ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Energy Efficient Encryption scheme for Mobile Ad-Hoc network

Pooja Mundhe, Vitthal Gutte, Pramod Mundhe

Asst. Professor, Dept. of IT, MIT College of Engineering, Kothrud, Pune, India

Asst. Professor, Dept. of IT, MIT College of Engineering, Kothrud, Pune, India

Asst. Professor, Dept. of IT, MIT College of Engineering, Kothrud, Pune, India

ABSTRACT: A mobile ad-hoc network is a part of wireless ad-hoc network or ad-hoc network. It is self-configured, distributed network of mobile devices connected with each other without any infrastructure. Mobile nodes in this network communicate with each other without any centralized authority. In MANET, nodes are battery constraints i.e. energy consumption is a major issue due to lack of battery power. Researchers have shown that different network coding techniques can reduce energy consumption by decreasing number of transmission. Data transmission or routing is not the only source of energy consumption, energy can also be consumed during encryption and decryption process. This paper provides a comparative study of different energy efficient encryption technique to reduce energy consumption while encoding/decoding the packet in ad-hoc network.

KEYWORDS: Mobile ad-hoc network, Energy efficient encryption, network coding, LEE, feistel cipher.

I. INTRODUCTION

Mobile Ad Hoc Networks are important multi hop wireless communication standard. These multi hop wireless network accommodatingly uphold connectivity of network. Ad hoc network are convenient to use where temporary networks are needed without any infrastructure. Building a mobile ad hoc network poses technical challenges. In such networks, node may have limited energy supply [1]. In these networks, improving the energy efficiency and decreasing the energy consumption is still an important issue. Thus, the device should be light-weight. However, due to unstable network topology and inconsistent network links in MANET energy consumption and secure communication received much attention from industrial and researchers circle.

Although network coding play important role in reducing the energy consumption in MANET, Security is still a challenge [2]. Network coding refers to the coding or mixing of data at a node, which maps data from input to output. When network coding is applied every node in the network can encode the data and forward it to the destination node. Furthermore, since the devices or node in the network are battery operated, they need to be energy preserving to maximize the battery life [3]. There is substantial energy consumption while a node communicate with the other node in the network.

As the network traffic can be quickly increase, energy efficiency is becoming an important metric. With the help of network coding network throughput could be maximized and energy consumption should be minimized to improve energy efficiency in the wireless network. There are two types of network coding Fountain coding (FC) and random linear network coding (RLNC) [4].

This coding techniquesprovides an effective method for the file transfer. When network coding is applied at the source on the file both the relay nodes can be engaged simultaneously for the file transfer which completely avoids the problem of identical packets and also achieve higher throughput. This paper focus on reducing energy consumption while providing secure communication.

DOI: 10.15680/IJIRCCE.2017. 0504295

II. Related work

In [5], Author proposes a security scheme against eavesdropping attack called P-coding. This achieves computational security against global eavesdropper for NC-based applications. P-coding provides some significant features like security, efficiency, transparency, scalability and robustness. Here author addresses the problem, where intruder aims at interrupting packets and decoding them to gather meaningful information. The proposed system in this paper presents the concept of permutation encryption.

In [6], the proposed work focus on reducing power usage during transmission of data in wireless sensor network. Here author investigate different data aggregation techniques for minimizing power consumption. Initially, dynamic node formation is performed, followed by multilevel clustering to form cluster heads for data aggregation. LEACH Protocol is implemented with updating at TDMA. Finally, author compare the working of normal LEACH with Proposed LEACH protocol for better result.

Multi-hop multi-cast routing offers improved communication performance in multi-hop wireless network. In [7], author studies energy efficient multi-cast communication at multi-hop wireless network. Here author has derived an algorithm to named network coding based multicast to address the problem. In this paper, a multi-hop wireless network is considered without center, i.e. without support of fixed basic devices. Where all the nodes in the network are relay nodes that can send and receive data packets independently. Here author discusses how the optimal multicast tree is built in multi-hop network for multicast communication where minimum energy is consumed.

In [8], author addresses the problem of energy consumption in Mobile ad hoc network while the nodes are idle. According to the author, when nodes are in the idle state, consumes large portion of overall energy consumption. Therefore it is important to work on reducing idle energy consumption. Here author compares the energy consumption by different routing protocol in different states of node like sending, idle, sleep and receiving.

In [9] paper, author considered the problem of unreliable communication in multi-hop wireless network due to unstable wireless medium. The proposed technique, erasure coding is compared with the other techniques such as, retransmission and backup paths. Erasure coding is a coding technique, which converts a message into large set of coded blocks such that any adequately large subset of coded blocks can rebuild the original message.

III. LIGHT-WEIGHT ENERGY EFFICIENT ENCRYPTION

The light weight energy efficient encryption (LEE) uses the concept of feistel cipher which is a symmetric encryption algorithm used for the creation of block cipher. In feistel cipher the encryption and decryption operation are very similar to each other with the difference of reverse key scheduling. The proposed methodology discusses the encryption technique which provides security to the nodes in the network in energy efficient way. This technique can be used with the devices which are battery powered. LEE does not contain any complex operations or operations like s-boxes.

Following figure 1 depict the structure of feistel cipher. Since the operation of feistel cipher such as encryption and decryption are similar which requires only reversal of key schedule the size of the circuitry or code is almost halved. This structure is iterative in nature thus makes easier implementing the cryptosystem in hardware. Feistel cipher are stream cipher which syndicate numerous rounds of repetitive operations such as, bit shifting (P-boxes), Simple non-linear functions (s-boxes) and linear mixing to produce a large amount of confusion and diffusion.

Feistel structure contains numerous rounds of processing of the plaintext, each round consists of substitution followed by permutation step [10]. The plaintext given as input is divided into two halves i.e. L (left) and R (right). In each round, the left have is encrypted with key along with the right half. In every subsequent round, input block is split into two parts (Left) L and (right) R. The left part goes through the procedure that depends on R and the encryption key. First the encryption function is applied on the key and the right part which produces the f(K, R). Then this output of this function is XORed with the left part i.e. L. Here unlike DES each round derive a new key for each subsequent round, although all the sub keys are related to the original key.

The permutation operation at the each round swaps both parts of the input. The modified L is swiped with the unmodified R. therefore, in next round R will be the L of the current round. Finally, when the last round is completed then the two sub parts are combined in order to form the cipher text.

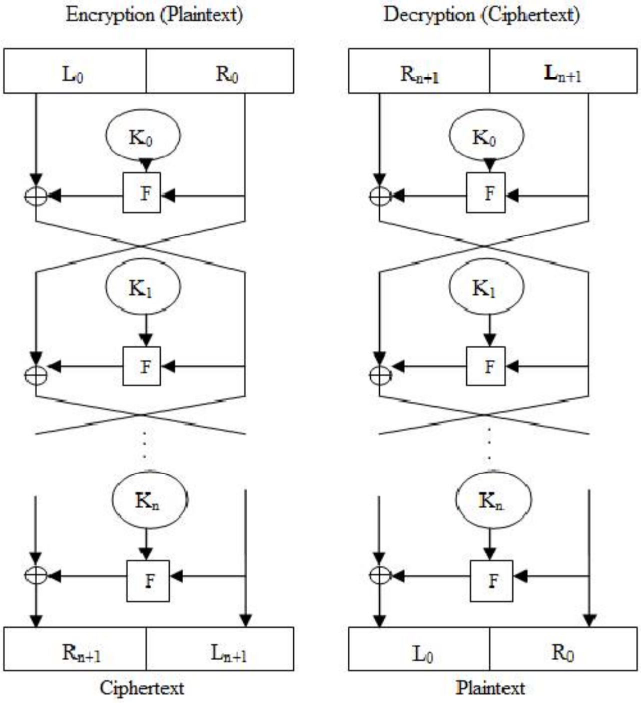

Figure 1: Feistel Cipher [1].

The decryption process of the feistel cipher is very much similar to the encryption process. The input for the decryption is the block of cipher text. Then this cipher text block is divided in half again same as plaintext in encryption process. In case of decryption the key used for the process is revere key of the key used for encryption. The final swapping of the two parts of encryption process is important to get the cipher text otherwise cipher text cannot be decrypted successfully [11].

IV. PROPOSED WORK

With the help of light weight energy efficient encryption scheme it is impossible to the intruder to recover the original message. The light weight energy efficient encryption scheme used here requires less time to process the encryption and decryption on the message. The time required for the processing is reduced thus reduces the energy consumption of the node. The architecture for the proposed system based on the following parts:

The introduced algorithm is motivated based on the XTEA algorithm [12], LEE is a 64-bit block cipher which uses 128 bit length of key and 32 rounds. Feistel cipher structure is used for building of block cipher. The advantage of using feistel cipher is that the encryption and decryption operations are similar, which only requires the reversal of the key schedule for the encryption and decryption. Therefore, the code required for the implementation of the algorithm is nearly halved, which in turns reduce the time consumed for the operation and the energy consumption. At the source node the feistel cipher structure encrypts the plaintext before transmitting the packet towards destination node. LEE includes some steps like fixed length rotation, shift operation, XOR and addition modulo 2^{32}.

DOI: 10.15680/IJIRCCE.2017. 0504295

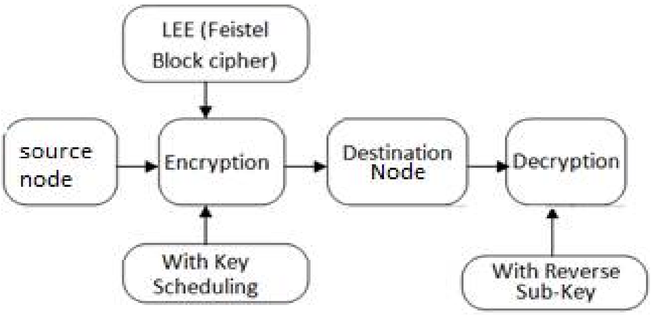

Figure 2: Architecture of Proposed System

Let the source node wants to send a message to destination node. At the source, the message is divided into two half for the process of encryption and decryption. These both the parts of plaintext after 32 rounds of processing combined to produce a cipher text block. Therefore, the original input given to the algorithm is P = L_0R_0 and the final cipher text is C= $L_{32}R_{32.}$

At the source node message is encrypted with the help of light weight energy efficient encryption. In LEE, the original message is split in two parts. The right half is used along with the key to encrypt the left half. After combining these both the parts cipher text is produced.

On receiving the encrypted message from source node, destination node follows the similar process to decrypt the cipher text to get the original message. At the destination node, again the cipher text is divided in two halves and the reversal of the key used for the encryption is used along with the right part to produce the plaintext. Due to these process of using reversal key code needed to implement is reduced. As compare to other algorithms used for the encryption and decryption this requires less time and energy and also provides better security [14].

In MANET, not only transmission of message consumes more energy but also the encryption and decryption operation requires more energy.

- When a source node has a packet to send to destination node the packet is encrypted with the feistel structure.
- Source encrypts the message by diving it and encrypting the message with the other part of message and the key.
- The function is applied on the part of message and the key to produce the sub key which is XORed with the other part.
- The key scheduling algorithm is used to produce the 128 bit key.
- At the receiving node, the cipher text is again divided and same procedure is followed to get the original message.
- At destination node, cipher text is used as the input to algorithm and the key used is in reverse order.

V. SYSTEM MODEL

LEE is 64-bit block Feistel network with 32 rounds and 128- bit key.

Table 1: Notations Used in the Description of Lee [1].

Symbol	*Description*
←	Shift To Left
→	Rotation to Right
⊕	XOR

The Feistel function is based on shift operation and XOR, fixed length rotation and additions modulo 232.

DOI: 10.15680/IJIRCCE.2017. 0504295

- Consider a MANET where S (Source node) wants to send a message to D (destination node).
- When a source wants to send message to destination node, it encrypts the message as follows:
- Size of the message is calculated in bytes for the further computation.
- The given plaintext is divided into the two halves L_0 (left-half) and R_0 (right-half). Therefore input of the algorithm is, P= L_0 and R_0 and the cipher text C=$L_{32}R_{32}$ .The relation between the output L_{i+1},R_{i+1} and input L_i,$R_i$for *i*th round of algorithm is as follows:
- To calculate time required to perform encryption and decryption define following:
- Let X be the start time defined before execution of algorithm.
- Let F be the round function and K_0, K_1 …. $K_n$be the number of keys for round 0, 1…..n Respectively. Following calculation is done for each round:
- $L_{i+1} = R_i R_{i+1} = L_i \oplus F(R_i, K_i)$ Where K=K_0, K_1,….$K_n$keys for n rounds.
- Function F operates in following way:
- $R_i' = (R_i \leftarrow 4) \oplus (R_i \rightarrow 5)$
  R_i'can be calculated with performing XOR operation on Bitwise rotation to right of $R_i$and Bitwise shift to left of R_i.
- Then Round function can be calculated as follows:
  $F(R_i,K_i) = (R_i' + K_i)$ Here, calculated R_i'and key K_i are added to get the round function.
- Decryption of the cipher text can be produced in the following way:
  $R_i = L_{i+1}$ $L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$ Where, i = n, n-1 …0
- Finally, the plaintext (L_0, R_0) can be obtained.
- Let Y be the end time defined after the execution of algorithm.
- Let T_E as total time required to perform encryption operation, From 1 and
  $$T_E = (Y – X) / 1000$$
- Let T_D as total time required to perform decryption operation,
  $$T_D = (Y - X) / 1000$$
- Since execution time is known, energy consumption can be calculated by calculating energy used by CPU.
- Here total Energy Consumption T_E, for Process of encryption and decryption can be calculated as follows,

$$T_E = [(T_E + T_D) * 65.74] / 1000$$

Here it is considered that, CPU requires 65.74 watts of energy for executing the algorithm. So it is divided by 1000 to convert it into the Joules.

VI. EXPERIMENTAL EVALUATION

The performance of the proposed system for the MANET is evaluated with the help of some metrics such as energy consumption, encryption time and decryption time. For implementing the LEE, initially message is divided into two halves. This process is followed by encryption to get the required cipher text. This cipher text is given as input to the decryption process with the reverse key to produce the original message.

VII. CONCLUSION

In this paper, a lightweight energy efficient encryption algorithm is discussed to reduce the energy consumption while providing security to the messages communicated in the network. Thus rather than using traditional encryption algorithm which consumes more energy while providing security, a LEE is used to reduce the energy consumption in MANET. The LEE algorithm requires less time for process of encryption and decryption which in turns reduce the energy consumption. In future work, this algorithm can be extended to provide better security in energy efficient way in multi-hop multicast network.

REFERENCES

[1] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, Vol. 25, No. 9, September 2014.

[2] Siddhartha S. Borkotoky and Michael B. Pursley, "Network-Coded File Distribution in an Ad Hoc Relay Network" IEEE Information Theory and Applications Workshop (ITA), 2016.

[3] Ali Khan, Qifu Tyler Sun, ZahidMahmood, and Ata UllahGhafoor, "Energy Efficient Partial Permutation Encryption on Network Coded MANETs" Hindawi Journal of Electrical and Computer Engineering Volume 2017, Article ID 4657831, 10 pageshttps://doi.org/10.1155/2017/4657831.

[4] Jalaluddin Qureshi, "Random Linear Fountain Code with Improved Decoding Success Probability" Communications (APCC), 2016 22nd Asia-Pacific Conference on Networking and Internet Architecture (cs.NI); Information Theory (cs.IT).

[5] Yanfei Fan, Xuemin (Sherman) Shen, Peng Zhang, Yixin Jiang, Chuang Lin "P-Coding: Secure Network Coding against Eavesdropping Attacks" INFOCOM, Proceedings IEEE 14-19 March 2010.

[6] SnehalLonare, Dr. A. S. Hiwale "A Data Aggregation Protocol to Improve Energy Efficiency in Wireless Sensor Networks" AVCOE, Sangamner iPGCON-2015 SPPU, Pune

[7] Dingde Jiang, ZhengzhengXu, ZhihanLv, "A multicast delivery approach with minimum energy consumption for wireless multi-hop networks" Telecommunication SystemsAugust 2016, Volume 62, Issue 4, pp 771–782.

[8] K. Arulanandam And Dr. B. Parthasarathy, "A New Energy Level Efficiency Issues In Manet" International Journal of Reviews in Computing© 2009 IJRIC. All rights reserved. E-ISSN: 2076-3336

[9] Sethulekshmi C G, Manoj Kumar G, "Energy Efficient Secure Routing in Manets Based on Multipath Erasure Coding" International Journal Of Engineering And Computer Science ISSN: 2319-7242Volume 4 Issue 10 Oct 2015, Page No. 14717-14724.

[10] Komninos, N., Soroush, H. &Salajegheh, M. (2007). "LEE: Light-Weight Energy- Efficient encryption algorithm for sensor networks" Paper presented at the IEEE 9th InternationalSymposium on Communication Theory & Applications (ISCTA'07), 16 - 20 July 2007, Ambleside,UK.

[11] Choy, J., Chew, G., Khoo, K., Yap, H.: Cryptographic Properties and Applications of a Generalized UnbalncedFeistel Network Structure. Cryptography and Communications 3(3), 141–164 (2011) (revised version).

[12] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, Handbook ofApplied Cryptography, CRC Press, Inc., 2001.

[13] N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols, " IEEE Trans. Mobile Computing, vol. 5, no. 2, pp. 128- 143, Feb. 2006.

[14] N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols, " IEEE Trans. Mobile Computing, vol. 5, no. 2, pp. 128- 143, Feb. 2006.