The International Journal Of Engineering And Science (IJES)
|| Volume || 3 || Issue || 3 || Pages || 07-12 || 2014 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN

[1,] Ms. Ankita Umale, [2,] Ms. Priyanka Fulare
[1, 2,] *Department of Computer Science and Engineering, G.H.R.I.E.T.W*

ABSTRACT

Advanced mobile devices, known as smartphones, are a class of devices built at their core around ease of connectivity and always-on accessibility of online services. Security is one of the most challenging aspects in the internet and network applications. Symmetric key algorithms are a typically efficient and fast cryptosystem, so it has significant applications in many realms. For a Mobile adhoc network with constraint computational resources, the cryptosystem based on symmetric key algorithms is extremely suitable for such an agile and dynamic environment, along with other security strategies. The paper presents a comparison study of block ciphers such as AES, DES, 3DES, Blowfish, RC2, and RC6 on the basis of block size, key size, and speed.

Keywords- *Mobile caching, symmetric encryption, AES, DES, 3DES, Blowfish, RC2, and RC6*

Date of Submission: 10 February 2014 Date of Acceptance: 15 March 2014

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is comprised of a group of mobile nodes which have the capability of self organization in a decentralized fashion and without fixed infrastructure [1]. A fundamental method of data protection in the area of information and network security is cryptography, which has been widely accepted as a traditional platform of data protection for decades. Through the data encryption and decryption, the protection of data confidentiality and integrity are achieved. However, based on the features of wireless devices, a mobile ad hoc network has special security and efficiency requirements for conventional cryptographic algorithms. The concept of caching frequently accessed data provides efficient communications among mobile nodes. Through the data encryption and decryption, the protection of data confidentiality and integrity are achieved. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blow-fish, and AES.

RC2 uses one 64-bit key. DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blow¯sh uses various (32-448); default 128bits while RC6 is used as various (128,192,256) bit keys.

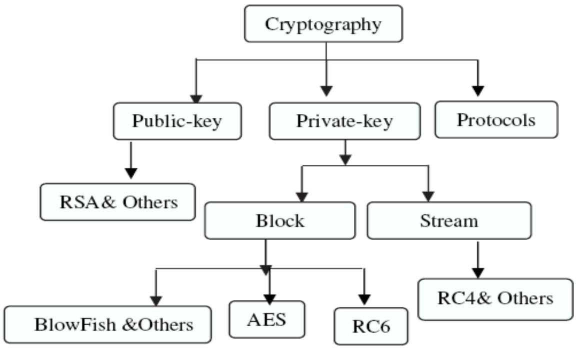


Fig. 1: Classification of symmetric Encryption Algorithms

This paper examines a method for evaluating performance of selected symmetric encryption of various algorithms. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Battery power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at a slower rate than other technologies. This causes a “battery gap” [9], [10].We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices. This study evaluates six different encryption algorithms namely; AES, DES, 3DES, RC6, Blowfish, and RC2. The performance measure of encryption schemes will be conducted in terms of energy, changing data types -such as text or document and images- power consumption, changing packet size and changing key size for the selected cryptographic algorithms.

II. LEATERATURE REVIEW

In [1], MANET environment, data caching is essential because it increases the ability of mobile devices to access desired data and improve overall performance. Data accessibility in ad hoc network is lower than that in conventional fixed network. Encryption algorithms play a main role in information security systems.In [2], This paper provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types ,battery power consumption, different key size and finally encryption/decryption speed.In [3], W.Zhang and G. Cao introduces Caching techniques that can be used to reduce bandwidth consumption and data access delay in wireless ad hoc networks. Various algorithms has been studied to deal with cache invalidation strategies by A.Elmagarmid, J.Jing, A. Helal, and C. Lee in [8],[9]. The security algorithm for cache consistency in [5],[12] the author gives a comparative study of various security algorithm like AES, DES, 3DES, RC2, Blowfish and RC6 . Caching has been well accepted method to ease the ever growing bandwidth needs, reduce the server load, and decrease the client access latency. In a typical ad hoc environment each node acts as router and transceiver. M. Abolhasan, T. Wysocki and E. Dutkiewicz [2] focuses on several caching techniques and routing protocols are implemented to tackle the problem of MANET environment such as node mobility and resource (battery and bandwidth) consumption .

III. CRYPTOGRAPHY WITH BLOCK CIPHER

In Cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and outputs a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of cipher text together with the secret key, and yields the original 128-bit block of plaintext. To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used. Block ciphers can be contrasted with stream ciphers; a stream cipher operates on individual digits one at a time and the transformation varies during the encryption. The distinction between the two types is not always. clear-cut: a block cipher, when used in certain modes of operation, acts effectively as a stream cipher as shown in Fig 2.

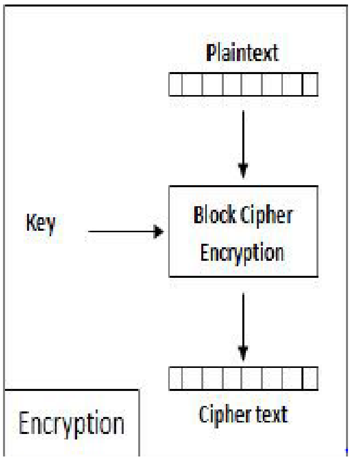


Fig 2: Encryption process

An early and highly influential block cipher design is the Data Encryption Standard (DES). The (DES) is a cipher (a method for encrypting information) Selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm was initially controversial, with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny, and motivated the modern understanding of block ciphers and their cryptanalysis. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard .

3.1 Data Encryption Standard (DES)

56-bit key is used in DES and 16 cycle of each 48-bit sub keys are formed by permuting 56-bit key. Order of sub keys is reversed when decrypting and the identical algorithm is used. Block size of 64-bit is made from L and R blocks of 32-bit.

3.2 Triple DES

Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force

3.5 RC2

RC2 is a symmetric block cipher that operates on 64 bit (8 byte) quantities. It uses a variable size key, but 128 bit (16 byte) key would normally be considered good. It can be used in all the modes that DES can be used. A proprietary algorithm developed by RSA Data Security, Inc.,. The algorithm expands a single message by up to 8 bytes. RC2 is a block cipher that encrypts data in blocks of 64 bits.

3.6 RC6

RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. RC6 is patented encryption algorithm and is rolalty free. It is very similar to RC5 in structure, using data-dependent rotations, modular addition and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

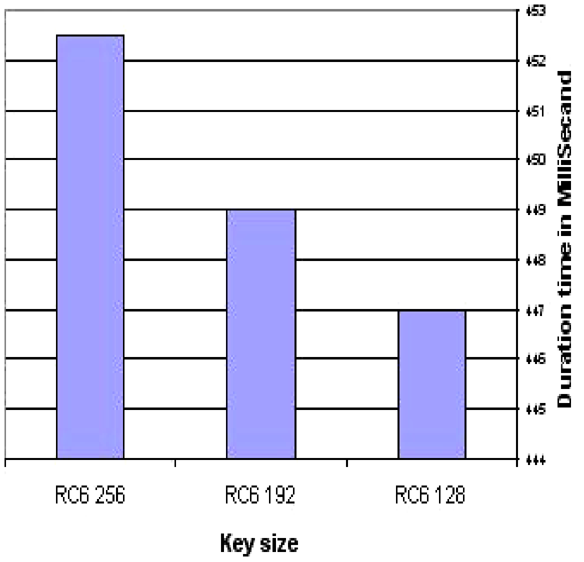


Fig 3: *Time consumption for different key size for RC6*

RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard

3.7 BLOWFISH

Blowfish is 64-bit block cipher- used to replace DES algorithm. Ranging from 32 bits to 448 bits, variable-length key is used. Variants of 14 round or less are available in Blowfish. Blowfish is unpatented and license-free and is available free for all uses. Blowfish is one of the fastest block ciphers developed to date. Blowfish suffers from weak keys problem, still no attack is known to be success.

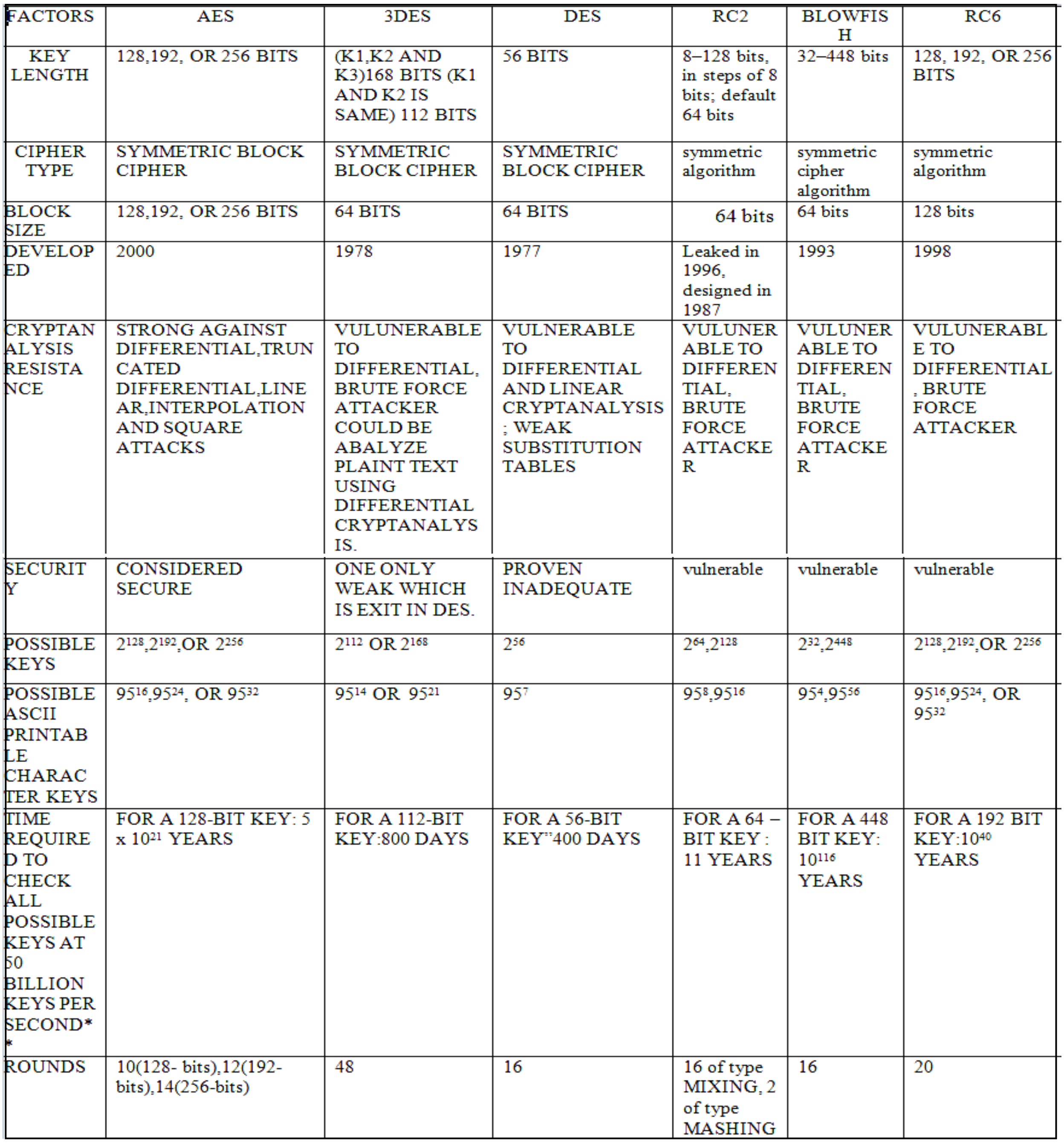
IV. COMPARISON BETWEEN AES, 3DES, DES, RC2, RC6 AND BLOWFISH

Advance Encryption Standard (AES) and Triple DES (TDES or 3DES) are commonly used block ciphers. By design AES is faster in highlight their differences in terms each of 16 rounds. For example, switching bit 30 with 16 is much simpler in hardware than software. DES encrypts data in 64 bit block size and uses effectively a 56 bit key. 56 bit key space amounts to approximately 72 quadrillion possibilities. Even though it seems large but according to today’s computing power it is not sufficient and vulnerable to brute force attack. Therefore, DES could not keep up with advancement in technology and it is no longer appropriate for security. Because DES was widely used at that time, the quick solution was to introduce 3DES which is secure enough for most purposes today.3DES is a construction of applying DES three times in sequence. 3DES with three different keys (K1, K2 and K3) has effective key length is 168 bits (The use of three distinct key is recommended of 3DES.). Another variation is called two-key (K1 and K3 is same) 3DES reduces the effective key size to 112 bits which is less secure.The security of RSA algorithm has so far been validated and checks can be electronically signed with RSA. RSA can be applied to any electronic system that needs to have a cryptosystem implemented.

RC6 is a new block cipher submitted to NIST for consideration as the new AES. The design of RC6 began with a consideration of RC5 as a potential candidate for an AES submission. The philosophy of RC6 is to exploit operations that are efficiently implemented on modern processors. RC6 takes advantage of the fact that 32-bit integer multiplication is now efficiently implemented on most processors.

For most applications, an implementation of RC6 in software is probably the best choice. RC6 could be written with well under 256 bytes of code each for the tasks of key setup, block encryption, and block decryption. Unlike many others, RC6 does not use look-up tables during encryption. Means RC6 code and data can readily fit within today’s on-chip cache memory, and typically do so with room to spare. RC6 is a secure, compact and simple block cipher. It offers good performance, considerable flexibility, allows analysts to quickly refine and improve our estimates of its security.

Comparative analysis of symmetric encryption algorithms:



FACTORS	AES	3DES	DES	RC2	BLOWFISH	RC6
KEY LENGTH	128,192, OR 256 BITS	(K1,K2 AND K3)168 BITS (K1 AND K2 IS SAME) 112 BITS	56 BITS	8–128 bits, in steps of 8 bits; default 64 bits	32–448 bits	128, 192, OR 256 BITS
CIPHER TYPE	SYMMETRIC BLOCK CIPHER	SYMMETRIC BLOCK CIPHER	SYMMETRIC BLOCK CIPHER	symmetric algorithm	symmetric cipher algorithm	symmetric algorithm
BLOCK SIZE	128,192, OR 256 BITS	64 BITS	64 BITS	64 bits	64 bits	128 bits
DEVELOPED	2000	1978	1977	Leaked in 1996, designed in 1987	1993	1998
CRYPTANALYSIS RESISTANCE	STRONG AGAINST DIFFERENTIAL,TRUNCATED DIFFERENTIAL,LINEAR,INTERPOLATION AND SQUARE ATTACKS	VULUNERABLE TO DIFFERENTIAL, BRUTE FORCE ATTACKER COULD BE ABALYZE PLAINT TEXT USING DIFFERENTIAL CRYPTANALYSIS.	VULNERABLE TO DIFFERENTIAL AND LINEAR CRYPTANALYSIS; WEAK SUBSTITUTION TABLES	VULUNERABLE TO DIFFERENTIAL, BRUTE FORCE ATTACKER	VULUNERABLE TO DIFFERENTIAL, BRUTE FORCE ATTACKER	VULUNERABLE TO DIFFERENTIAL, BRUTE FORCE ATTACKER
SECURITY	CONSIDERED SECURE	ONE ONLY WEAK WHICH IS EXIT IN DES.	PROVEN INADEQUATE	vulnerable	vulnerable	vulnerable
POSSIBLE KEYS	2^{128},2^{192},OR 2^{256}	2^{112} OR 2^{168}	2^{56}	2^{64},2^{128}	2^{32},2^{448}	2^{128},2^{192},OR 2^{256}
POSSIBLE ASCII PRINTABLE CHARACTER KEYS	95^{16},95^{24}, OR 95^{32}	95^{14} OR 95^{21}	95^{7}	95^{8},95^{16}	95^{4},95^{56}	95^{16},95^{24}, OR 95^{32}
TIME REQUIRED TO CHECK ALL POSSIBLE KEYS AT 50 BILLION KEYS PER SECOND**	FOR A 128-BIT KEY: 5 x 10^{21} YEARS	FOR A 112-BIT KEY:800 DAYS	FOR A 56-BIT KEY"400 DAYS	FOR A 64 – BIT KEY : 11 YEARS	FOR A 448 BIT KEY: 10^{116} YEARS	FOR A 192 BIT KEY:10^{40} YEARS
ROUNDS	10(128- bits),12(192-bits),14(256-bits)	48	16	16 of type MIXING, 2 of type MASHING	16	20

V. CONCLUSION

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. Several points can be concluded from the comparative results. First; there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. Secondly; in the case of changing packet size, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Third; in the case of changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. Also, we find that 3DES still has low performance compared to algorithm DES. Finally –in the case of changing key size – it can be seen that higher key size leads to clear change in the battery and time consumption.

Unlike many others, RC6 does not use look-up tables during encryption. For most applications, an implementation of RC6 in software is probably the best choice. Means RC6 code and data can readily fit within today's on-chip cache memory, and typically do so with room to spare. RC6 is a secure, compact and simple block cipher.

REFERENCES

[1] K. Fawaz, H.Artail, "DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks ," IEEE Transactions on Mobile Computing, vol 12, no.4, April 2013

[2] M. Abolhasan, T. Wysocki and E. Dutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks, Vol. 2, pp.1-22, 2004.

[3] W. Li, E.Chan,Y. Wang,D. Chen ,"Cache Invalidation Strategies for Mobile Ad Hoc Networks",IEEE International Conference on Parallel Processing, 2007

[4] W. Zhang, G.Cao , "Defend Against Cache Consistency Attacks in Wireless Ad Hoc Networks", IEEE International Conference on Mobile and Ubiquitous Systems: Networking and Services , 2005

[5] S. Abdul. Elminaam, H. M. Abdul Kader, M.M.Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms" **,**Proceedings from International Business Information Management Association (IBIMA) 2009

[6] Q. Hu and D. Lee, "Cache Algorithms Based on Adaptive Invalidation Reports for Mobile Environments," Cluster Computing, vol. 1, pp. 39-50, 1998.

[7] Z. Wang, S. Das, H. Che, and M. Kumar, "A Scalable Asynchronous Cache Consistency Scheme (SACCS) for Mobile Environments," IEEE Trans. Parallel and Distributed Systems, vol. 15, no. 11, pp. 983-995, Nov. 2004.

[8] A.Elmagarmid, J.Jing, A. Helal, and C. Lee, "Scalable Cache Invalidation Algorithms for Mobile Data Access" IEEE Transactions On Knowledge And Data Engineering, Vol. 15, No. 6, Nov/Dec 2003

[9] N. Sabiyath Fatima ,Dr. P. Sheik Abdul Khader , " Enhanced Adaptive Data Cache Invalidation Approach For Mobile Ad Hoc Network" , IEEE 2012, pg 76-80

[10] N. Sabiyath Fatima,Dr. P. Sheik Abdul Khader, " A Hybrid Cache Invalidation Technique for Data Consistency in MANET" , International Journal of Computer Applications, Vol 16– No.5, February 2011

[11] Ali I. El-Desouky Hesham A. Ali,Engy A. El-Shafaiy, "A Wireless Cache Adaptive Invalidation Algorithm In connection and reconnection periods" ,©2006 IEEE

[12] P. Papadimitratos, Z. Haas. "Secure data transmission in mobile ad hoc networks",ACM workshop on wireless security, pp. 41–50, New York, 2003.

[13] A.H. Ragab, N.A. Ismail, " Enhancement and Implementation of RC6 Block Cipher for Data Security" IEEE International Conference , 2001, pp- 133-137.