Secured Approach to Implement Using a KEY Counter and AES for MANETS

1Dr. Mamatha C M, 2Jagadish P, 3Anjank Koundinya
1Associate Professor, 2Assistant Professor, 3Assistant Professor
1Cambridge Institute of Technology North Campus,
2BMS, Institute of Technology and Management, Bengaluru,
3BMS, Institute of Technology and Management, Bengaluru

Abstract - **Mobile Adhoc network is the most sophisticated promising technology in the field of Wireless communication. MANETs essentially have the competence of enabling peer to peer communication between the nodes with decentralized network architecture. MANETs are relevant chiefly to military applications, mobile communications, home networking and rescue operations. Practically, data mobility in such decentralized networks could be attacked using manifold methods in numerous ways. As MANETs does not befit the security mechanism associated with static networks, the current exploration on MANET emphasizes on the secure data mobility issues. This paper primarily emphasizes on securing data and its mobility using ciphers, incorporated in MANETs. It puts forth the realization of Advanced Encryption standard using a biometric key counter for MANETs. Biometric Advanced Encryption Standard with Key Counter (BAESK) implementation includes the design of most robust sub key selection realization for presented AES. The key for AES is obtained by precise biometric processing. In this paper, the plain text input is encrypted using the BAESK cipher and is decrypted using the reverse process.**

keywords - **MANET, AES, RSA, DES, Biometric, key counter**

I. INTRODUCTION

MANET is non static environment and has the potential to send out signals in linking mobile nodes. Their self-design attribute fundamentally deals with self-motivated aspect of the stirring nodes. MANETs lack a structured infrastructure in line to ascertain secure data mobility. Thus impose inadequacy in processing ability, throughput and performance of the system [1].

Taking memory and processing power into consideration Cipher for MANET is to be designed. There is a soaring demand for high level security systems to be designed for MANET infrastructure. Literature from decades throws light on innumerable ciphers applicable to such network. Most admired cipher pointed to in literature is Advanced Encryption Standard (AES). Key generation and selection for encryption or decryption of message is a vital aspect in ciphers. Use of asymmetric or symmetric key states its own merits and demerits in securing data mobility. Securing data at minimal processing power in context of MANET is the objective.

The generation of symmetric key in literature is made complex by integrating biometric input [6][7][9]. Substitution-box used for encryption process is generated using Galios Field GF (2^n) which has greater design complexity and is difficult to crypt analyze. Normal key generation and expansion in AES confronts security threats. Nevertheless ciphers in MANET can be made more secure by incorporating enhanced features. Out of the many popular and extensively used authentication systems biometric processing stands out. Magnitude of research is done on different type and methods of processing. Biometrics has two classifications, physical biometric and behavioral biometric. Fingerprint which falls into physical genre is considered as most convenient approach in context of MANET.

II. RELATED WORK

In cryptography, block cipher and stream cipher are two genres of cipher and symmetric key and asymmetric key are two genres of keys used. Block cipher, a symmetric key cipher operating on aggregation of bits with fixed length and immutable transformation is termed as a block.

Elliptic Curve Cryptography was devised as an auxiliary mechanism to implement public-key cryptography. ECC is mainly based on elliptic curve theory. ECC has the capability of creating smaller and faster, effective keys comparatively with its counterparts. In ECC elliptic curve equation is made use of for encryption. ECC yields an effective security level with 164 bit key, whereas its counterparts may require 1024 bit key to achieve an equivalent level of security. Hence ECC offers at most security with reduced bit sizes, while being power efficient.

International Data Encryption algorithm is one of the genres of block encryption algorithms which were illustrated initially in 1991. The native algorithm was subjected to series of modifications and eventually acquired the name International Data Encryption Algorithm. IDEA operates with blocks of 64-bit cipher text and 64-bit plain text, which is further divided into four 16 bits sub-blocks for encryption purpose. It is governed by 128 bit key. IDEA was made use of in Pretty Good Privacy and is also an optional algorithm in Open PGP standard

Twofish is one of the illustrations for symmetric block cipher based algorithms, having a symmetric structure. It came into existence in 1998 and embellished later on. It works effectively with firmware or software on smaller processor. It permits

developers to tailored encryption celerity, size of the code and time complexity involved in key setup, to balance performance requirements. Twofish encryption operates with 128, 192 or 256 bits key sizes. Threefish a symmetric key block cipher was first proclaimed in 2008 and is a tweakable block cipher. It has a direct reference to Blowfish and Twofish. Input to a tweakable block cipher algorithm is a block of message, a key and a tweak. In Threefish every block of message is encrypt using unique 128 bits nibble value. The keys employed for encryption in Threefish are equal to the block size and may be varying in length as 256 bits, 512 bits or 1024 bits.

The RSA a public-key encryption algorithm is one of the most standard and impregnable encryption algorithms. This algorithm exploited the fact that a no proper way existed to factor numbers of huge magnitude ranging from 50 to 200 digits.

Triple DES designed to address inadequacy in DES is just advancement to existing DES without modeling entirely a new cryptosystem. Triple DES applies DES algorithm thrice in succession using three identical keys by simply extending the key size of DES. The amalgamated key size of Triple DES is 3 times of 56 which is equivalent to 168 bits. 168 bits key size cannot be easily surpassed by brute-force practices. No serious flaws in design of Triple DES have been discovered. It finds its applications in a number of Internet protocols.

III. BIOMETRIC ADVANCED ENCRYPTION STANDARD WITH KEY COUNT

The prime idea is to design a cipher which is well-matched with MANET environment.

The most suited cipher in context of MANET is AES. The cipher proposed uses the cryptographic system, AES. AES with biometric key is used here to secure data mobility over dynamic wireless network like MANET. In symmetric key ciphers a pre shared key is used. Similarly in the proposed Biometric Advanced Encryption Standard with Key count (BAESK) design, a pre shared key is generated using Fingerprint Biometric trait. The key for encryption is used by selecting a 16-byte sub key based on a key count value. The key count value is obtained by the sequence number of packets transmitted. Later the sub key is given to key expansion process and used in order to encrypt the 128-bit plain text or decrypt the 128-bit cipher text.

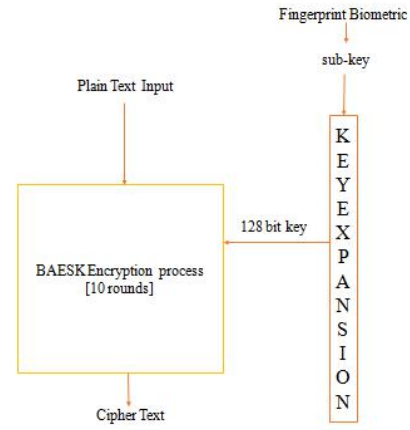

Fig. 1. BAESK encryption architecture

As shown in fig 1. 128-bit plain text input which is intended to be transmitted is encrypted by transforming the text using 10 rounds of following phases , add round Key, Shift rows, mix columns and Substitution using S-box. The 128-bit key, used in add round key phase is, the expanded biometric sub key obtained from fingerprint trait.

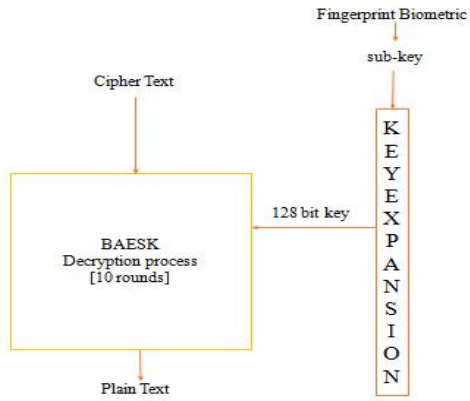

Fig. 2. BAESK decryption architecture

Message to be transmitted is sent in terms of 128-bit blocks. First plain text block is encrypted using first 16-bytes of key, second plain text block is encrypted using next 16-bytes and the process repeats for all the data blocks that needs to be transmitted. Employing this scheme provides two levels of security for secure data mobility in MANETs.

The encrypted plain text is identified as cipher text. In decryption process as shown in fig 2, the cipher text undergoes inverse of encryption process to decipher and obtain the plain text that is the original message.

IV. IMPLEMENTATION

A variety of data communication networks use AES cipher. It works with data block size of 128 bits, which is transformed to be called the cipher text. AES is implemented using biometric key and its sub keys as an integral part of the cipher. It also generates a substitution matrix S-box which is a vital element of AES and aids in encryption process.

A. Biometric based key generation

The steps for biometric key generation are stated below:

Step 1: Considering the Region of Interest identify number of Minutiae points.
Step 2: Obtain the modulus of total Minutiae points by 128
Step 3: Calculate P= P-Rem, from step 2.
Step 4: obtain a value I= P/128. I value provides number of recursive iteration required. It is necessary to perform key compression to 128-bit.
Step 5: for 1 to I, Drop 64 bit Right and 64 bit Left. Remaining key set is divided into N_R and N_L. Swap N_R and N_L.
Step 6: Finally, these 128 bits are converted to hexadecimal values.

B. Biometric based key selection

The steps in selecting biometric sub key are stated below:

Step 1: Identifying number of blocks in message to be transmitted.
Step 2: For the first block b0 to be transmitted assign key counter value k=n, n=1,2,3…m (n value is based on the sequence number of message that is transmitted it can range from 1 to m)
Step 3: for k=1 to m,
if k=1 first 16 bytes of biometric key is selected
if k=2 next 16 bytes of biometric key is selected
……
if k=m, m^{th} 16 bytes of biometric key is selected
Step 4: Finally selected sub key is input to key Expansion process.

V. COMPARATIVE STUDY OF AES AND BAESK

This section gives comparison of the ciphers BAESK and AES. The performance metric taken into account for comparison are memory utilized by the cipher and time taken for execution of cipher. Fig 7, clearly depicts time taken in milli seconds to encrypt the input plain text using AES and BAES.

X-axis represents 128- bits in input plaintext block which are encrypted using existing AES and simulated BAESK. Y-axis represents time taken to encrypt the input plain text.

The time taken and memory utilized by both the cipher is tabulated in Table I. Simulation results show that AES and BAESK utilize same amount of memory but BAESK provides better security with a minimal time over head.

TABLE I Comparison of AES and BAESK

Parameters	AES	BAESK
Memory utilized	16KB (64 bits data)	16KB (64 bits data)
Time in milli sec	70	107

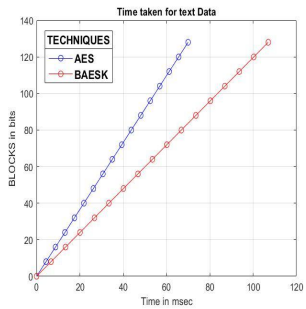

Fig. 3. Time taken to encrypt text data in AES and BAESK

A. Comparative Study of DES and BAESK

This section gives an analysis of the proposed BAESK cipher with existing DES cipher. Fig 8, shows time taken in milli seconds to encrypt input plaintext using DES and BAESK.

From simulation study, it is observed that BAESK utilizes lesser memory when compared to DES, providing better security with a minimal processing time overhead.

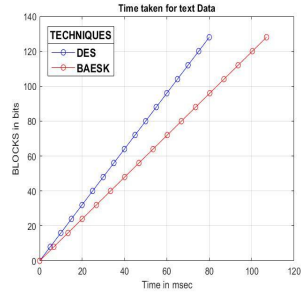

Fig. 4. Time taken to encrypt text data in DES and BAESK

Table II gives comparison of DES and BAESK considering Memory utilized and processing time.

TABLE II Comparison of DES and BAESK

Parameters	DES	BAESK
Memory utilized	20KB (128bit data)	16KB (64 bits data)
Time in milli sec	80	107

B. Comparative Study of RSA and BAESK

This section gives an analysis of the proposed BAESK cipher with existing RSA cipher. Fig 9, clearly indicates time taken in milli seconds to encrypt input plain text using RSA and BAES.

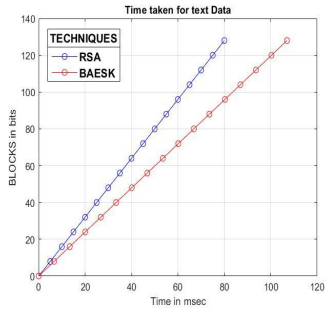

Fig. 5. Time taken to encrypt text data in AES and BAESK

Table III gives comparison of DES and BAESK considering memory utilized and processing time.

From Table III, we observe that BAESK utilizes lesser memory when compared to RSA, but with a minimal time overhead.

TABLE III Comparison of RSA and BAESK

Parameters	RSA	BAESK
Memory utilized	30KB (128 bits data)	16KB (64 bits data)
Time in milli sec	81	107

C. Comparative Study of avalanche effect

Avalanche effect is one of the metrics used to measure the efficiency of ciphers. Avalanche effect is the ratio of number of bits changed in cipher text for one bit change in input text or one bit change in key used, by the total number of bits in cipher which is multiplied by 100. Avalanche effect is represented using eqn (1)

$$Avalanche\ Effect = \frac{number\ of\ bits\ changed\ in\ cipher\ text * 100}{total\ number\ of\ bits\ in\ Cipher\ text} \quad (1)$$

VI. CONCLUSION

The Biometric Advanced Encryption Standard Algorithm has emerged as promising encryption techniques for data mobility in MANET routing protocol. Even though the implementation of BAES is simple, the multi dimensional features involved in the mechanism of BAES needs a proper understanding. The rich securities for data mobility with good performance metric of BAES is due to the contribution of fingerprint biometric and the pre calculated hop count value between source node and destination node in AODV protocol. The study and understanding of each of these concepts is vital.

The primary objective of the present research is to investigate this multi dimensional sophisticated encryption algorithm through simulation and numerical study. To fulfill this goal, two different experimental setups have been considered and tested. Numerical models were used to study the encryption and decryption process at various nodes in MANET. This paper implements a cipher for secure data mobility for MANET application. The cipher is designed using Biometric as a key to AES. For Encryption or decryption process a sub key from the biometric key is selected, which defines multiple levels of security. The biometric input is selected based on the feasibility for this context. It is processed to extract minutiae with optimum processing complexity. Biometric key is preferred here since in symmetric ciphers like AES key plays a vital role and it is easy to replace the biometric key, in the worst possible case if any cryptanalyst knows the existing key.

REFERENCES

[1] Amol Bhosle, Yogadhar Pandey, "Applying Security to Data Using Symmetric Encryption in MANET" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013)

[2] T. Priyanka and E.Ramara, "Biometric Based Authentication for MANET Using Efficient Fingerprint", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 3, Special Issue 20, April 2016
[3] Bawna Bhat,Abdul Wahid Ali and Apurva Gupta, "DES and AES Performance Evaluation", published in proceedings of International Conference on Computing, Communication and Automation (ICCCA) 2015.
[4] Tingyuan Nie and Teng Zhang," A Study of DES and Blowfish Encryption Algorithm" ,published in IEEE 2009, 978-1-4244-4547-9/09
[5] Amish Kumar and Namita Tiwari," EFFECTIVE IMPLEMENTATION AND AVALANCHE EFFECT OF AES",published in International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.
[6] S. Sridevi Sathya Priya & P. Karthigaikumar, "Mixed Random 128 Bit Key Using Finger Print Features and Binding Key for AES Algorithm", 978-1-4799-6629-5/14/$31.00_c 2014 IEEE
[7] S. Sridevi Sathya Priya, P. Karthigaikumar, and N.M. SivaMangai, "Generation of 128-Bit Blended Key for AES Algorithm", © Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Emerging ICT for Bridging the Future Volume 2, Advances in Intelligent Systems and Computing 338, DOI: 10.1007/978-3-319-13731-5_47.
[8] Jong Yeon Park, Dong-Guk Han, Okyeon Yi and Dooho Choi, "Ghost Key patterns with equidistant chosen message attack on RSA-CRT", proceedings of 2011 Carnahan Conference on Security Technology, 18-21 October 2011.
[9] Michael Bourg and Pramod Govindan, "RSA Based Biometric Encryption System Using FPGA for Increased Security", 978-1-5090-1071-1/16, 2016 IEEE.
[10] Asma Chaouch, Belgacem Bouallegue and Ouni Bouraoui, "Software Application for Simulation-Based AES, RSA and Elliptic-Curve Algorithms", proceedings of 2nd International Conference on Advanced Technologies for Signal and Image Processing- ATSIP'2016, March 21-24,2016, Monastir, Tunisia.
[11] P. Kocher, J.Jaffe, and B.Jun, "Differential Power Analysis", in 99, ser.LNCS, vol.1666. Springer-Verlag, 1999, pp.388-397
[12] Levent Ordu and Berna Ors, "Power Analysis Resistant Hardware Implementation of AES", 1-4244-1378-8/07/$25.00, 2007 IEEE.
[13] Weiming Yang Jinhui Xu Yingjian Yan Kai Liu," Research on Time Randomization of AES against Differential Power Analysis", 978-0-7695-3865-5/09 $26.00, 2009 IEEE.
[14] ZOU Cheng, ZHANG Peng, XIANG Kai-quan,ZHAO Qianng, "Implementation of AES with Handshake Protocol against Differential Power Analysis", 978-0-7695-4031-3/10 426.00, 2010 IEEE.
[15] Hridoy Jyoti Mahanta and Ajoy Kumar Khan, "A Heuristic Approach to Identify AES Cryptosystem from the Power Traces", 978-1-4673-6708-0/15/$31.00,2015, IEEE.