Journal of Computer Science

Original Research Paper

CCMP Advanced Encryption Standard Cipher For Wireless Local Area Network (IEEE 802.11i): A Comparison with DES and RSA

[1]Velayutham, R. and [2]D. Manimegalai

[1]*Einstein College of Engineering, Tirunelveli, Tamilnadu, India*
[2]*Department of IT, National Engineering College, Kovilpatti, Tamilnadu, India*

Article history
Received: 10-06-2011
Revised: 19-02-2014
Accepted: 26-08-2014

Corresponding Author:
Velayutham, R.
Einstein College of Engineering, Tirunelveli, Tamilnadu, India
Email: murugan.vetech@gmail.com

Abstract: The comparative analysis of the renowned cryptographic algorithms AES, DES and RSA. The Rijndael algorithm was adapted as Advanced Encryption Standard (AES) algorithm, to Data Encryption algorithm (DES), which have been in the security standards since long time. The comparative analysis is implemented in IEEE 802.11i wireless platform. Compared to DES, AES contains CCMP which is a security standard that provides the highest level of security to encrypt and authenticate the data simultaneously. CCMP protocol is to provide robust security. The CCMP protocol is based on Advanced Encryption Standard (AES) encryption algorithm. It uses the Counter Mode with CBC-MAC (CCM) mode of operation. The CCM mode combines Counter (CTR) mode for privacy and Cipher Block Chaining Message Authentication Code (CBC-MAC) for authentication. The implementation is done on the NS-2 platform to compare and analyzes the performance of this with DES and RSA algorithms, based on the following three criteria: (a) Bit rate; (b) Packet delay; and (c) The number of packets. Thus the motivation is to provide a secure data transfer in the wireless medium in IEEE 802.11i.

Keywords: AES-CCMP, DES, RSA, IEEE 802.11i

Introduction

Various cryptographic algorithms have been put forth to provide security for the sensitive information across internet. RSA is an algorithm for public-key cryptography. It is vulnerable to the chosen plaintext attacks. The DES algorithm was used to protect sensitive information, but DES is vulnerable to brute force attack because of its relatively short key length. As the key length is only 56 bits there are only 2^{56} possible keys. Earlier AES was proposed as a substitute for DES. AES is symmetric block cipher. It accepts 128 bits size block and the key size can be 128, 192 and 256 bits. The operations are performed in a certain number of rounds, which varies between 10, 12 and 14 depending on the size of key length. For both its cipher and Inverse cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations.

Mobility support is a salient feature of wireless networks that grant the users anytime anywhere network access. Despite their promising feature, security has become one major concern in wireless networks. Wireless Local Area Networks (WLANs) are groups of wireless networking nodes within a limited geographic area, such as an office building or campus that are capable of having radio communication. WLANs are usually implemented as extensions to the existing wired Local Area Networks (LAN) to provide enhanced user mobility and network access.

As Wireless Local Area Networks become more widely deployed, wireless security has become a serious concern for an increasing number of organizations. CCMP is based on the Advanced

Science Publications

Encryption Standard (AES), a Federal Information Processing Standard (FIPS-197) certified algorithm approved by National Institute of Standards and Technology (NIST). AES (128 bits key length) operates in a Counter Mode (AES-128-CM) within 802.11i with CBC-MAC (CCM). It has been created to replace two predecessors: TKIP and WEP. The implementation of AES-CCMP protocol and it is analyzed with the DES and RSA algorithm. The comparative analysis took part in the Wireless medium (Daemen and Rijmen, 1998; Doomun and Soyjaudah, 2008; Islam *et al*., 2008; NIST, 1993; Samiah *et al*., 2007; Sanchez-Avila and Sanchez-Reillo, 2001; Schneier and Whiting, 2000; Sivakumar and Velmurugan, 2007; Smyth *et al*., 2006; Stallings, 2013).

IEEE 802.11i is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. IEEE 802.11i addresses the security flaws in the original IEEE 802.11 standard with built-in features providing robust wireless communications security, including support for FIPS validated cryptographic algorithms. The 802.11i specification defines two classes of security algorithms: Robust Security Network Association (RSNA) and Pre-RSNA. Pre-RSNA security consists of Wired Equivalent Privacy (WEP) and 802.11 entity authentication.

Advanced Encryption Standards

AES is symmetric block cipher encryption converts data to an unintelligible form called cipher text; decrypting the cipher text which converts the data back into its original form, called plain text. Important characteristics of this algorithm include security, performance, efficiency, ease of implementation and flexibility. The AES block diagram is shown in the Fig. 1.

The AES algorithm has four basic transformations.

Sub Byte Transformation

A nonlinear transformation is applied to the elements of the matrix. This first step in each round is a simple substitution that operates independently on each byte of state using S-box.

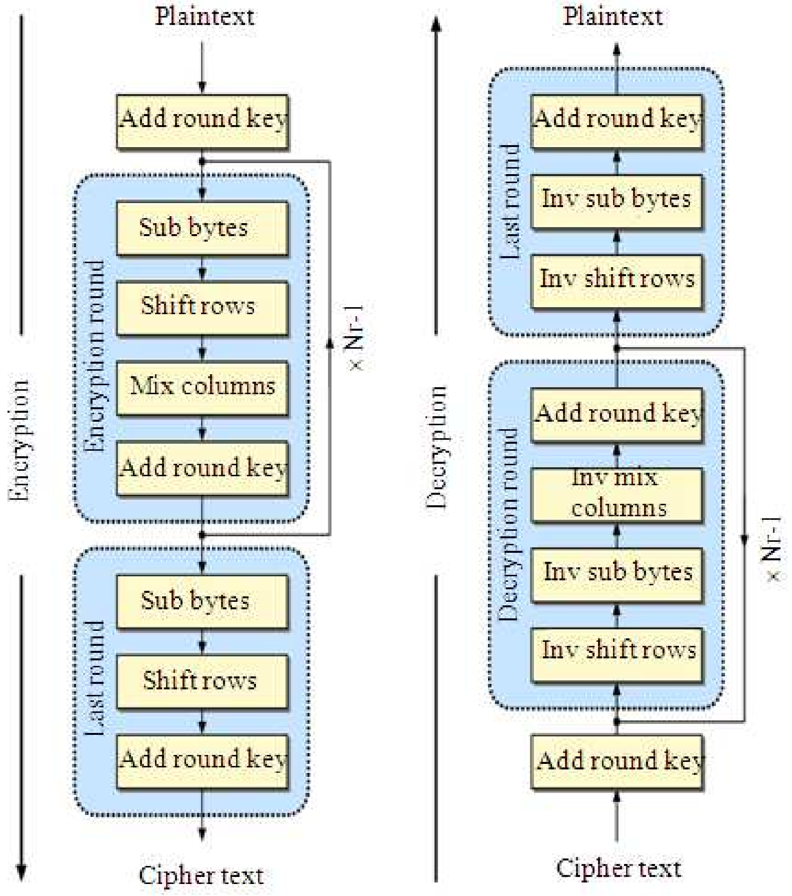

Fig. 1. AES block diagram

Shift Rows Transformation

In the Shift Rows transformation, the bytes in the last three rows of the state are cyclically shifted over different numbers of bytes.

Mix Column Transformation

Mix Columns is a 32-bit operation that transforms four bytes of each column in the state. The Mix Columns transformation operates on the state column-by-column, treating each column as a four-term polynomial.

Add Round Key Transformation

During each round of an AES process, a separate 128-bit round key is used. This performs XOR operation on the round key, which is obtained from the initial key by a key expansion procedure.

CCM Protocol

Network connectivity is becoming an increasingly integral part of computing environments. Wireless Networks offers users anytime network access. WEP the first security protocol was introduced based on RC4. Due to some security issues it was replaced with TKIP. TKIP was based on same security algorithm i.e., RC4. It was better than Wired Equivalent Privacy (WEP) but still same security challenges were faced again. To overcome these security issues CCMP was adopted.

Counter Mode

Counter mode operates by encrypting the initial counter and the resulting output is XORed with the plaintext to produce the cipher text. The initial counter is constructed from the flags field, length of the payload and the nonce. The nonce is constructed from the Packet Number (PN), MAC layer A2 Address field (A2) and MAC layer priority field.

CBC-MAC Mode

In Cipher-Block Chaining Message Authentication Code (CBC-MAC) mode, each block of plaintext is XORed with the previous cipher text block before being encrypted.

Implementation of the CCMP block can be viewed as a single process with inputs and outputs. The decryption phase has the same inputs as the encryption phase (except that the input MPDU is encrypted). This is because the header information, including the CCMP header, is transmitted across the link in the clear and can therefore be extracted by the receiver prior to decryption.

The computation occurs in two stages: First, the MIC is calculated and appended to the MPDU (MAC Protocol Data Unit) and then the entire MPDU (including MIC) is encrypted as shown in the Fig. 2.

The implementation of CCMP (as a “block”) use a sequence counter called the Packet Number (PN), which it increments for each packet processed. This prevents an attacker trying to reuse a packet that has previously been sent. The PN is 48 bits long; large enough to ensure it never overflows.

The first important point is that CCMP encrypts data at the MPDU level. There is one MPDU for each frame transmitted and the MPDU itself might be the result of fragmenting larger packets passed from a higher layer. An overview of the steps in encrypting an MPDU is described below:

- It start with an unencrypted MPDU, completely with IEEE 802.11 MAC header. The header includes the source and destination address, but the values of some fields will not be known until later and are set to 0 for now
- The MAC header is separated from the MPDU and put aside. Information from the header is extracted and used while creating the 8-byte Message Integrity Code (MIC) value. At this stage the 8-byte CCMP header is constructed for later inclusion into the MPDU
- The MIC value is now computed so as to protect the CCMP header, the data and parts of the IEEE 802.11 header. Liveness is ensured by the inclusion of a nonce value. The MIC is appended to the data
- The combination of data and MIC is encrypted. After encryption the CCMP header is prepended

Finally the MAC header is restored onto the front of the new MPDU and the MPDU is ready to the queue for transmission. The transmission logic needs to have no knowledge of the CCMP header. From here until transmission, only the MAC header will be updated.

The CCMP header must be prepended to the encrypted data and transmitted in the clear (that is unencrypted). The CCMP header has two purposes. First, it provides the 48-bit Packet Number (PN) that provides replay protection and enables the receiver to derive the value of the nonce that is used in the encryption. Second, in the case of multicasts, it tells the receiver in which group key has been used. The format is shown in the Fig. 3. In CCMP the first block of the CBC-MAC computation is not taken directly from the MPDU but is formed in a special way using a nonce value. The nonce guarantees freshness by ensuring that each encryption uses data that has never been used before (under a given key).

However, one should remember that the key is shared between at least two communicating parties (more for the group key) and these parties may, each at some point, use a PN that has already been used by another party, violating the "use once per key" rule. To avoid this problem, the nonce is formed by combining the PN with the MAC address of the sender. The CCMP process gives protection against forgery, eavesdropping and copy/replay attacks. This study is implemented in NS2 and the performance is compared with DES and RSA. The methodology of the proposed is as follows (Fig. 4).

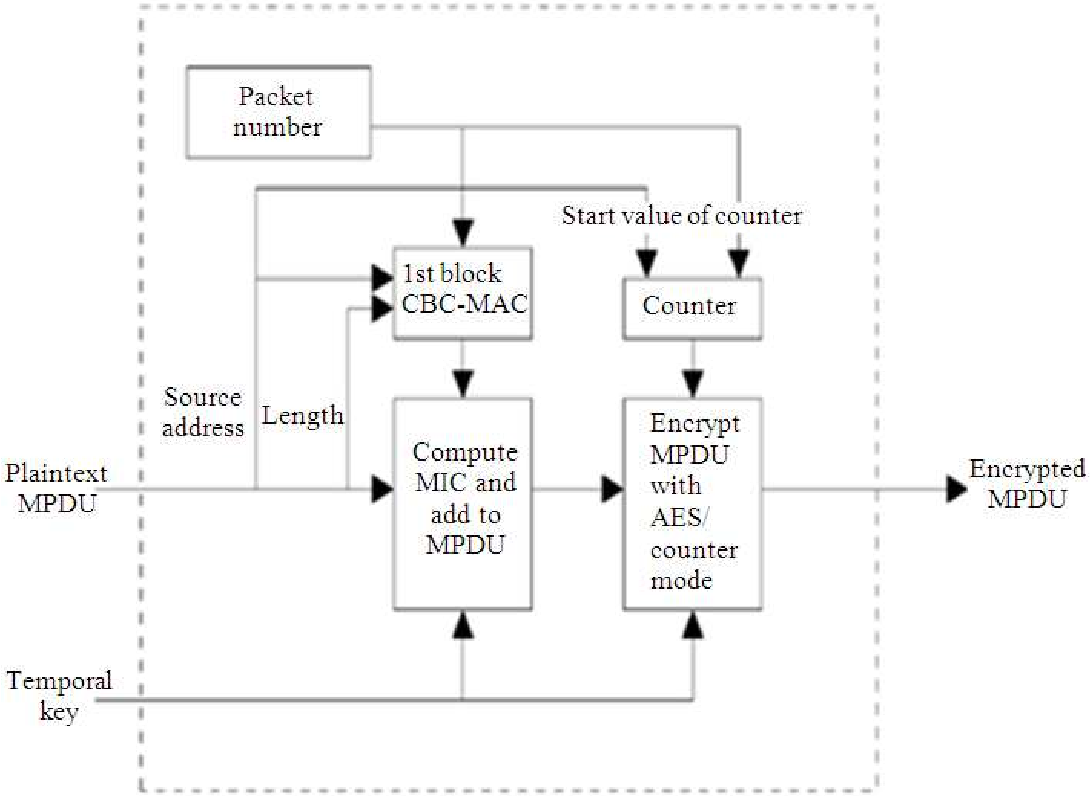

Fig. 2. CCMP encryption block

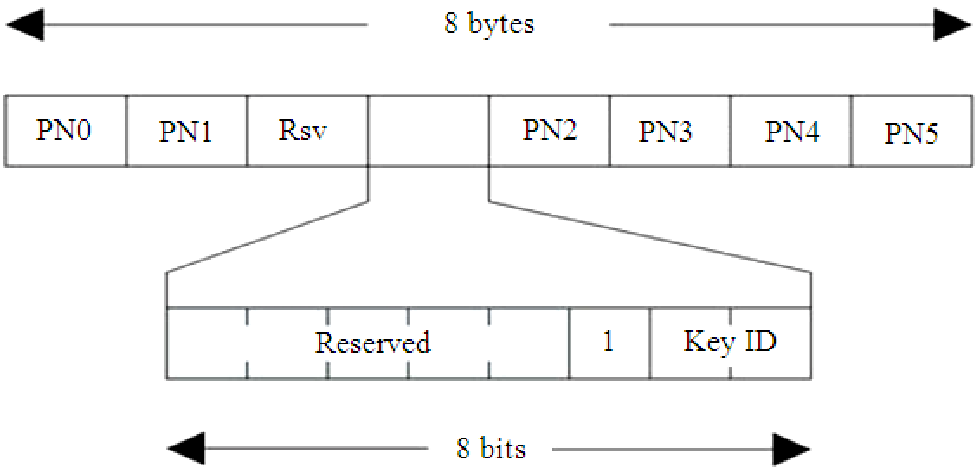

Fig. 3. CCMP header

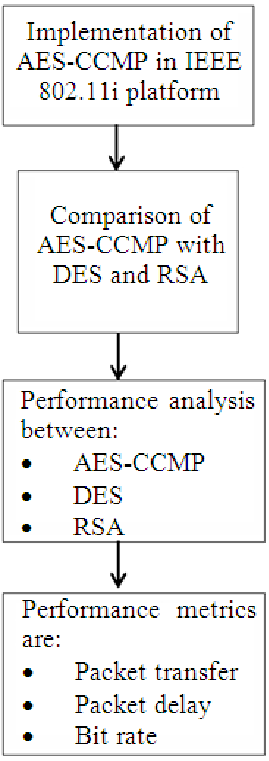
Implementation of AES-CCMP in IEEE 802.11i platform
Comparison of AES-CCMP with DES and RSA
Performance analysis between:
• AES-CCMP
• DES
• RSA
Performance metrics are:
• Packet transfer
• Packet delay
• Bit rate

Fig. 4. Methodology

Results

In this study, there are three primary performance measures are taken using the route-driven methods (Table 1-3).

Encryption methods have been established in two separate levels, one for the data transmission from sensor nodes to the cluster head and another from cluster heads to base station. By this encryption levels, the malicious data from sensor nodes and data congestion to base station is reduced, further additional encryption is provided from cluster head to base station in the similar manner.

For the sensor nodes and cluster head encryption, key generation parameters are distributed dynamically within the cluster itself rather than getting common key from the base station. This reduces the unnecessary overhead of the base station.

The values obtained during the execution of the simulation environment are tabulated and the graphical analysis is shown. The sample values obtained for the bit rate, packet delay and Packet transfer rate between these algorithms are as follows.

Based on the obtained values AES algorithm combined with the CCM Protocol shows a clear advantage over the DES and RSA algorithms.

Table 1. Bit rate analysis values

Time (sec)	RSA	DES	AES with CCMP
0.08512	2.85	3.35	3.75
0.12768	2.90	3.40	3.80
0.17024	2.95	3.45	3.85
0.2128	3.00	3.50	3.90
0.29792	6.85	7.35	7.95
0.34048	6.90	7.40	8.00
0.38304	6.95	7.45	8.05
0.4256	7.00	7.50	8.10
0.51072	10.85	11.35	11.95

Table 2. Packet delay analysis values

Time (sec)	RSA	DES	AES with CCMP
0.592778	5.50	4.50	3.00
0.696389	10.50	7.50	7.00
0.730926	14.50	11.50	11.00
0.743001	18.85	17.35	14.85
0.744776	18.90	17.40	14.90
0.745417	18.95	17.45	14.95
0.748195	19.00	17.50	15.00
0.758558	23.80	22.30	19.80
0.765465	26.50	25.00	23.00

Table 3. Packet transfer rate analysis values

Time (sec)	RSA	DES	AES with CCMP
2	2.85	3.85	4.35
5	3.00	4.00	4.50
10	7.00	8.20	13.20
15	11.00	13.00	18.00
20	15.00	17.20	18.70
25	19.00	20.00	21.50
30	23.00	24.00	25.00

The first graphical representation analyzed between the time and the number of bits transferred at a particular time period in second's similarly number of packets delayed at the certain interval of time also the number of packets transferred analyzed between the times in seconds. These values are obtained through the NS2 simulation environment.

Discussion

The result analysis of the most existing system are based on the data transfer rate, in this proposed scheme the analysis take part for the Bit rate transfer and the Packet delay. Based on the results, the discussions are as follows.

The bit rate performance in the Fig. 5 shows that in the case of RSA, DES and AES with CCMP algorithms are compared. The performance results show that the AES with CCMP shows better results than the other two algorithms. With the security implementations, all the data are being encrypted both in cluster head and base station that is represented in the graphical analysis.

The performance results in the Fig. 6 shows that the AES with CCMP shows reduced delay results than the other two algorithms. The data transmission between adjacent packets is considered as delay based on the encryption standards.

The performance results in the Fig. 7 show that the AES with CCMP shows good packet reception than the other two algorithms.

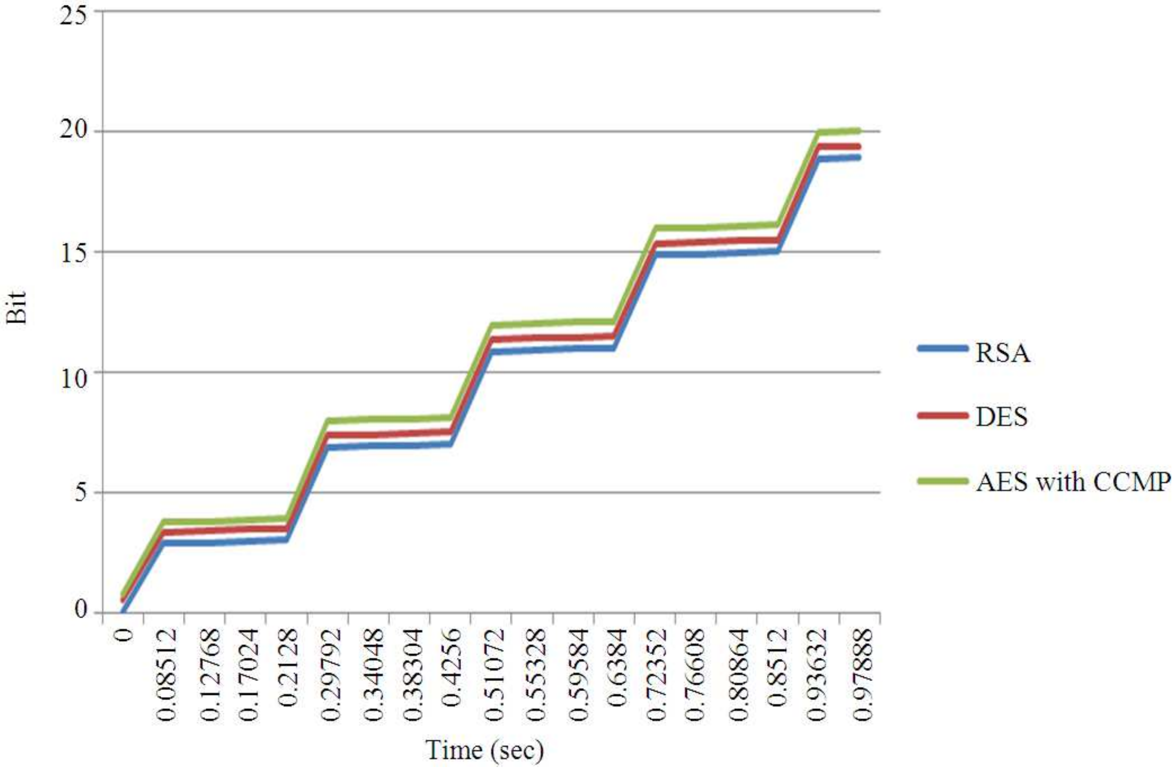

Fig. 5. Dynamic key management-bit rate

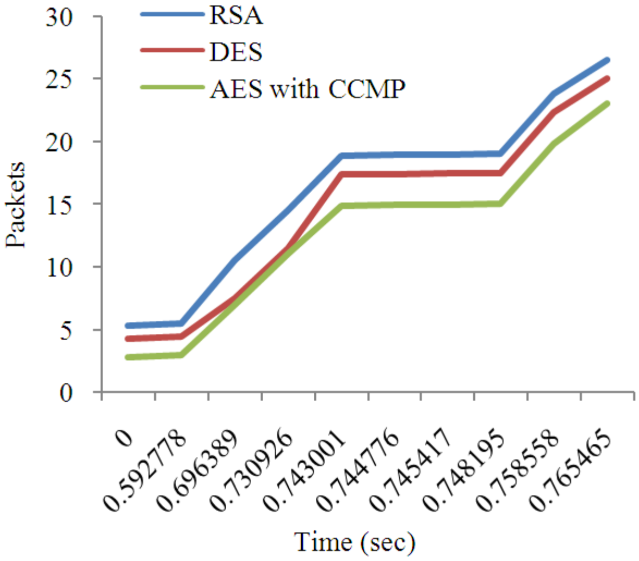

Fig. 6. Dynamic key management-packet delay

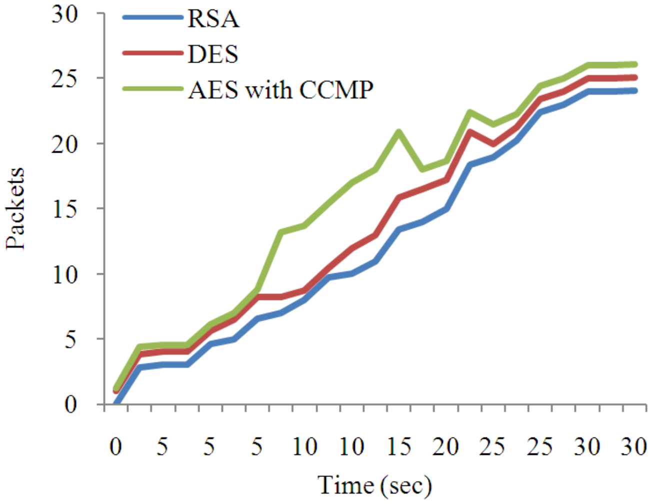

Fig. 7. Dynamic key management-no of packets

Conclusion

In this study, we have implemented AES with CCMP in IEEE 802.11i and compared the performance of this with the other two algorithms namely DES and RSA. The proposed work also presented a dynamic key management strategy for cluster-based Heterogeneous Sensor Networks (HSN) to maintain required security and service quality levels consisting of three attributes, which are bit rate, packet delay and number of packets. The implementation is done in the NS-2 and through simulations; we have compared the performances of RSA, DES and AES with CCMP algorithms. The results show that AES with CCMP shows better performance with respect to the Quality Of Service (QOS)-bit rate, packet delay and number of packets. This computation has done by using the randomized file selection for dynamic key management level both in cluster head and base station. As a further process, we plan to extend the proposed strategy to control security and service quality for multiple clusters of various wireless networks such as WLAN and MANET in addition to the heterogeneous sensor networks.

Funding Information

The authors have no support or funding to report.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Daemen, J. and V. Rijmen, 1998. AES Proposal: Rijndael. 1st Edn., Springer-Verlag, Berlin Heidelberg.

Doomun, M.R. and K.M.S. Soyjaudah, 2008. Resource saving AES-CCMP design with hybrid counter mode block chaining-MAC. Int. J. Comput. Sci. Netw. Security, 8: 1-13.

Islam, M.N., M. Mia, M. Chowdhury and M.A. Matin, 2008. Effect of security increment to symmetric data encryption through AES methodology. Proceedings of the 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Aug. 6-8, IEEE Xplore Press, Phuket, 291-294. DOI: 10.1109/SNPD.2008.101

NIST, 1993. Data encryption standard, FIPS. National Institute of Standards and Technology.

Samiah, A., A. Aziz and N. Ikram, 2007. An efficient software implementation of AES-CCM for IEEE 802.11i wireless st. Proceedings of the 31st Annual International Computer Software and Applications Conference, Jul. 24-27, IEEE Xplore Press, Beijing, pp: 689-694. DOI: 10.1109/COMPSAC.2007.62

Sanchez-Avila, C. and R. Sanchez-Reillo, 2001. The rijndael block cipher (AES Proposal): A comparison with DES. Proceedings of the 35th International Carnahan Conference on Security Technology, Oct. 16-19, IEEE Xplore Press, London, pp: 229-234. DOI: 10.1109/.2001.962837

Schneier and D. Whiting, 2000. A performance comparison of the five AES finalist. Proceedings of the 3rd AES Candidate Conference, Mar. 15-15.

Sivakumar, C. and A. Velmurugan, 2007. High speed VLSI design CCMP AES cipher for WLAN (IEEE 802.11i). Proceedings of the International Conference on Signal Processing, Communications and Networking, Feb. 22-24, IEEE Xplore Press, Chennai, pp: 398-403. DOI: 10.1109/ICSCN.2007.350770

Smyth, N., M. McLoone and J.V. McCanny, 2006. WLAN security processor. IEEE Trans. Circuits Syst. I: Regular Papers, 53: 1506-1520. DOI: 10.1109/TCSI.2006.877888

Stallings, W., 2013. Cryptography and Network Security: Principles and Practice. 6th Edn., Pearson Education, Limited, London, ISBN-10: 0133354695, pp: 731.