of routing information of nodes which further protects leakage of other secret information of network and geographic area. It ensures protection of information to be transmitted from MANETs from any unauthorized party.

- **Integrity**: Integrity prevents information to be transmitted from corruption as it allows any modification by only authorized party and in some authorized manner.
- **Authentication:** A formal authentication is a key requirement of security, only authorized party or nodes are allowed to participate in communication in MANETs and can access any routing information or resources.
- **Availability:** Availability refers to all routing information, resources and services are available when desired to nodes and authorized users. Without much processing time, information to reach a particular node should be easily available on demand. MANETs should able to provide any data or service even in case of denial of service attack.
- **Dependability & Reliability:** In case of emergency, MANETs should provide alternate path for transmission and should maintain functioning of network even if some nodes are disturbed [2].

1.7 OVERVIEW OF CRYPTOGRAPHY

Cryptography is a method of encoding messages to convert them to non-readable format. It is the method of hiding information in insecure environment. Cryptography helps to secure sensitive data and transmit it securely over the network so that data is understood only by the intended recipient .Cryptography is used in many aspects for security and for many applications such as securing computer passwords, for secure network communication, encrypting data for applications such as WhatsApp, security in Smart Grids. Cryptography helps to achieve security by using mathematics to encrypt the data at sender side and decrypt the data at the receiver side. Cryptography is the science of securing data while cryptanalysis is analysis on breaking secure communication. Cryptology includes cryptography and cryptanalysis [6].

A Cryptography Algorithm works with the combination of key and plaintext to produce the cipher text. Some of the important terms of cryptography are:

- **Plaintext**: message or original text to be encrypted before transmission.
- **Cipher text**: data in unreadable format that is encrypted by using encryption algorithm.
- **Encryption**: The method of hiding data using some mathematical functions.
- **Decryption**: The process to convert cipher text to its original text is called decryption.

Different cipher texts are produced by using same plaintext and different key. The security of cryptography algorithm depends on strength of the key. The harder it is to discover the key,

the more is the security of the cryptography mechanism. Cryptography can be explained by an example of two users (A and B) who want to communicate over an insecure environment. A transmits the data in encrypted form over the channel so that any attacker may not understand the confidential data and may not modify the data so that only the intended recipient(B) receives the correct data. B decrypts the data using decryption algorithm to achieve desired information [7].

1.7.1 Design Constraints in Cryptography

Cryptography services help to ensure the following:

- **Authentication:** Assures that the data originates from a particular user by using digital certificates.
- **Confidentiality:** Ensures privacy of data. This service guarantee that the information is accessible to only to authorized users.
- **Data Integrity:** It ensures information is not modified or changed during transmission from source to destination [7].

1.7.2 Block Diagram of Encryption and Decryption in Cryptography

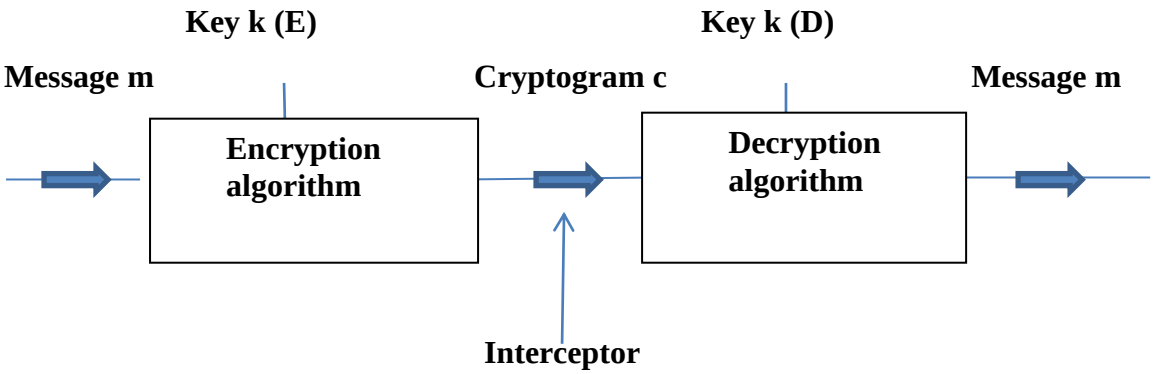

Figure 1.7: Block diagram of Encryption and Decryption

Figure 1.8 describes complete cryptography system explaining how confidential information is transmitted without any interference from unauthorized user. The message or incoming packet m is input to encrypting algorithm along with enciphering Key k (E) to produce an encrypted data c which is transmitted over the channel. The recipient at the other end who has already agreed on the encrypting algorithm use the matched pair of key i.e. the deciphering key k(D) and deciphering algorithm to decrypt the data into the desired information or message m. It already assumed the cryptography algorithm is already known to any interceptor, even if it known not, it is easy to find out the encrypting algorithm. The strength of the protection of message depends on secrecy of key and management of key. If

interceptor has a knowledge of deciphering key k(D) , it is easy to obtain the secret message. If the deciphering key k(D) is obtainable from enciphering key k(E),it is symmetric algorithm, otherwise in asymmetric algorithm ,it is infeasible to obtain k(D) from k(E)[8].

1.7.3 Types of Cryptography

Cryptography deals with converting plaintext (ordinary text) into cipher text by a process called encryption and then converting back cipher text to plaintext by a process of decryption. Various ways to classify the cryptography algorithms are:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

- **Symmetric Key Cryptography**: In Symmetric Key Cryptography, encryption and decryption is performed using a same key. The sender uses the key to encrypt the message or plaintext to convert it to cipher text which is transmitted to the receiver. The receiver also uses the same key to decrypt the message and recover the plaintext. In this cryptography, key must be known only to sender and receiver ,i.e. kept secret, therefore this form of cryptography is also known as Secret Key Cryptography. One of the difficulties faced by this form of cryptography is distribution of the key.
- **Asymmetric Key Cryptography**: In Asymmetric key Cryptography, a key pair is used which has a public key and a private key. The sender uses the receiver's public key to encrypt the message and transmit it to the receiver, where receiver uses its private key to decrypt the message. Security is basically based on keeping private key secure and public key may be shared in the network.

1.7.4 Symmetric Key Cryptography

Symmetric key Cryptography can be categorized into two forms which can be either block ciphers or stream ciphers

***1.7.4.1 Block Cipher*:** In block cipher, the message breaks into fixed block where one block of data is encrypted at a time using the same key for each block. For each set of plaintext using the same key, same cipher text is generated each time. The block cipher is further divided into two parts:

- **Substitution and Permutation Network:** In block cipher such as AES, Present, Shark and Square a series of consecutive operations are done block of data. A block of plaintext and key is taken as inputs and layers of mathematical operation such as Substitution box (S-Box) and permutation boxes (P-boxes) are applied in each round. After execution of these mathematical operations in assigned number of rounds using

sub key or Round key derived from secret key. By reversing the complete process decryption can be easily done.

- A S-box basically substitute bits in input block to form a complete new output block, where substitution can be bit wise or byte wise. S-box provides one of the essential properties of avalanche effect where changing one bit in input bits will change half of the output bits.
- A P-Box permutes all the bits in the input block to form the output block of bits.

- **Feistal Network:** Feistal Network forms a symmetric structure which provides advantage as encryption and decryption operations are similar. In this network, firstly the plaintext block is split into two half. In each round ,L(i+1) is equal to R(i) and R(i+1)=L(i) xor F{L(i),R(i)} to generate a final cipher text by fixed number of rounds. Function F has its own advantage that it does not need to be inverted while decryption process. A large number of block cipher use this scheme to produce confusion and diffusion such as DES.

1.7.4.2 Stream cipher: In stream cipher operation is done on a single bit at a time, and a feedback mechanism is used so that key is updated at constant interval. Stream Ciphers are designed in a way that they are much faster and simple in implementation than block cipher. A stream cipher generates key stream by using some mathematical functions performed in a process of Key Generation [6].

The general structure of stream cipher can be explained as stream cipher consists of an initial state and an update function which updates this initial state for next rounds. Initial Vector (IV) and key is taken as initial inputs to generate a random sequence of key stream which is pseudo random sequence. This generated key stream sequence is exclusive or (XOR) with plaintext to produce a cipher text. The strength of the stream cipher completely depends on the randomness of the key [9].

Stream Cipher can be categorized based on the generation of the key stream as:

- ***Synchronous stream cipher*:** In synchronous stream cipher, key stream is generated independent of plaintext and cipher text, and at the decryption side also same procedure is followed for key generation as for the encryption.

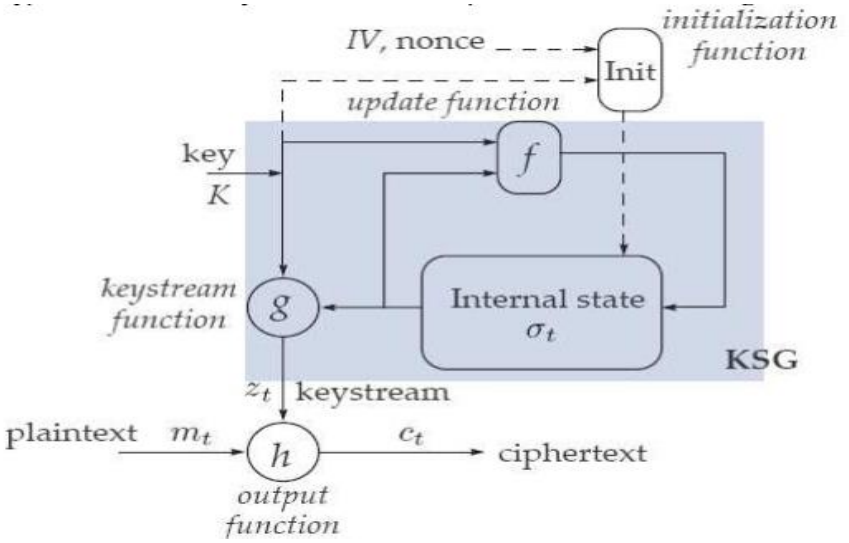

Figure 1.8 Synchronous stream ciphers

In synchronous stream cipher as shown in Figure 1.9, update function takes secret key as input and is independent of plaintext and cipher text. Internal state holds the input for key stream generator to produce a random sequence. Initialization function stores the initial value of IV and secret key, whereas update function taking input of secret key and data from internal state update the internal state to produce input for pseudorandom generator. Output function h is generally exclusive-or operation between the plaintext and the random key stream sequence generated.

- ***Self-synchronous stream cipher****:* For Self-synchronous stream cipher, generation of key stream is dependent on previous cipher text stream and the internal state in the key generation phase as shown in Figure 1.10 [6].

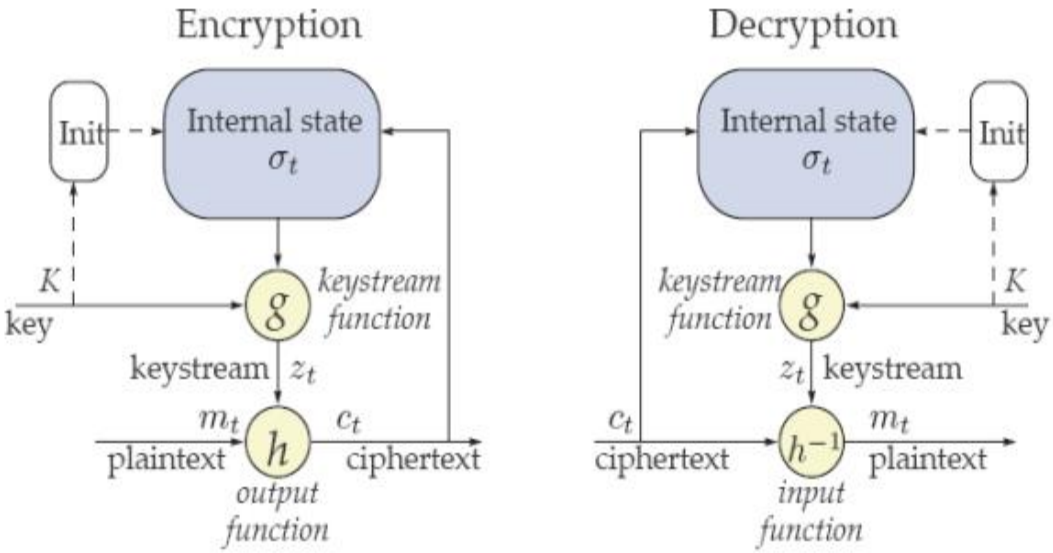

Figure 1.9 Self-synchronous stream cipher

Table 1.2 Comparative analysis of Block and Stream Cipher

Block Cipher	Stream Cipher
Encryption is done block wise which can be 128 bit, 256 bits etc.	Encryption operation is done bit by bit.
Same Key is used for each block.	Different key is used for each block
Slower in operations	Fast and small so these are used for resource constraint devices for example: cell phones, small embedded devices.
More complex in terms of operations in algorithm	Less complex or simple in terms of operations in algorithm
Slow Execution	Fast Execution
Most Secure	Security depends on key generation mechanism
Popular block ciphers are AES (Advanced Encryption Standard), DES (Data Encryption Standard)	Some of the stream ciphers are RC4, SEAL, and A5 family of stream cipher.

1.8 OVERVIEW OF KEY GENERATION IN STREAM CIPHER

Key stream Generation is one of the main components of stream cipher which is used to produce a pseudorandom key stream sequence by using public IV and a secret key. In initial times, stream ciphers used to take a single key as an input which was required to be kept secret. Later on to solve the key management problem, two inputs were used in stream cipher, one is the secret key that is to be kept secret and the other is the initialisation vector that is made public.

Two main phases included in key generation are initialisation phase and key generation phase. The initialisation phase is classified further as Key and IV loading phase and State updating phase.

- **Initialisation Phase:** The IV (initialisation vector) and secret key are used to form the internal state in the initialisation phase. The key generator has to go through this phase before encrypting the plaintext where key and IV are diffused properly so that there is no correlation between Key, Key generated and IV and Key generated.
    - **Key-IV loading phase**: In this phase Key and IV are loaded in the internal state by some fixed rule. We get a loaded state of Key and IV at the end of this phase.

- **State Updating Phase:** With the help of state update function, the initial loaded state is updated to obtain new state by some fixed number of iterations. At the end of this phase, we obtain a state called the initial state. The number of iterations affects the diffusion of key generated, causing the cipher prone to attack.

- In the **key generation phase**, state update function is used to update the internal state and mathematical functions are performed to obtain the key stream sequence.

Encryption is performed by using some operation on plaintext and key generated which is usually bitwise XOR operation. XOR is preferred as we observe the truth table of XOR operation, if we assume input bit to be x=0, output bit has equal probability of occurrence of either 1or 0, same is the case for input bit x=1.Therefore, it becomes completely unpredictable and shows exactly 50% chance of occurrence of zero and one, and generated sequence shows behaves perfectly randomly [11].

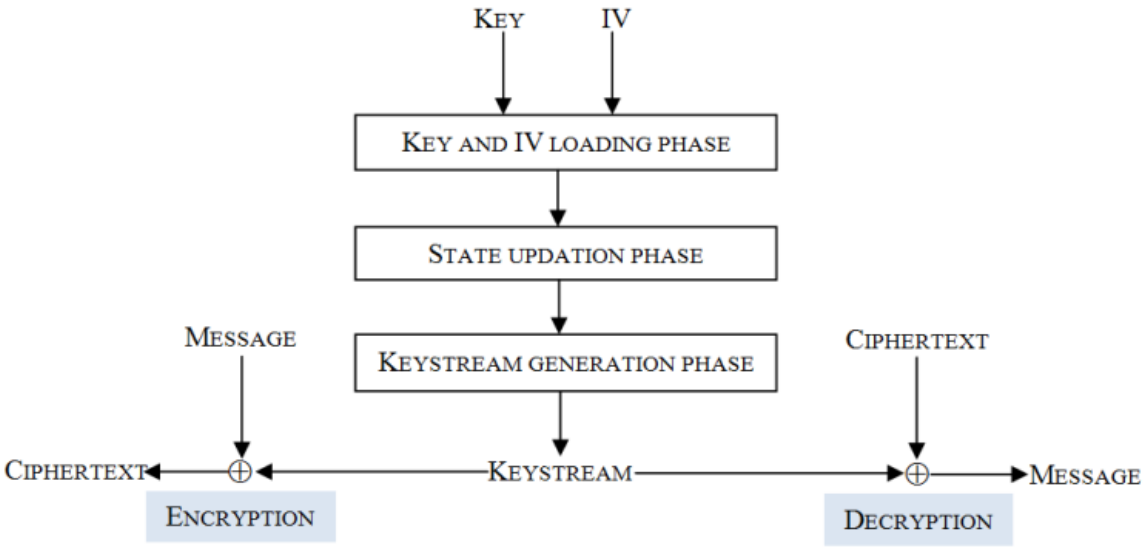

Figure 1.10 Block diagram for different phases of stream cipher

1.9 OVERVIEW OF CRYPTOGRAPHY IN MANETS

There are major threats to MANETs due to various attacks discussed in the Section 1, so securing the message packets and authentication of nodes is the at most important task for MANET's security [10]. In the Figure 1.11 shows a flow diagram of secure data communication. There are two features desired are generation of unpredictable and random key by using a seed generator and reliable key generation mechanism and a strong logic circuit for encrypting the message packets to be transmitted. A good Pseudo random Number Generator can be used as a key Generation mechanism which uses a seed as an initial

parameter and a deterministic algorithm and always produces same sequence for the same seed point. A truly random number generator produces non repeatable and unpredictable sequence from some alphabet A. Securing data can be achieved by cryptography algorithm which can be classified based on the key used if same key is used, it can be referred as symmetric key algorithms. Encryption of packets at sender nodes is usually done using symmetric key algorithms. If a key pair is used public key for encryption and private key for decryption can be called asymmetric cryptography algorithm which are used for authentication of nodes before transmission of message packets [6].

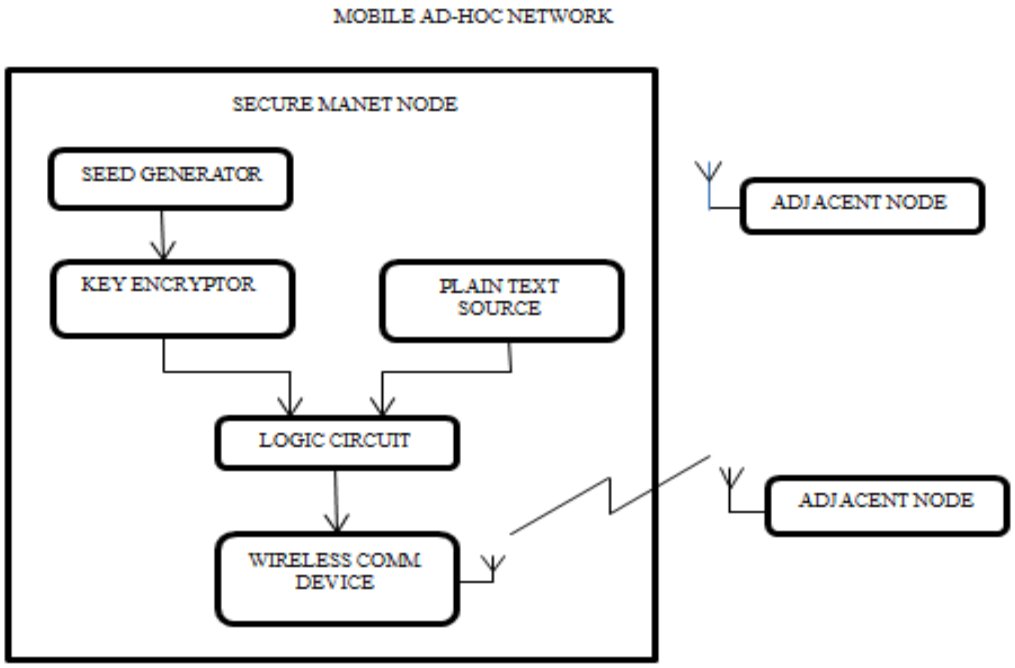

Figure 1.11 Encryption Module of Data Stream in MANETs.

1.10 RANDOM NUMBER GENERATOR

The basic process of encryption and decryption is quite simple and easy to break. The major security depends entirely on the randomness and secrecy of the key stream generated. Since, Randomness plays a very major role in keeping the key secure from any attack, so there are two methods of random number generation.

- **True Random Number Generators (TRNG):** In TRNG, random number once produced cannot be generated again. It is a physical process by which TRNG can produce random sequences. A truly random number generator produces non repeatable and unpredictable sequence from some alphabet A. TRNG are often used in cryptography also to produce random sequence for keys to be used in each round or in successive sessions of transmission of data. Some of the examples used for TRNGs are rolling of dice, radioactive decay, semiconductor noise, flipping of coin etc.

- **Pseudo-Random Number Generators (PRNG):** Pseudorandom number generators (PRNGs) are used to generate sequences which are computed by using an initial seed value .A pseudo-random Number generator is used as a key stream generator to produce random key as desired for security. A good pseudo-random number generator helps in designing a good synchronous stream cipher. A pseudorandom number generator follows a particular algorithm to produce independent sequence using a seed point as initialization parameter but produces same sequence for same seed point.

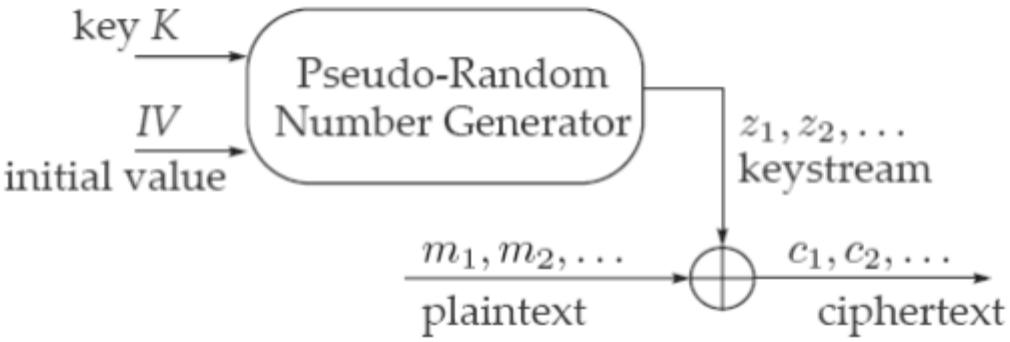

Figure 1.12 Pseudo-Random Number Generators

There are some of the properties that a PRNG must satisfy to produce randomness each time. Some of these statistical requirements are:

- **Period Length:** Period length should be large enough for a PRNG that it should take a large time to reach the same state where it has been already.
- **Statistical Properties**: Sequence generated by PRNG should be uniformly distributed in terms of zeros and ones i.e. probability of occurrence of 1 and 0 should be approximately ½ for both. There are various other statistical test that shows the randomness of key stream generated like Frequency test, Run test, approximate entropy test, Block Frequency test, Longest Run test [12].

1.11 OUTLINE OF THESIS

This section explains all the segments of thesis briefly .In chapter 2,survey of symmetric and asymmetric algorithm along with generation and management of key is done from various research papers discussing the limitations of some work defined and obtaining solutions to overcome them. In chapter 3, based on the study and survey done, work to solve these issues and objectives are defined .In chapter 4, AES and modelling of AES is discussed briefly. An Improved AES algorithm is proposed where substituting of mix column operation by random dynamic shifting operation is done and performance analysis is done based on correlation and

avalanche effect between plaintext and cipher text obtained. AES and improved AES are used as pseudo random number generator as an application in Key generation for stream cipher and randomness of key generated is verified by performing statistical test by NIST. Chapter 5 includes the conclusion of the complete thesis work and analysis of performance parameters of work done. Next section includes all references whether they are directly or indirectly helpful in this thesis.

CHAPTER 2

LITERATURE SURVEY

To give some prospective about key generation and encryption algorithms keen study of some research papers is done in this section.

2.1 SURVEY ON KEY GENERATION

Kavita T.Patil, *et al.*[13] proposed an design of Adjustable Key cipher based on AES where sub keys are generated for each block of plaintext and mix column is performed only for five rounds instead of ten rounds to reduce the simulation time along with introduction of new S box which is used for both encryption and decryption process. This propose design is implemented with CGA and compared with the use of SHA-1 in CGA and has shown significant improved results in terms of throughput ,delay dropping ratio, energy consumption and also provides protection against linear, differential ,and brute Force attack.

Amit Kumar, et *al*. [14] discussed a key management technique in this paper which provides localization of information using transmission over multiple ranges by anchor selection method, and generating key by using hashing function. To achieve secure communication back–off communication is used and performance is analysed based on parameters like computation complexity, storage requirement, overhead generated.

Mayur Solanki, *et al.* [15] discussed an enhanced version of Key generation using Snow and AES encryption algorithm depending on whether identifier is 0001 or 0010 which can be deployed in any system using LTE. In the proposed work using sub key CK2 and bitwise right rotation operation, algorithm becomes more complex but still take reduced time for encryption and decryption function. Implementation of the work is done on MATLAB using R2010a simulator**.**

The author **Pankaj, *et al.* [16],** came up with an improved LFSR based Key generation for stream cipher algorithm. This paper shows improvement done to reduce cryptography weakness in A5 family of stream cipher algorithms by introducing new clocking scheme, by increasing size and number of LFSR registers and adding a Non-linear combination function. Implementation is done on MATLAB and randomness of generated key is verified by using Randomness Test Suite defined by NIST.

Paresh Ratha, *et al.* [17], presented an optimized cryptography algorithm using arbitrary matrix key for key sequence generation by multiplying by an initialization vector and by performing further conversions. One of the additional features is substitution function that provides security to the key as it becomes difficult to recover the key and thus provides

security to the plaintext. Performance is evaluated by considering the parameters such as execution time, throughput and Avalanche Effect.

2.2 SURVEY ON ENCRYPTION ALGORITHM

L. Raja, *et al.* [18] has introduced a technique to detect any kind of intrusion by malicious nodes which can be detected by the neighbouring node. This Dual Authentication Hashing technique is compared on the basis of delay and routing overhead and show better results with respect to the use of Digital Signature Technique for the security of MANETS.

Peng Zhang, *et al.*[19], focussed on reducing the energy consumption for encryption and decryption of data which is the major concern where Network coding is preferred. P coding is used to create randomness of stream and then lightweight encryption scheme is used due to resource constraints in MANETS before Network coding which further reduce consumption of energy. Analysis is done based on throughput, energy consumption, and encryption time.

Ajay Kushwaha, *et al.* [20], proposed a Selective Significant data encryption algorithm which encrypts selected data form the incoming message thus reducing encryption overheads due to limited power supply and increasing the uncertainties in data encryption method. This work deploys the Blowfish Algorithm for encrypting significant data and excluding the ones which are conjunctions, articles, prepositions and articles etc. The results show that the proposed work is a feasible solution for wireless network.

Yang Cao, *et al. [*21], has shown comparative analysis of various cryptography algorithms like AES, Blowfish, Ghost on the basis of encryption and decryption time where blowfish has better performance compared to others. Time consumed in key expansion is also measured which shows blowfish require a significant amount of key expansion time**.**

R.D. Sparrow, *et al.* [22], presented the LEOPARD cryptography algorithm derived from AES with reduced processing time and comparative results with AES. For the application of UAV also, LEOPARD has proven to have less power consumption and increased throughput.

Suman Brar, *et al.* [23], has worked on detecting and removing the grey hole attack from a MANET network. A Particle Swam Optimization method is used, which is updated to infinity on detection of malicious node which is done by the neighbor of the corrupted node. Based on parameters such as Throughput, End-to End delay, Routing overhead, performance of proposed work is analyzed.

Ravilla Dilli, *et al.* [24], proposed a secure hash algorithm is used for MANETS routing Security and HMAC (hash message authentication code) for authentication and integrity of data and using Zone Routing Protocol as a routing technique. The author has implemented both SHA 3-256 and SHA 3-512 and analysis of performance is done which shows SHA 3-

512 has better performance in terms of Throughput, End -to -End Delay and packet delivery fraction than SHA3 -256.

Shruti Patel, *et al.* [25] discussed various cryptography algorithms like AES, DES, 3DES, HEF, P-coding provide less encryption time, high throughput ,no computational overhead, but AES provides high security .Use of network coding gives high benefits throughput, less energy consumption and transmission time and high security.

Sunil Kumar Sahu, *et al.* [26], works on symmetric key cryptography algorithms which are used to provide security for Mobile ad-hoc network. Comparative analysis of different cryptography algorithms is done based on encryption and decryption time , battery consumption and end-to-end delay which concludes a better performance of AES algorithm while Blowfish has better throughput performance compared to other algorithms.

Qi Zhang, *et al*.[27], discussed image encryption by using AES Algorithm and implemented in MATLAB since basic unit used in AES is matrix and MATLAB provides an ease in calculations array and matrix. Analysis is done based on key sensitivity also and security of encrypted image is shown with the help of histogram when inappropriate key is used.

Sneha .V. Trivedi, *et al.* [28], focussed on image encryption and decryption using proposed AES algorithm which is implemented on single core NIOS II system on Ahera DE2 FPGA (Cyclone II EP2C35F672) board along with W7 key stream generator which remove noise from the encrypted image depicted in histogram. The decrypted image obtained is highly enhanced and better quality image.

M.Madhurya, *et al*. [5], has explained a novel method for security over the hostile network. This is achieved by proposing a novel cryptography algorithm which incorporates both symmetric cryptography for encryption and asymmetric cryptography for authentication with additional circular rotation that provides increased security over the network by enhancing the security the algorithm. In order to avoid malicious behaviour of nodes and in the path between the nodes ,Disturbance detection mechanism is proposed .Performance results are compared with normal AODV protocol and show improved results for average throughput, routing and control overhead and for end to end delay.

CHAPTER 3

PROBLEM FORMATION

From the literature survey, the following problems are defined on which research work is done. In the wireless network, MANETs have advantage over centralized nodes network that provides mobile devices an easy way to communicate by changing link between devices and nodes can act as router whenever required transmitting data to the destination node. But since there is no centralised authority it is more vulnerable to various attacks such as man in the middle attack, replay attack, Black hole attack [1]. Therefore, the major concern of MANETs is to provide security. Encrypting the data before transmission is the key requirement where the security is concerned so that any intruder or malicious node cannot obtained any meaningful information. The security of encrypting the secret data depends on the strength of the algorithm and secrecy and randomness of the key.

3.1 GAPS FROM LIERATURE SURVEY

- In the MANETs, for encryption block cipher algorithms are also used for security purposes such as AES, Blowfish, and DES *etc*. The authors showing benefits of AES and Blowfish over DES, 3DES,Gost in terms of execution time, attacks, throughput [21,25,26]. Also, most used algorithm is AES because it is recommended by NIST. But, it's have limitations such as large memory requirement and execution time. In paper [22], shuffling of shift row, mix column ad add round key transformations is done and removal of S-box transformation from 9 rounds is done to obtain comparative correlation of AES Algorithm. However memory requirement remain same due to use of S-box even if it is executed only for one round although execution time reduces.

  So, one research direction is to design improved AES which consumes less area and execution time.
- Randomness of Key: In wireless network, stream cipher are also preferred over block cipher for continuous transmission of data, the overall security in stream cipher depends on randomness of key. In paper [16], LFSR (Linear Feedback Shift Register) based key generation is discussed. This technique provides randomness to the key by using number of LFSR in the key generation mechanism which is analysed based on statistical tests validated by NIST

(National Institute of Standards and Technology). But the limitation in using LFSR that the feedback bit is a linear function of state bit.

So, it is desired to design pseudo random number generator as key generation mechanism which provide non-linearity and randomness at each instant of transmission.

- Block cipher as application in stream cipher: In paper [13],author discussed key generation using AES with reduced number of mix column operation to reduce execution time but resource requirement remain same since mix column operation require same amount of memory even if it is called only in five rounds.

  However, this technique includes using fixed IV (initialisation vector) in each iteration, thus reducing the randomness of the key generated and secrecy of IV.

  So designing key generation mechanism using limited resource requirement and these fixed IV problems can be resolved by modifying IV each time of transmission can provide security as well as authentication since same procedure is followed by receiver to update IV. This updating of IV can resolve the replay attacks on MANETs.

3.2 OBJECTIVE

- Study and Analysis of existing Cryptography and Key generation Algorithms.
- Implementation of AES Algorithm and designed improved AES Algorithm. Also, done comparative analysis between basic AES and improved AES algorithms on the basis of Avalanche Effect, Correlations.
- The AES Algorithm application is used for Key generation for Stream Cipher and Statistical analysis is also done and compared with the existing key generation techniques.

3.3 MEHTODOLOGY

The proposed work methodology and their following steps in chronological order are shown in Figure 3.1.

1. The proposed work begins with understanding of MANETs, their Attacks and countermeasures through literature survey. Based on survey, AES algorithm is selected because it's recommended by NIST.
2. Modelling is done for Improved AES Algorithm and its simulation is performed on MATLAB.

3. Performance Analysis is done of AES and Improved AES Algorithm based on Avalanche Effect and Correlation Factor.
4. AES and Improved AES Algorithm is used as an application for Key Generation in stream cipher for MANETs
5. Analysis of Randomness of Key Generated is done on the basis of NIST statistical Test and their comparative Analysis with A5 stream cipher

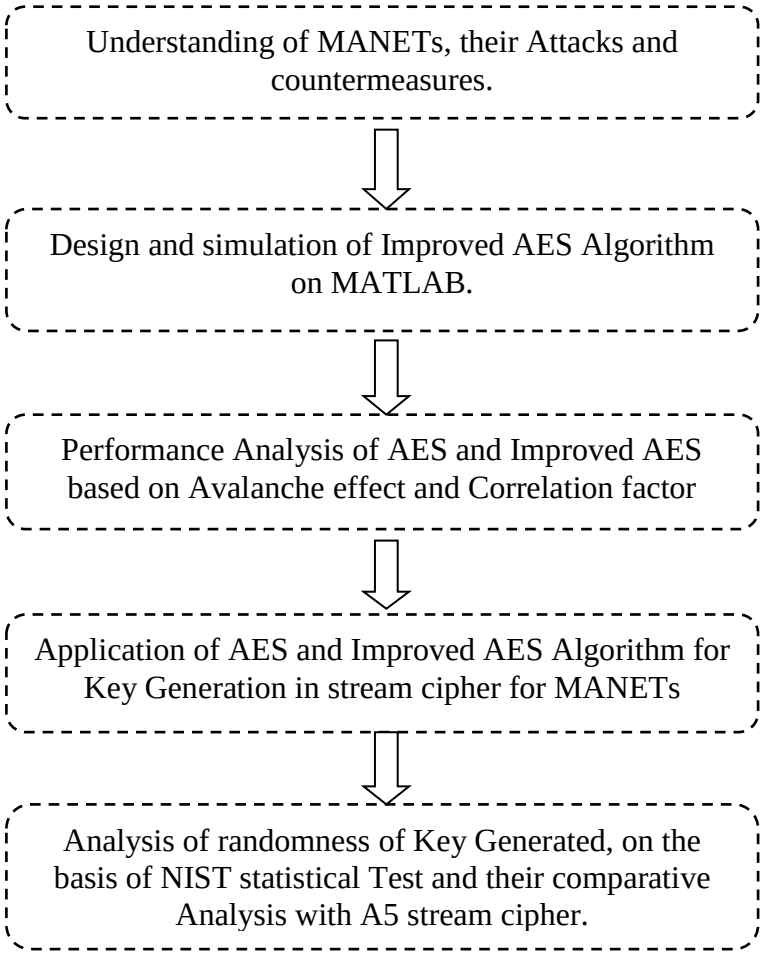

Figure 3.1: Flow chart of design methodology of proposed work

CHAPTER 4

SIMULATION OF PROPOSED ALGORITHM AND PERFORMANCE ANALYSIS

In this section the AES and Improved AES algorithms flow and their modelling is defined. The algorithms are simulated on MATLAB 2013a environment for text data encryption. The security of improved algorithm is compare with existing AES algorithm based on Avalanche effect and correlation factor. Further, the application of proposed algorithm is used for key generation and their NIST statistical test is done on the basis of frequency test, run test, block frequency test, approximate entropy test,

4.1 OVERVIEW OF AES

The Advanced Encryption Algorithm (AES) is the encryption standard recommended by NIST (National Institute of Standard and Technology) in 2001 in a competition of encryption algorithm standard. AES is a highly secure algorithm and most widely used due to its simplicity and high efficiency. AES is a symmetric key algorithm which uses single key for encryption as well as decryption. Key size in AES can vary from 128,192,256 bits which refers to AES-128, AES-192, AES-256 and any combination of plaintext or data of 128 bits. The 128 input data is represented in the form of 4*4 matrixes called state where each element is represented as byte. In AES number of rounds depends on the key length, for 128 bit key length 10 rounds are executed, similarly for 192 bits key length 12 rounds and for 256 bits of key length 14 rounds. Firstly for the case of 128 bit key, both for encryption and decryption add round key operation is performed, then for the nine rounds four of these transformations are performed in each round.

1. Sub-byte operation
2. Shift row operation
3. Mix column
4. Add round key

In the final round i.e. the 10^{th} round, mix column operation is not performed. Decryption is the inverse process of encryption using same operation in their inverse form .i.e. Inverse Sub byte operation, Inverse Shift row, and Inverse mix column.

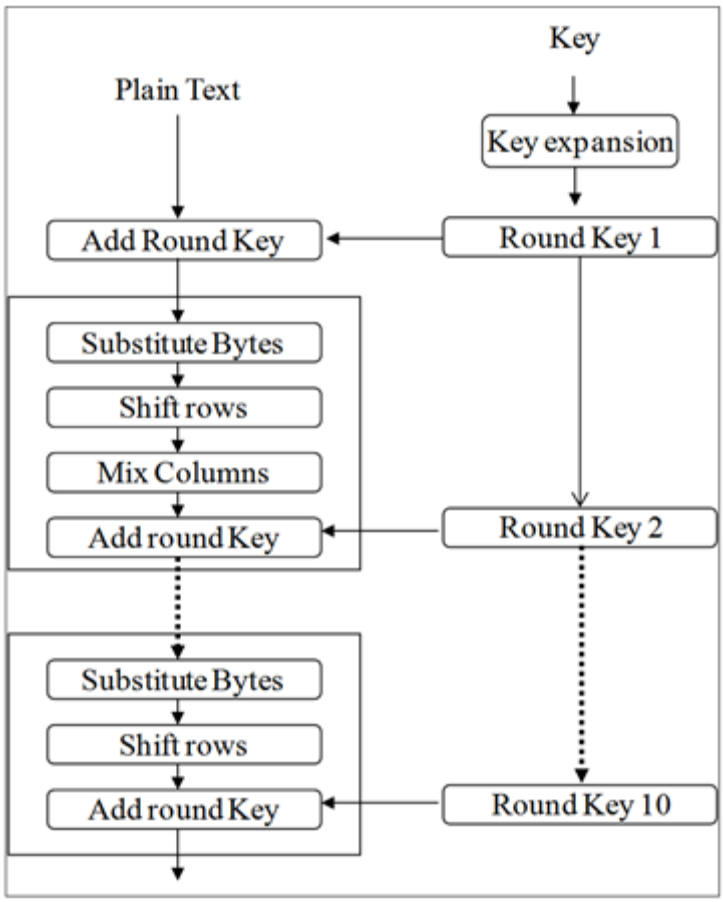

Figure 4.1 AES (Advanced Encryption Standard) process

- **Sub-Byte transformation**: Each byte in the state matrix is substituted by another byte using a non-linear Rijndael S-Box represented in the form of Look up table. AES has 128 bit of data which require 16 byte substitution in one round.
- **Shift Rows transformation:** In this step, the bytes in the last three rows of a 4*4 state matrix are circularly depending on their row position. For 1st row ,there is no shifting to be done, for 2nd row one byte circular shift to left is performed ,similarly for 3rd row and 4th row two byte and three byte circular shifting to left is done respectively.
- **Mix columns transformation:** Mix column operation performs a multiplication operation on the 4*4 matrix using each column of the state matrix. A predefined fixed matrix is multiplied with each column to generate new column of the resulting state matrix.
- **Add round key transformation: Each** byte of the state matrix is bitwise XORED with the byte of the corresponding Round key for that particular round where each round key is obtained from the initial secret key.

- **Key Expansion operation**: Round keys which are used for each round in add round key transformation is obtained by the initial Secret Key using a Key scheduling process which performs circular shift, S-Box operation and XOR operation with Rcon constant matrix to obtain Sub keys [29].

Table 4.1Parameters for AES-128, AES-192, AES-256

Key Size	128 bits	192 bits	256 bits
Plaintext Block Size	128 bits	128 bits	128 bits
No. of Rounds	10	12	14

4.2 MATHEMATICAL MODELLING OF AES

Galois Field Mathematical Modeling is used in AES Algorithm for Security Purposes. Galois Field which is also known as finite fields where there is an existence of finitely many elements. Galois Field is useful in translating binary data or data stored in computer in the form of 1and 0.To ease the calculation and mathematical operations, data is represented in the form of vector.

- **Addition (XOR):** Addition in Galois filed is simple operation.
  - $(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$
  - $\{01010111\} \oplus \{10000011\} = \{11010100\}$
  - $\{57\} \oplus \{83\} = \{d4\}$
- **Multiplication**

  It is a tricky and tedious operation.

  $x^6 + x^4 + x^2 + x + 1)\ (x^7 + x + 1) =$

  $$x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1$$

  $$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

  and

  $x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$ modulo $(x^8 + x^4 + x^3 + x + 1)$

  $$= x^7 + x^6 + 1.$$

4.3 IMPROVED AES ALGORITHM FOR MANETS

An Improved AES algorithm is proposed based on using AES S-box and key expansion mechanism and a random dynamic shifting is performed to produce avalanche effect using permutation and XOR operations[30]. The input plaintext state is XORED with the round key '0'. For the next 10 iterations, three of these transformations are performed as shown in Figure4.2:

AES ALGORITHM
INPUT1: PLAINTEXT (STATE)
INPUT2: KEY
ADD ROUND KEY
LOOP: I=1 TO 9
{
S-BOX TRANSFORMATION
SHIFT ROW OPERATION
MIX COLUMN OPERATION
ADD ROUND KEY
}
S-BOX TRANSFORMATION
SHIFT ROW OPERATION
ADD ROUND KEY
OUTPUT: CIPHERTEXT

IMPROVED AES
INPUT1: PLAINTEXT (STATE)
INPUT2: KEY
ADD ROUND KEY
LOOP: I=1 TO 10
{
S-BOX OF AES
RANDOM DYNAMIC SHIFTING
ADD ROUND KEY
}
OUTPUT: CIPHERTEXT

Figure 4.2 Pseudo codes of AES and Improved AES

1. S-box: The state obtained from add round key operation is transformed into new state by using Nonlinear Rijndael S-box which creates reduced correlation between plaintext and cipher text.

2. Random Dynamic Shifting: In random dynamic shifting , each row of 32bits of state matrix is permuted to obtain new 32 bits rows where each row is circularly rotated by random values of nine, seven, four, one respectively and then cascaded XOR operation is done to generate a new state matrix .This operation provides required avalanche effect since it create significant amount of diffusion and confusion which was obtained by mix column operation in original AES .Since mix column is a complex operation requires a large amount of execution cycles, to resolve this step random dynamic shifting is used to obtain comparative avalanche effect using simple permutation and cascaded XOR operation shown in Figure 4.3[30].

3. Add Round Key: The final state obtained is again exclusive or (XOR) with a round key for that particular round.

After completing the required iterations, final 128 bit cipher text is obtained.

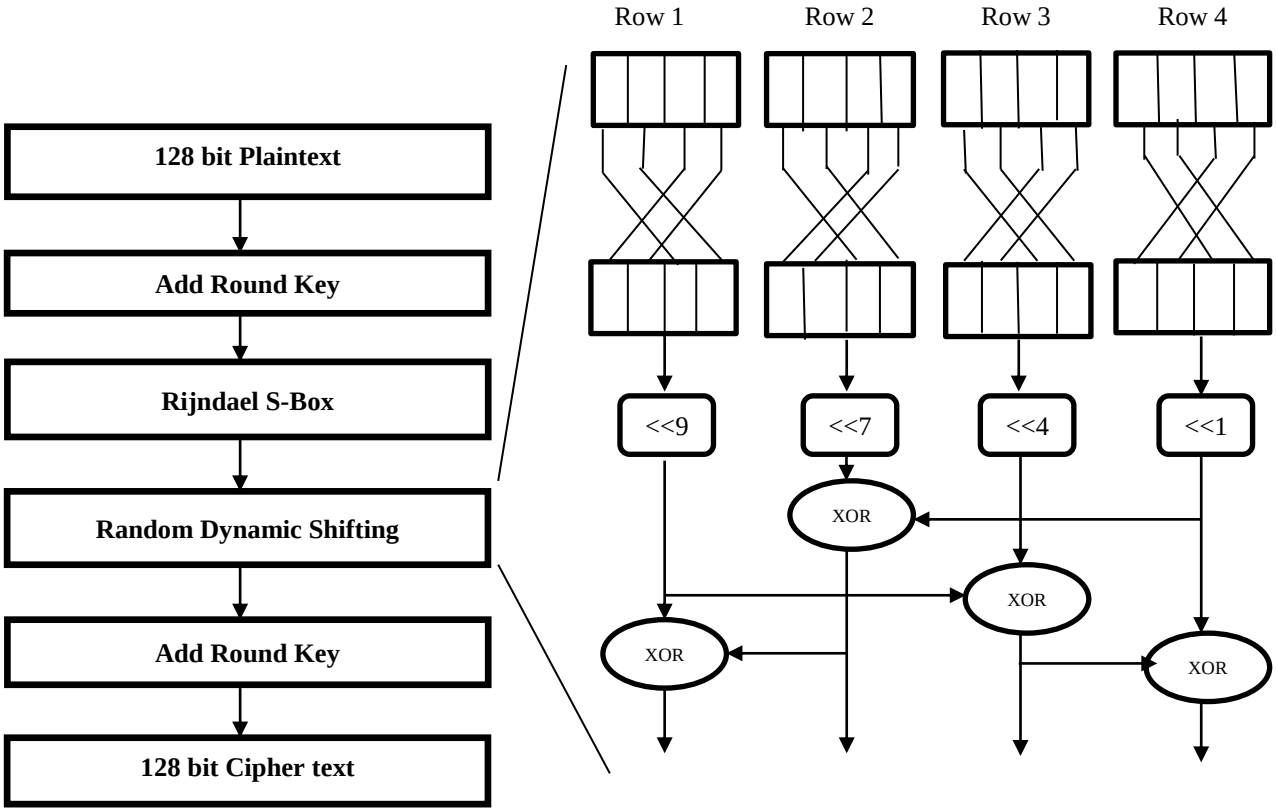

Figure 4.3 Block Diagram of Improved AES

4.3.1 Analysis of Correlation and Avalanche test for AES and Improved AES.

- **Correlation Test:** Correlation Coefficient is an important criterion that analyse the security of any cryptography algorithm to deal with the dependency of output bits or encrypted data on input bits or plain text. It measures the degree of similarity between the two streams *i.e* the plaintext and cipher text. Correlation coefficient lies between -1 and 1.It basically measures the linearity between two sequence or two variables.In the case of independent sequence the correlation coefficient is zero (0).For perfect positive linear relationship, correlation coefficient is +1. For perfect negative linear relationship, correlation coefficient is -1. For values between 0 and 0.3 sequence have weak positive linear relationship and for values between 0.3 and 0.7 moderate positive linear relationship. For values between 0.7 and 1, sequence shows strong positive linear relationship [31].

$$\text{Correlation Factor}=\frac{N\sum xy-(\sum x)(\sum y)}{\sqrt{[N\sum x^2-(\sum x)^2][N\sum y^2-(y)^2]}}$$

N=number of bits in cipher text

∑xy=sum of pair of 128 bits cipher texts

∑x=sum of 128 bits of original cipher text

∑y= sum of 128 bits of cipher text obtained with one bit change in plaintext.

$\sum x^2$=sum of squared bits of original cipher text

$\sum y^2$=sum of squared bits of cipher text obtained with one bit change in plaintext.

- **Avalanche Test**: Avalanche effect is basically calculating hamming distance between two ciphers obtained by changing one bit in the plaintext .One bit change in plaintext or in key should give approximately 50 percent changes in bits of cipher text[32].

Table 4.2 Comparative Analysis of Correlation and Avalanche effect of AES and Improved AES.

Plaintext in decimal	Cipher text in decimal	Correlation between plaintext and cipher text(AES)	Correlation between plaintext and cipher text(Improved AES)	Correlation between two cipher(AES)	Correlation between two cipher(Improved AES)	Avalanche effect of two ciphers(AES)	Avalanche effect of two cipher(Improved AES)
Plaintext: [1 5 9 13 2 6 10 14 3 7 11 15 4 8 12 16]	Cipher AES: [78 216 249 230 118 40 39 222 84 90 246 204 104 230 197 107] **Cipher IAES**: [44 81 248 20 124 241 184 87 149 15 62 2 35 132 204 149 240]	0.4519	**0.2435**	-0.1015	**0.3031**	50%	50%
Plaintext: [1 **4** 9 13 2 6 10 14 3 7 11 15 4 8 12 16]	Cipher AES: [39 97 88 63 61 146 213 201 73 205 117 84 78 213 132 210] **Cipher IAES**: [82 0 236 164 146 96 119 199 133 166 12 141 93 227 239 139]	0.4609	**0.3470**				
Plaintext: [51 55 59 63 52 56 60 64 53 57 61 65 54 58 62 66]	Cipher AES: [64 176 13 253 237 199 115 139 115 174 228 204 144 108 8 112] **Cipher IAES**: [153 232 8 121 215 195 216 168 44 173 212 214 27 153 229 45]	0.0220	**0.0563**	-0.2956	**-0.0247**	46.093%	**49.218%**
Plaintext : [**59** 55 59 63 52 56 60 64 53 57 61 65 54 58 62 66]	Cipher AES: [197 150 145 179 4 120 241 169 37 191 206 22 225 238 178 185] **Cipher IAES**: [111 108 22 81	0.2534	**-0.5057**				

	177 45 78 28 169 178 24 46 222 223 232 65]						
Plaintext: [100 105 109 113 102 106 110 114 103 107 111 115 104 108 112 116]	Cipher AES: [143 251 160 10 3 247 233 145 87 120 87 43 215 115 5 189] **Cipher IAES:** [3 66 112 48 144 10 63 183 221 34 83 212 0 18 25 65]	-0.1740	**0.2088**	-0.4266	**-0.0997**	58.593%	**46.093%**
Plaintext: [**116** 105 109 113 102 106 110 114 103 107 111 115 104 108 112 116]	Cipher AES: [138 126 34 210 154 141 22 202 189 0 250 85 64 20 242 146] **Cipher IAES**: [57 98 1 89 245 44 248 142 22 142 107 157 160 209 208 151]	0.2168	**-0.0045**				
Plaintext: [201 205 209 213 202 206 210 214 203 207 211 215 204 208 212 216]	Cipher AES: [99 137 167 248 66 203 39 251 121 11 129 213 118 80 127 255] **Cipher IAES**: [148 40 207 122 205 232 138 7 196 45 195 231 185 94 34 70]	0.6088	**0.3020**	-0.2858	**0.0869**	50.781%	**52.343%**
Plaintext: [**233** 205 209 213 202 206 210 214 203 207 211 215 204 208 212 216]	Cipher AES: [45 244 13 58 17 248 255 72 244 226 32 189 87 86 225 4] **Cipher IAES**: [50 70 133 165 18 217 6 154 245 120 186 23 72 7 32 223]	-0.3184	**-0.0989**				
Plaintext : [255 199 167 178 240 200 189 145 239 23 154 165 155 11 167 121]	Cipher AES: [42 44 214 54 204 209 137 142 93 183 166 67 113 29 2 19]	0.0747	**0.1685**				

	Cipher IAES: [36 252 114 160 97 203 188 193 217 219 218 39 128 7 192 1]			-0.0012	**-0.3036**	52.343%	**47.656%**
Plaintext: [**191** 199 167 178 240 200 189 145 239 23 154 165 155 11 167121]	Cipher AES: [25 235 9 53 226 181 50 223 205 87 24 93 196 214 40 142] **Cipher IAES**: [180 63 78 157 157 71 211 229 12 2 191 95 144 163 197 189]	0.0351	**0.0094**				
Plaintext: [84 79 78 32 119 110 105 84 111 101 110 119 32 32 101 111]	Cipher AES: [41 87 64 26 195 20 34 2 80 32 153 215 95 246 179 58] **Cipher IAES**: [162 187 100 1 122 49 52 188 92 251 50 102 137 179 194109]	0.0242	**-0.0459**	-0.0517	**-0.0571**	45.312%	**58.593%**
Plaintext: [**68** 79 78 32 119 110 105 84 111 101 110 119 32 32 101 111]	Cipher AES: [169 163 59 106 53 10 1 64 86 26 153 157 87 179 112 148 236] **Cipher IAES**: [117 228 189 110 150 131 14 21 230 15 46 40 53 77 148 104]	-0.1845	**0.0504**				
Average Value:		0.235	**0.170**	0.194	**0.146**	50.521	**50.651**

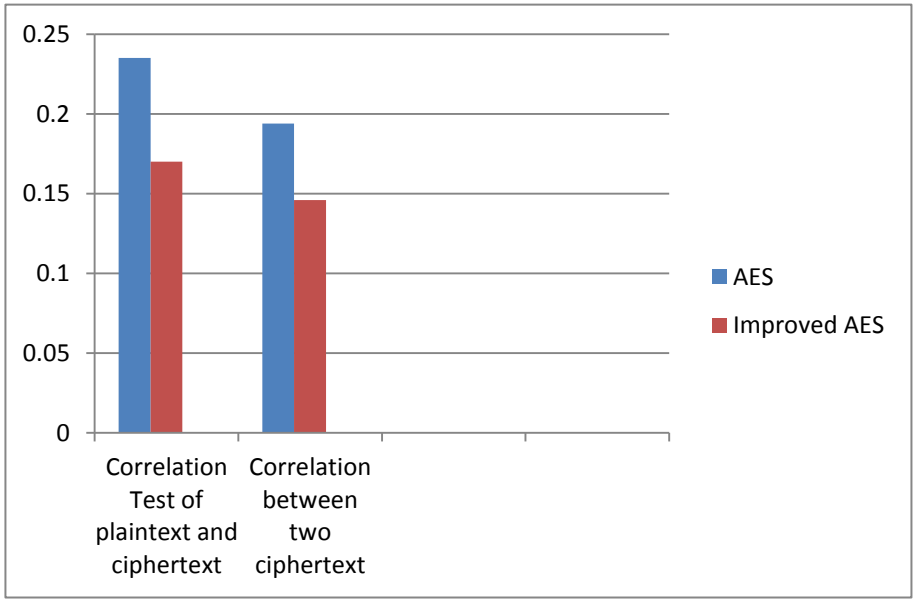

Figure 4.4 Correlation Tests of AES and Improved AES

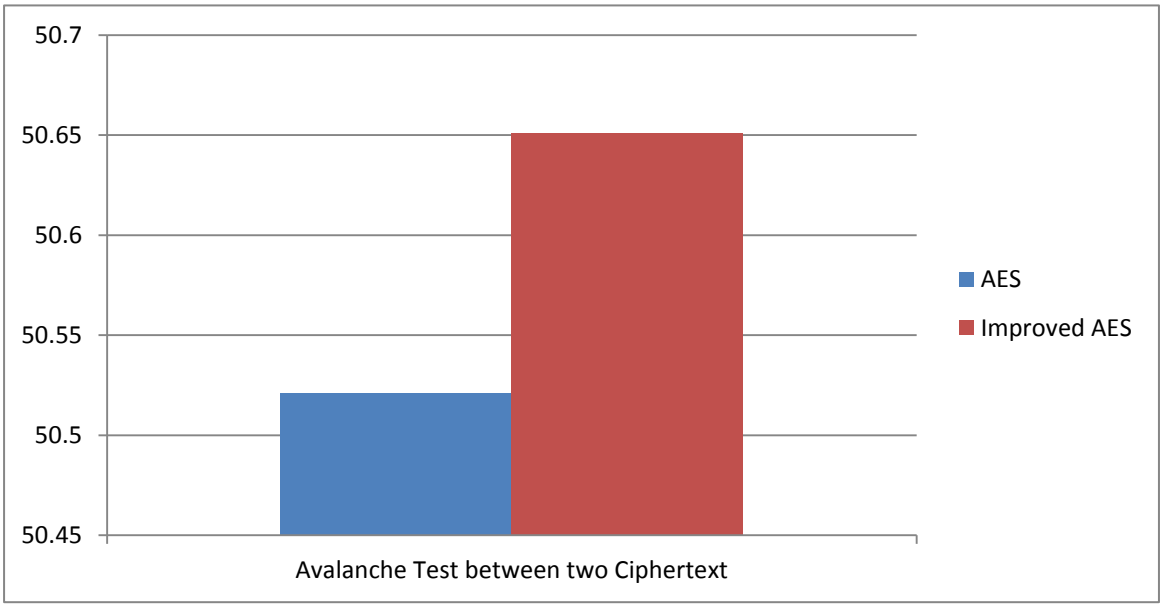

Figure 4.5 Avalanche Test for AES and Improved AES

From Figure 4.4 and 4.5, it is clearly shown that Improved AES has less correlation between the plaintext and cipher text of 0.140 in comparison AES which is 0.235 for an average of various test cases shown in Table 4.2.The less is the correlation factor, the less are the chances of determining plaintext if attacker has some knowledge of cipher text. Similarly for the case correlation between two ciphers, original cipher and cipher obtained by one bit change in plaintext shows better performance or low correlation in

case of Improved AES by a factor of 0.048.Avalanche factor obtained is approximately same for both AES and Improved AES *i.e.* 50.521 And 50.651 respectively

4.4 AES AS APPLICATION IN KEY GENERATION MECHANISM

A new Key generation mechanism using an improved AES is proposed based on AES since it is an already secure block cipher algorithm according to National Institute of Standards and Technology (NIST)[22].In the proposed design, initial 128-bit seed point is defined by the sender which can be transmitted over the channel. This initial seed point generates an 128 bit initialization vector(IV) by using value based rotation which depends on a function of initial message packet .Secret key is obtained by applying non-linear function on IV to produce randomness in the key generated. For the next message packet or nth message packet, the IV is updated based on a varying value in (n-1)th secret key i.e. value based left rotation is performed on 128 bit (n-1) th secret key. The supreme advantage of using value based rotation step is to reduce the correlation between input (plaintext) and output (cipher text) and hike the randomness which can be verified by performing some of the statistical test.

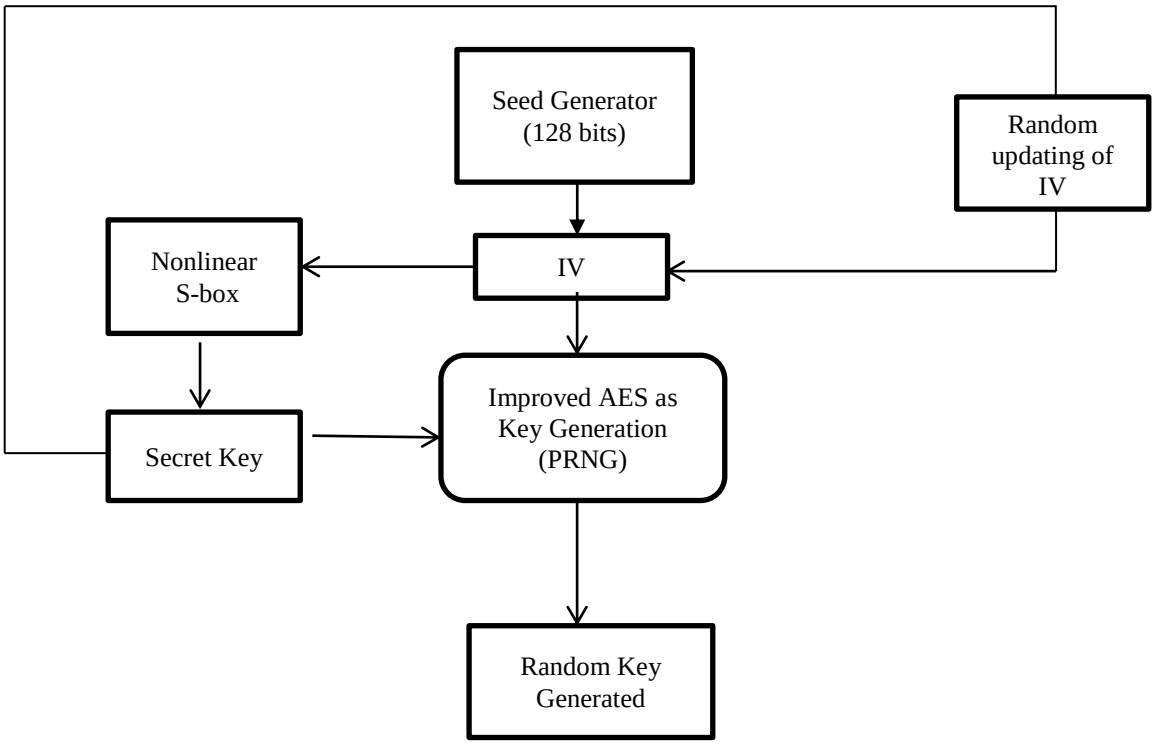

Figure 4.6 Key Generation Mechanism by PRNG

4.4.1 Statistical Tests for Key Generation

Analysis has been done for the key generated by the proposed algorithm with reference to the National Institute of Standards and Technology (NIST S.P. 800-22) statistical analysis program. Several Test are performed to analyse the unique feature of randomness of the sequence generated of the key stream which are : Frequency test, Run test, Approximate Entropy Test., Block Frequency Test ,Longest Run Test .If the p-value determined is greater than 0.01 then it indicates the randomness of the sequence , otherwise the sequence is non-random. Very small value of p infers non-randomness of stream evaluated [33].

- **Frequency Test:**

  For a bit stream, frequency test is a test to check for number of ones and zeroes are approximately same, which shows the randomness and balance in the bit sequence. This test checks the closeness of fraction of ones to ½. If the p-value determined is greater than 0.01 then it indicates the randomness of the sequence, otherwise the sequence is non-random.

- **Run Test:**

  The purpose of this test is to check the uninterrupted run in the sequence where run basically refers to occurrence of identical bit without any interruption. This test verifies whether the oscillation between ones and zeros is too fast or too low. If the calculated p-value is greater than 0.01, it indicates that the sequence is random, otherwise shows the non-randomness of the sequence.

- **Approximate Entropy Test:**

  Entropy is a measure of uncertainty of a sequence generated. It basically measures the randomness of a sequence usually represented in bits. It represents the frequency of all overlapping blocks patterns in the entire sequence.

- **Block Frequency Test:**

  The focus of this test is to check whether the number of ones in an M-bit block is approximately M/2, which is expected under the conditions of randomness.

- **Longest Run Test:**

  This test is used to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence [33].

Table 4.3 Statistical Test for randomness of Key Generation Techniques

Serial No.	Test Name	P-value	P-value	P-value
		A5/1[16]	Original AES with IV Updation	Improved AES with IV Updation
1	Frequency Test	0.684	0.859	0.723
2	Run Test	0.370	0.302	0.936
3	Approx. Entropy Test	0.195	0.390	0.658
4	Block Frequency Test	0.593	0.491	0.876
5	Longest Run Test	0.617	0.743	0.805

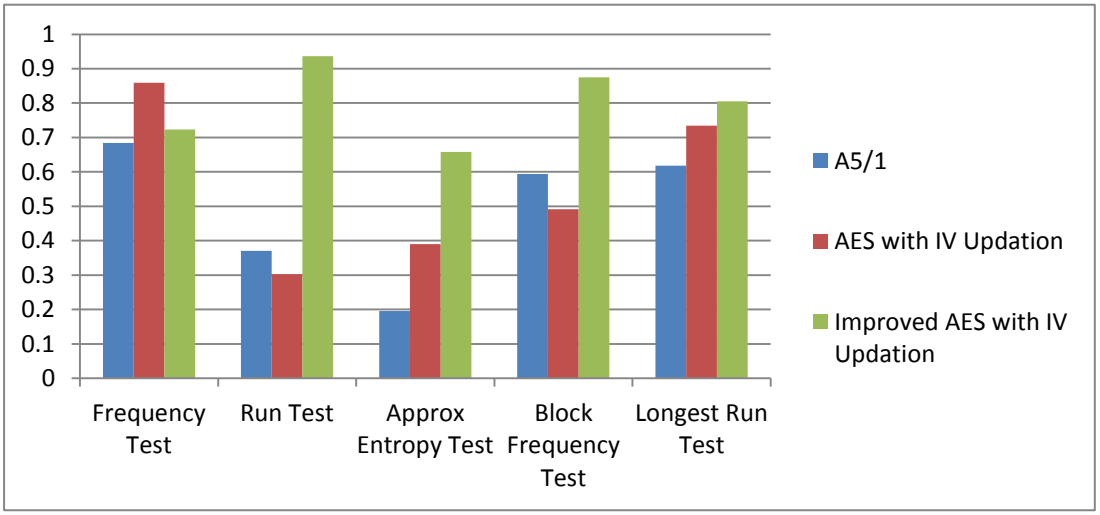

Figure 4.7 Statistical Tests for Key Generation Techniques

4.4.2 Analysis of Randomness of Key Generated

From the Table 4.3 and Figure 4.7, Improved AES algorithm has shown a hike in randomness which can be described by various test defined by NIST (S.P.800-22) statistical analysis program [33]. All the tests such as frequency test , run test, approximate entropy text ,block frequency test, longest run test shows an increment of P-value by 0.048, 0.566, 0.463, 0.283,0.188 for Improved AES Algorithm as compared to A5/1 stream cipher whereas for AES algorithm P-value shows an increment of 0.175,0.195,0.126 for frequency test, approx. entropy test ,longest run test respectively while for run test and block frequency test P-value is slightly less than achieved in A5/1 stream cipher *i.e.* a factor of 0.068 and 0.102 respectively.

CHAPTER 5

CONCLUSION

MANETS are now-a-days one of the most widely used technology which do not require a predefined infrastructure and mobile nodes cooperatively form a network which provides a number of advantages of device portability and scalability of network. However, MANETS also undergo various attacks due to absence of centralized authority .These attacks need to be prevented by securing the data from malicious nodes which can be done by encrypting the information to be transmitted. The proposed work includes a cryptography algorithm which is derived from AES algorithm which is already a secure cryptography algorithm, Rijndael S-box and Key expansion mechanism is taken from the AES while instead of mix column transformation which was a much complex operation, a much simple but effective mechanism of random dynamic shifting is used, which produces a significant avalanche effect and provides randomness to the algorithm by circular shifting operation and cascaded XOR operation. The AES algorithm and proposed work is designed and simulated in MATLAB 2013 on Windows 8 platform. Performance Analysis is done based on parameters like Correlation Test and Avalanche effect Test which shows improved AES has better performance than AES Algorithm in terms of providing security to the data packets transmitted. Furthermore, we proposed a key generation mechanism using AES and improved AES as an application of block cipher in stream ciphers and updating of IV mechanism is used to produce a highly random 128 bit key stream. The proposed work completely satisfy the desired expectation of randomness of key by satisfying the tests done based on NIST analysis program such as Frequency Test, Run Test, Approximate Entropy Test, Longest Run Test, Block Frequency Test and shows better randomness when compared with the A5/1 stream ciphers. It assures that the resulting stream cipher algorithm is highly secure.

Reference

[1] Sachdeva S and Kaur P (2016). Routing Attacks and their Countermeasures in MANETs: A Review, *International Journal of Advanced Research in Computer Science*, 7(4), 48-52.

[2] Singh G (2011). Security Threats and Maintaince in Mobile Ad-hoc Networks, *International Journal of Electronics & communication technology*, 2(3), 68-70.

[3] Aarti and Tyagi SS (2013). Study of MANET: Characteristics, Challenges, Application And Security Attacks, *International Journal of Advance Research in Computer Science And Software Engineering*, 3(5), 252-257.

[4] Rajni and Reena (2014).Review of MANETS Using Distributed Public-key Cryptography, *International Journal of Computer Trends and Technology (IJCTT),* 10(3), 143-147.

[5] Madhurya M, Krishna BA and Subhashini T (2014). Implementation of Enhanced Security Algorithm in Mobile Ad hoc Networks, *I .J. Computer Network and Information Security*,6 (2),30-37.

[6] Ayushi (2010). A Symmetric Key Cryptographic Algorithm, *International Journal of Computer Applications*, 1(15), 1-4

[7] Alia MA, Tamimi AA, and AL-Allaf ONA (2014). Cryptography Based Authentication Methods, Proceedings of [the World Congress on Engineering and Computer Science], [1: San Francisco, USA: 22-24 October2014].

[8] Piper F, *Basic principle of cryptography*, Savoy Place, London WCPR OBL. UK, Printed and published by the IEE, 1996, 1-3.

[9] Ekdahl P and Johansson T (2002). A New Version of the Stream Cipher SNOW, Proceedings of [International Workshop on Selected Areas in Cryptography], [9:Verlag London, UK:15-16 August 2002] , pp.47-61.

[10] Woungang MSOI, Dhurandher SK and Koo V (2014) . A cryptography-based protocol against packet dropping and message tampering attacks on mobile ad -hoc networks, *Journal of Security and Communication Network*, 7(2), 376-384.

[11] Chungath S, *Certain investigations on the design and analysis of initial vector dependent synchronous stream ciphers*, Amrita Vishwa Vidyapeetham (University), 2015.

[12] Keller J and Wiese H, Period Length of Chaotic Pseudo-random number generator, Proceedings of [LG Parallelit¨at und VLSI], [Hagen, Germany]

[13] Patil KT and Patil ME (2014). Improve the Security of CGA using Adjustable Key Block Cipher based AES, to Prevent Attack on AES in IPV6 over MANET, Proceedings of [IEEE Global Conference on Wireless Computing and Networking (GCWCN)], [Lonavala, India:22-24 December 2014], pp.148-152.

[14] Kumar A, Katiyar VK and Kumar K (2016). A Purely Localized Random Key Sequencing Using Accelerated Hashing in Wireless Ad-Hoc Networks, Proceedings of [International Conference on Frontiers in Intelligent Computing: Theory and

Applications], [5: Bhubaneswar,India: 16-17 September 2016] , pp.269-279.

[15] Solanki M, Salehi SM and Esmailpour A (2013). LTE Security:Encryption Algorithm Enhancements, Proceedings of [ASEE Northeast Section Conference] ,[Norwich University,14-16March 2013]

[16] Pankaj, Singh AK and Bora BS (2016) ,Design of Enhanced Pseudo-Random Sequence Generator usable in GSM Communication, Proceedings of [IEEE WiSPNET conference], [Chennai, India: 23-25 March 2016] ,pp.530-534.

[17] Rathaa P *et al.* (2015). An optimized encryption Technique using an arbitrary matrix with Probabilistic encryption, Proceedings of [International Conference on Recent Trends in Computing2015 (ICRTC2015)], [3: December 2015], pp. 1235-1241.

[18] Raja L and Dr. Periasamy PS (2016). Dual Authentication Hashing for Security Enhancement in MANETs , *Journal of Circuits and Systems*, 7(4) ,350-359

[19] Zhang P and Lin C, Lightweight Encryption for Random Linear Network Coding, *Security in Network Coding*, Beijing, China, Springer International Publishing 2016, 43-68.

[20] Kushwaha A, Sharma HR and Ambhaikar A (2016). A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network, Proceedings of [International Conference on Communication, Computing and Virtualization 2016], [7: Bhilai ,India:March 2016], pp.16-23.

[21] Wu L , Detchenkov I and Cao Y(2016).A Study on the Power Consumption of Using Cryptography Algorithms in Mobile Devices,[IEEE International Conference on software Engineering and Service Science(ICSESS)], [7 : Beijing,China : 26-28 August 2016],pp.957- 959.

[22] Sparrow RD, Adekunle AA and Berry RJ(2016). LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion, Proceedings of [International Conference on Signal Processing and Communication Systems (ICSPCS)], [10: Gold Coast, QLD, Australia: 19-21 December 2016]

[23] Brar S and Angurala M (2017). Cooperative Black Hole Attack Prevention by Particle Swarm Optimization with Multiple Swarms , *International Journal of Advance Research,Ideas and Innovations in Technology*, 3(1),858-863

[24] Dilli R and Reddy PCS (2016). Implementation of Security features in MANETs using SHA-3 Standard Algorithm, Proceedings of [International Conference on Computational Systems and Information Systems for Sustainable Solutions],[Bangalore, India: 6-8 Oct. 2016],pp.455-458

[25] Patel S and Khatiwala F (2016).A Review Paper of an Encryption Scheme using Network Coding for Energy Optimization in MANET, Proceedings of [IEEE WiSPNET Conference],[Chennai, India: 23-25 March 2016],pp.1054-1058.

[26] Sahu SK and Kushwaha A (2014). Performance Analysis of Symmetric Encryption Algorithms for Mobile ad hoc Network, *International Journal of Emerging Technology and Advanced Engineering*,4(6),619-624 .

[27] Zhang Q. Qunding (2015). Digital Image Encryption Based On Advanced Encryption Standard (AES) Algorithm, Proceedings of [International Conference on Instrumentation and Measurement, Computer, Communication and Control], [5: Qinhuangdao,China: 18-20 Sept. 2015], pp.1218-1221.

[28] Trivedi SV, Hasamnis MA, Development of Platform Using NIOS II Soft Core Processor for Image Encryption and Decryption Using AES Algorithm, Proceedings of [IEEE International Conference on Communications and Signal Processing],[Melmaruvathur , India :2-4 April 2015],pp.1147-1151

[29] Singh G and Supriya (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, *International Journal of Computer Applications*, 67(19), 0975 – 8887.

[30] BANSOD Gaurav , PISHAROTY Narayan and PATIL Abhijit(2017) , BORON: an ultra-lightweight and low power encryption design for pervasive computing, *Frontiers of Information Technology & Electronic Engineering*,18(3), 317-337

[31] Kumar M and Chahal A (2014). Effect of Encryption Technique and Size of Image on Correlation Coefficient in Encrypted Image, *International Journal of Computer Applications,97(12),0975-8887*

[32] ALabaichi A , Ahmad F and Mahmod R(2013) , Security Analysis of Blowfish algorithm,[International Conference on Informatics & Applications (ICIA)],[2: Lodz, Poland: 23-25 Sept 2013],pp.12-18

[33] Andrew R et *al.*, A *Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application, Computer* Security, Gaithersburg, MD, United States: National Institute of Standards and Technology, 2010.

LIST OF PUBLICATIONS BY THE CANDIDATE

Mansi Sharma, Alpana Agarwal, "**Survey on Authentication and Encryption Techniques for Smart Grids Communication,"** *7th IEEE International Conference on Power Electronics*, November 2016.

==========END OF THE THESIS==========

n2

ORIGINALITY REPORT

%9	%6	%8	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	students.cs.byu.edu Internet Source	%1
2	www.informatica.si Internet Source	%1
3	Kessler, Gary. "An Overview of Cryptographic Methods", Best Practices, 2000. Publication	<%1
4	ntnu.diva-portal.org Internet Source	<%1
5	Shrivastava, Manish, Shubham Jain, and Pushkar Singh. "Content Based Symmetric Key Algorithm", Procedia Computer Science, 2016. Publication	<%1
6	ac.itdurango.mx Internet Source	<%1
7	www.random.org Internet Source	<%1
8	Virginie Lafage. "Does vertebral level of pedicle subtraction osteotomy correlate with degree of spinopelvic parameter correction? :	<%1

	Clinical article", Journal of Neurosurgery Spine, 12/24/2010 Publication	
9	Joshi, Praveen. "Security issues in routing protocols in MANETs at network layer", Procedia Computer Science, 2011. Publication	<%1
10	www.iraj.in Internet Source	<%1
11	Kaur, Simranpreet, Rupinderdeep Kaur, and A.K. Verma. "Jellyfish attack in MANETs: A review", 2015 IEEE International Conference on Electrical Computer and Communication Technologies (ICECCT), 2015. Publication	<%1
12	www.iariajournals.org Internet Source	<%1
13	Anwar, Hassan, Masoud Daneshtalab, Masoumeh Ebrahimi, Juha Plosila, Hannu Tenhunen, Sergei Dytckov, and Giovanni Beltrame. "Parameterized AES-Based Crypto Processor for FPGAs", 2014 17th Euromicro Conference on Digital System Design, 2014. Publication	<%1
14	"Wireless Network Security", Springer Nature, 2007 Publication	<%1
15	www.ijcna.org Internet Source	

		<%1
16	Understanding Cryptography, 2010. Publication	<%1
17	www.ijarcsse.com Internet Source	<%1
18	Christof Paar. "Stream Ciphers", Understanding Cryptography, 2010 Publication	<%1
19	Computation Cryptography and Network Security, 2015. Publication	<%1
20	www.ukessays.com Internet Source	<%1
21	www.readbag.com Internet Source	<%1
22	es.scribd.com Internet Source	<%1
23	Bouillaguet, C., P. Derbez, O. Dunkelman, P.A. Fouque, N. Keller, and V. Rijmen. "Low-Data Complexity Attacks on AES", IEEE Transactions on Information Theory, 2012. Publication	<%1
24	Ratha, Paresh, Debabala Swain, Bijay Paikaray, and Subhadra Sahoo. "An Optimized Encryption Technique using an Arbitrary Matrix with Probabilistic	<%1

Encryption", Procedia Computer Science, 2015.
Publication

25	C. U. M. Smith. "A strand of vermicelli: Dr Darwin's part in the creation of Frankenstein's monster", Interdisciplinary Science Reviews, 03/01/1996 Publication	<%1
26	www.cse.tkk.fi Internet Source	<%1
27	ijcsit.com Internet Source	<%1
28	csrc.nist.gov Internet Source	<%1
29	Khakurel, Suman, Prabhat Kumar Tiwary, Niwas Maskey, and Gitanjali Sachdeva. "Security vulnerabilities in IEEE 802.11 and adaptive encryption technique for better performance", 2010 IEEE Symposium on Industrial Electronics and Applications (ISIEA), 2010. Publication	<%1
30	www.csd.uwo.ca Internet Source	<%1
31	"Voice Encryption using RSA Algorithm", University/Engineering, 2009-03-08 Publication	<%1

Saxena, Neetesh, and Narendra S.

32	Chaudhari. "An enhanced NPA protocol for secure communications in GSM network", International Journal of Security and Networks, 2013. Publication	<%1
33	Kayvan Tirdad. "Hopfield neural networks as pseudo random number generators", 2010 Annual Meeting of the North American Fuzzy Information Processing Society, 07/2010 Publication	<%1
34	thehackernews.com Internet Source	<%1
35	www.skarderud.net Internet Source	<%1
36	Anjum. "Introduction", Security for Wireless Ad Hoc Networks, 02/02/2007 Publication	<%1
37	spi.unob.cz Internet Source	<%1
38	www.rane.com Internet Source	<%1
39	documents.mx Internet Source	<%1
40	www.assuredbydesign.com Internet Source	<%1
41	Lecture Notes in Computer Science, 2009. Publication	<%1

42	www.certbibles.com Internet Source	<%1
43	213.55.83.214:8181 Internet Source	<%1
44	Piper, F.. "Incidence structures applied to cryptography", Discrete Mathematics, 19920901 Publication	<%1
45	citeseerx.ist.psu.edu Internet Source	<%1
46	Advances in Intelligent Systems and Computing, 2016. Publication	<%1
47	Kanhe, Aniruddha, G. Aghila, Ch. Yaswanth Sai Kiran, Ch. Hanuma Ramesh, Gabbar Jadav, and M. Gowtham Raj. "Robust Audio steganography based on Advanced Encryption standards in temporal domain", 2015 International Conference on Advances in Computing Communications and Informatics (ICACCI), 2015. Publication	<%1
48	Velayutham, R. and Manimegalai, D.. "Enhancing Confidentiality and Integrity in IEEE 802.11i Wireless Networks using AES-CCMP", European Journal of Scientific Research, 2011. Publication	<%1

49	www.ict.tuwien.ac.at Internet Source	<%1
50	www.springer.com Internet Source	<%1
51	ethesis.nitrkl.ac.in Internet Source	<%1
52	Fred C. Piper. "Codemakers versus Codebreakers", Interdisciplinary Science Reviews, 12/01/1990 Publication	<%1
53	Ahmad, Musheer, Omar Farooq, Sekharjit Datta, Shahab Saquib Sohail, Anoop L. Vyas, and David Mulvaney. "Chaos-based encryption of biomedical EEG signals using random quantization technique", 2011 4th International Conference on Biomedical Engineering and Informatics (BMEI), 2011. Publication	<%1
54	Lecture Notes in Computer Science, 2013. Publication	<%1
55	Heiser, Jay, Steve Stanek, Sasan Hamidi, Ben Rothke, Paul Lambert, Ralph Spencer Poore, James Tiller, Ronald Gove, and Mark Edmead. "Methods of Attacking and Defending Cryptosystems", Information Security Management Handbook on CD-ROM 2006 Edition, 2006. Publication	<%1

56	Eljadi, Fardous Mohamed, and Imad Fakhri Al-Shaikhli. "Statistical Analysis of the eSTREAM Competition Winners", 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2015. Publication	<%1
57	Patidar, Vinod. "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing", Informatica (03505596)/03505596, 20091101 Publication	<%1
58	Delgrossi, . "Cryptographic Mechanisms", Vehicle Safety Communications Protocols Security and Privacy, 2012. Publication	<%1
59	Wang, Cliff X., William J. Chimiak, and Steven C. Horii. "", Medical Imaging 1999 PACS Design and Evaluation Engineering and Clinical Issues, 1999. Publication	<%1

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		