Improved AES Algorithm for Key Generation in Stream Cipher for MANET Security

[1]Mansi Sharma, [2]Ajay Kumar, [3]Alpana Agarwal

[1]Master of Engineering, [2]Research Scholar, [3]Associate Professor
[1]Electronics and Communication Department,
[1]TIET, Patiala, India.

Abstract : In this paper, firstly an overview on MANET, their attacks, and encryption module are defined. In addition, a survey is carried out for MANET security. From, the survey found that AES is most used algorithm for data encryption as well as for key generation. The AES algorithm provides good security but not efficient in resource constraint devices. So, an Improved AES algorithm as an application for key generation for stream ciphers is proposed. In the Improved AES algorithm, by using Rijndaels substitution box and dynamic random shifting principle by reducing area and complexity as compared to AES, produced equivalent randomness. This paper introduces the concept of use of random initialization vector (IV) for resolving the replay attack on the network. The IV is randomly updated in each iteration and dependence of secret key on IV using nonlinear function producing the randomness of key. Moreover, based on NIST statistical analysis, it shows that more randomness is produced by proposed technique than A5/1 stream cipher.

***IndexTerms* – MANETs, Security, Key Generation in Stream Cipher, Improved AES, Initialization vector.**

I. INTRODUCTION

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 (Sakshi Sachdeva, Parneet Kaur, 2016).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.
- Infrastructure-less Network. Infrastructure-less network where there is no centralized node such as MANETs (Mobile Ad-hoc networks) in which temporarily designed network with no previously designated infrastructure.

The comparative analysis between infrastructure and infrastructure-less network is done in table 1. 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.

Table 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.

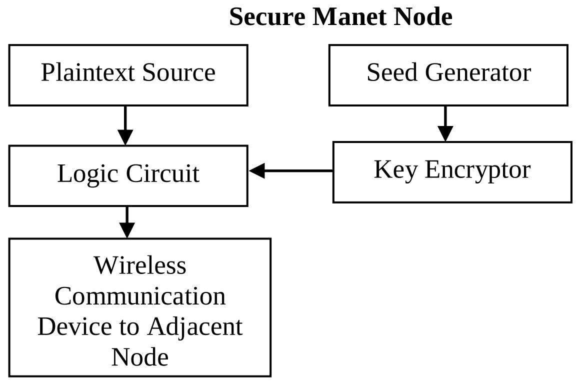

Figure 1 Encryption Module of Data Stream in MANETs

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 (Gurjeet Singh, 2011).

1.1 Attacks on MANETs

In the MANET, 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. The 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 Failed nodes , Badly failed nodes , Malicious nodes , Selfish nodes (Aarti , S. S. Tyagi 2013). The 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 (Sakshi Sachdeva, Parneet Kaur, 2016).

1.2 Need of Cryptography in MANETs

There are major threats to MANETs due to various attacks discussed in the Section 1.1, so securing the message packets and authentication of nodes is the at most important task for MANET's security (Mohammad, *et al.* 2014). In the Figure 1 shows a flow diagram of secure data communication where 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. There are two methods of random number generation i.e. True Random Number Generators (TRNG) and Pseudo-Random Number Generators (PRNG). 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. Securing data can be achieved by cryptography algorithm which can be classified based on the key used if single key is used, it can be referred as symmetric key algorithms. Encryption of packets at sender nodes is usually done using symmetric key algorithms.

Symmetric key cryptography can be divided into two categories:

- **Block ciphers:** In block cipher, the data streams break into fixed length and same operation applied on each block for data encryption.
- **Stream ciphers:** In stream cipher, bit by bit operation is done. The stream ciphers are faster than block cipher, are preferred for cases where the amount of data is continuous or either unknown - such as network streams. The stream ciphers are further differentiated based on key generation mechanism.
    - **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.
    - **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.

On the other hand, 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 (Ayushi 2010).

This paper is organized as: In section 2, survey of symmetric algorithm along with generation key is done from various research papers discussing the limitations of some work defined and obtaining solutions to overcome them. In section 3, based on the study, work to solve these issues are defined In section 4, AES and improved AES are used as pseudo random number generator as an application in Key generation using varying initialization vector and secret key for each packet transmission for stream cipher and randomness of key generated is verified by performing statistical test by NIST. Section 5 includes the conclusion of the complete proposed work and analysis of performance parameters of work done.

II. Literature Survey

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

Kavita T.Patil, *et al.* 2014 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 execution time along with introduction of new S-box which is used for both encryption and decryption process. This propose design is implemented with CGA (Cryptographically Generated Address) and compared with the use of SHA-1(Secure Hash Algorithm-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 .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 analyzed based on parameters like computation complexity, storage requirement, and overhead generated (Kumar, et al. 2016). An enhanced version of Key generation is discussed 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. Simulation of the work is done on MATLAB using R2010a simulator (Solanki, *et al.* 2013). The author (Pankaj, *et al.* 2016), came up with an improved LFSR based stream algorithm for Key generation. 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 Nonlinear combination function. Implementation is done on MATLAB and randomness of generated key is verified by using Randomness Test Suite defined by NIST such as Block Frequency Test, Approx. Entropy Test, Frequency Test, FFT, Linear Complexity Test, Longest Run Test *etc*. (Paresh Ratha, *et al.* 2015), presented an optimized cryptography algorithm using arbitrary matrix key for key sequence generation by multiplying by an initialization vector and by performing further conversions. Performance is evaluated by considering the parameters such as execution time, throughput and Avalanche Effect. (Peng Zhang *et al.* 2016**)**, focused 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. **(**Yang Cao *et al.* 2016), has shown comparative analysis of various cryptography algorithm 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**.** (Shruti Patel *et al.* 2016) 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.* 2014), 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.

III. MOTIVATION

The survey shows that AES, Linear Feedback Shift Register (LFSR) are the most used elements for key generation in stream cipher. The authors (Amit Kumar, *et al.* 2016**)**, discussed key generation using AES with reduced number of mix column operation and concept of fixed IV 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, using fixed IV in each iteration reduces the randomness of the key generated and secrecy of IV. The authors (Pankaj, *et al.* 2016)**,** used LFSR for key generation. 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). The LFSR required very less hardware for implementation but the limitation is that LFSR Boolean expression easy to analyze and also repeated sequence produced if properly xoring of bits is not done. So, random key generation mechanism is proposed using improved AES algorithm. Also, in place of fixed IV for each iteration the IV is randomly updated.

IV. PROPOSED WORK

The proposed work's modeling and simulation is done on MATLAB 2013a.

4.1 Overview of Improved AES Algorithm

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. 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 Figure 2.

- **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.

  Random Dynamic Shifting: The random dynamic shifting principle is taken from the Boron Cipher permutation layer (Bansod, *et al.* 2017). In random dynamic shifting, the 128 bit stream is divided into 4 rows and each row 32bit long. 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, which has obtained by mix column operation in original AES. Since mix column is a complex operation requires a large amount of memory and execution cycles, to resolve this step random dynamic shifting is used to obtain comparative avalanche effect using simple permutation and cascaded XOR operation.

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

```
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 2 Pseudo code of Improved AES

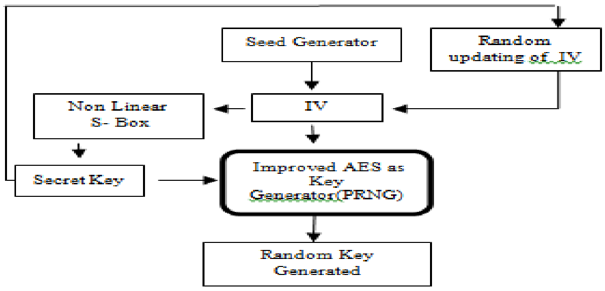

Figure 3 Key Generation Mechanism by PRNG

4.2 Key Generation using Improved AES Algorithm

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) (Mohit Kumar, Anju Chahal 2014). In the proposed design, initial 128-bit seed point is defined by the sender, which can be transmitted over the channel. This initial seed is circular rotated based on the initial message packet. The circular rotation is basically modular arithmetic and depends on the number of 1's concentration in initial message packet. The secret key is obtained by applying non-linear function on IV to reduce correlation between IV and secret key which can produce randomness in the key generated. For the next message packet or nth message packet, the IV is updated based on a varying number of ones in $(n-1)^{th}$ secret key i.e. value based left rotation is performed on 128 bit $(n-1)^{th}$ secret key. The key generation mechanism is shown in Figure 3.The supreme advantage of random rotation and non-linear function steps 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.

4.3 Experimental Results and Performance Analysis

The code is written in MATLAB 2013a and the performance evaluation of proposed key generation algorithm is done using statistical random test suite that is recommended by National Institute of Standards and Technology (NIST) (Rukhin, *et al.* 2010). The test suites used in our proposed algorithms are

- ***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. The entire subsequent tests are dependent on passing of this test.
- ***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.
- ***Approximate Entropy Test:*** Entropy is a measure of uncertainty of a sequence generated. It basically measure the randomness of a sequence usually represented in bits. It represents the frequency of all overlapping blocks patterns in the entire sequence.

Table 2 Statistical Test for randomness of Key Generation Techniques

Serial No.	Test Name	P-value	P-value	P-value
		A5/1 (Pankaj, *et al.* 2016)	AES with IV updating	Improved AES with IV updating
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

- ***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 on's within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence [18].

The comparative analysis of proposed technique with existing technique is shown in Table 2. The results reflects that the proposed technique have better randomness as compared to A5/9 algorithm and approximate equal as in existing AES algorithm.

V. CONCLUSION

A key generation mechanism is proposed using AES and improved AES as an application of block cipher in stream ciphers to produce a highly random 128 bit key stream. Rijndael S-box and Key expansion mechanism is taken from the AES while instead of shift row and mix column transformation which was a much complex operation, a much simple but effective mechanism of random dynamic shifting is used to produce improved AES providing randomness to the key generated and simulation is done on MATLAB. The proposed work completely satisfy the desired expectation of randomness of key by satisfying the tests done based on NIST analysis program as shown in Table 2 where 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 and shows better randomness when compared with the A5/1 stream ciphers. It assures that the resulting stream cipher algorithm is highly secure.

REFERENCES

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

[2] Gurjeet Singh 2011. Security Threats and Maintaince in Mobile Adhoc Networks. International Journal of Electronics & communication technology, 2(3): 68-70

[3] Aarti , S. S. Tyagi 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] Mohammad S. Obaidat Isaac Woungang, Sanjay Kumar Dhurandher, Vincent Koo 2014. A cryptography-based protocol against packet dropping and message tampering attacks on mobile ad hoc networks. Journal of Security and Communication Network,7:376-384

[5] Ayushi 2010. A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications, 1(15):0975 – 8887.

[6] Kavita T.Patil, Manoj E.Patil 2014. Improve the Security of CGA using Adjustable Key Block Cipher based AES, to Prevent Attack on AES in IPV6 over MANET. IEEE Global Conference on Wireless Computing and Networking (GCWCN), 148-152.

[7] Amit Kumar, Vijay K. Katiyar and Kamal Kumar 2016. A Purely Localized Random Key Sequencing Using Accelerated Hashing in Wireless Ad- Hoc Networks. 5th International Conference on Frontier in Intelligent Computing: Theory and Applications, 2: 269- 279.

[8] Mayur Solanki, Seyedmohammad Salehi, and Amir Esmailpour 2013. LTE Security:Encryption Algorithm Enhancements. ASEE Northeast Section Conference.

[9] Pankaj, Asit Kumar Singh, Bhupendra Singh Bora 2016. Design of Enhanced Pseudo-Random Sequence Generator usable in GSM Communication. IEEE WiSPNET conference, 530-534.

[10] Paresh Rathaa , Debabala Swainb , Bijay Paikarayc,Subhadra Sahoo 2015. An optimized encryption Technique using an arbitrary matrix with probabilistic encryption. 3rd International Conference on Recent Trends in Computing, 57:1235-1241

[11] Peng Zhang,Chuang Lin 2016. Lightweight Encryption for Random Linear Network Coding. Security in Network Coding, 43-68.

[12] Liehong Wu and Ilia Detchenkov, Yang Cao 2016. A Study on the Power Consumption of Using Cryptography Algorithms in Mobile Devices. 7th IEEE International Conference on Software Engineering and Service Science.

[13] Shruti Patel, Fenil Khatiwala 2016. A Review Paper of an Encryption Scheme using Network Coding for Energy Optimization in MANET, IEEE WiSPNET conference.

[14] Sunil Kumar Sahu, Ajay Kushwaha 2014. Performance Analysis of Symmetric Encryption Algorithms for Mobile ad hoc Network. International Journal of Emerging Technology and Advanced Engineering, 4(6):619-624

[15] R.D. Sparrow, A .A .Adekunle , R .J. Berry 2016. LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion. 10th International Conference on Signal Processing and Communication systems.

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

[17] Mohit Kumar, Anju Chahal 2014 Effect of Encryption Technique and Size of Image on Correlation Coefficient in Encrypted Image International Journal of Computer Applications,97(12): 0975-8887

[18] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, Davi Banks, Alan Heckert, James Dray, San Vo 2010. A Statistical Test Suite for Random and Pseudorandom Number Generators, for Cryptographic Application. Computer Security,1a.