ISSN No. 0976-5697

Volume 5, No. 7, September-October 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Securable and Energy Efficient Transmission in Remote Cooperative Groups: New DES Algorithm

Kalyani.M
M.tech Student, Department of Computer Science and Engineering, Vignan's Lara Institute Of Technology, Guntur, Andhra Pradesh, India

Deepthi.S.
Department of Computer Science and Engineering, Vignan's Lara Institute Of Technology, Guntur, Andhra Pradesh, India

Abstract: In MANET'S broadcasting of data to remote cooperative groups by using of key management paradigm technique cladding problems with the encryption, decryption of data. Key management paradigm creates public key infra structure for key generations, encryption and decryption processes. By using of public key infrastructure (PKI) it will generate the group keys and performs key distributions among the nodes those which are in hybrid network model with that transmission of data will be done in fast manner but it consumes more energy levels, which leads to consumption of more energy levels. By considering this in mind we proposed a new approach which uses a modified Data Encryption Standard algorithm instead of key management. A new DES Algorithm is proposed with 8/32 s-boxes instead of 6/4 s-boxes and uses addition modulo function in addition to the AND, XOR operations in existed in DES algorithm. we identified significant effects in energy levels and those are simulated with help of Network Simulator -2

Keywords: MANET'S, NS2 tool, Cooperative groups, Key management, S-boxes

I. INTRODUCTION

In many newly emerging networks, there is a need to encryption for transmission in broadcasting area's arising in wireless mesh networks (WMNs)[2], mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs).WMNs have been recently suggested as a promising low cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network [3].Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information. In the group communication scenarios, the common problem is to enable a sender to securely transmit messages to a remote cooperative group. A MANET is a system made up of wireless mobile nodes with wireless communication and networking characteristics and they can communicate without fixed infrastructures, which supports multicast in MANETs as given below Figure.1.

1.1 MANETS

Mobile Ad Hoc Networks (MANETs) are self-forming, self-maintained, and self-healing, allowing for extreme network flexibility[14], it is an infrastructure less network and manufactured with the nodes/routers (a node which can act as a node or router), every node has a wireless network interface to communicate with the other nodes. MANETs have been proposed for data exchanging between mobile devices even in infrastructure less network with an effective way. It is important that MANETs should support group-oriented applications, such as audio/video conference and data broadcasting from one-to-many [15].

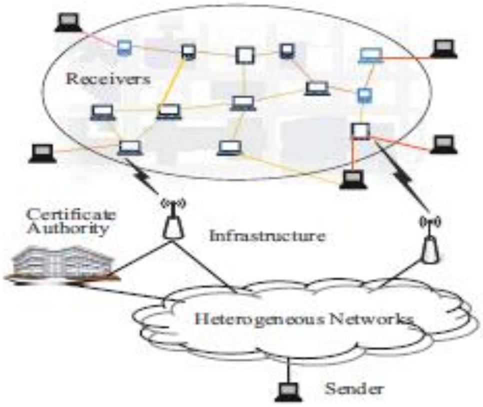

Fig1: System Architecture [1]

A. *Key management in MANET'S*

Key management is the key concept in MANE'T'S. It refers to the management of cryptographic keys in a cryptosystem which includes dealing with the generation, exchange, storage, use, distribution and replacement of keys as shown in Figure 2. The major challenge in MANET is to maintain security in group communication. Many key management schemes were proposed previously which still proves to be insecure.

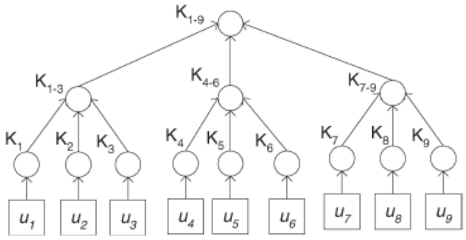

Fig 2: Key exchanging among the cooperative groups

II RELATED WORKS

A. *Key management paradigm*

In group oriented communications accessing of data and for security concerns maintaining of key management system is one way of approach [4]. For those concerns many key management systems have been developed two approaches. Those are Group key agreement and Key distribution system.

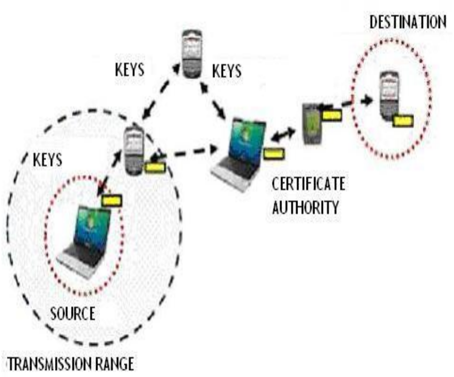

Fig3**:** Key management in MANET'S

But in the existing system includes one aspect in addition to the key management system for sake of secure and fast transmission, that is a core is to establish a one-to-many channel under certain conditions, it maintains a hybrid of group key agreement and public encryption[7]. In that each group member contain public/secret key pair for group key agreement and construct public key infrastructure (PKI)[5],[6] for knowing of public keys of group members a remote sender can securely broadcast a secret session key to any intended subgroup chosen in an *ad hoc* way[10], and, simultaneously, any message can be encrypted to the intended receivers with the session key [8]. Only the selected group members can jointly decrypt the secret session key and hence the encrypted message [9].But this key management system doesn't provide securable transmission of data efficiently because third party is fully trusted for secret key generation and distribution. If the centralized server is hacked then data can be pretended by others easily. Also the key distribution process happens for every time of data transmission and generating of keys for every level of transmission is expensive and confusing process. The system fails to provide security against attacks such as data confidentiality, integrity, and availability cannot be maintained. If the key distribution and key generation is more for every level of transmission then the energy levels may also increases more.

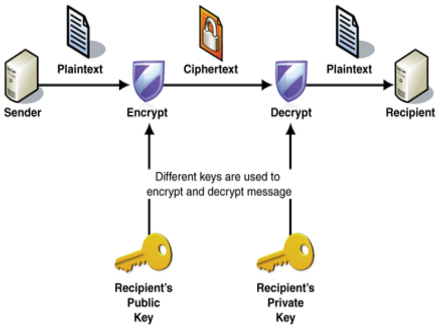

Fig 4: Key Distribution in MANET'S

B. *2.2 New Data Encryption Standard Algorithm with 8/32 s-boxes*

Even though using number of security algorithms which may not provide 100% assurance for security. For those issues a New DES Algorithm develop from the existed DES Algorithm. It uses 8/32 s-boxes for matching of bits and performs addition modulo (+) function on data. Existed DES algorithm uses to expanding data into 48 (8*6) bits and substitute in 6/4 bit s-boxes, this type of substitutions is time taking one and only same data works on long process, it is cost effective one and efficiency of getting data is decreased[13]. To recover this defect proposed DES algorithm uses 8/32bit s-boxes, by this way matching 8 bits instead of 6-bits at each round and perform addition modulo function for preventing carrying bits (when performing XOR if any carry occurs it will be through off) and also give more robustness to DES algorithm and make it stronger against any kind of intruding. This new algorithm gives avalanche effect than the original DES algorithm and also solves cryptanalysis attack

III PROPOSD METHOD

In MANET's transmitting of data in a secure way by using key management system facing problem like trusting third party and it doesn't fallow any standard and secured algorithms for encryption and decryption process ,it consumes more energy levels which leads more cost .by considering these issues we proposed a mechanism which uses of new DES algorithm and functionality is shown in Figure 5.here this architecture which uses a hybrid network model. it consist number of cooperative groups for transmition of data from sender to receiver, sender which adds the auxiliary nodes by knowing the Ip addresses of those nodes then sender will generates a pair of public /secret keys and auxiliary nodes will encrypt and decrypt the data by using new DES Algorithm .subgroups are added to auxiliary nodes where intended destination is connected.

Group key is maintained for every subgroup for identification and for security purposes. Now an auxiliary node which generates public key it is distributed over the subgroup by using key distribution mechanism and intended node which is used for transmission are going to get a shared session key along with public key. Intended node which delivers the data to destination and data is decrypted by destination using private key.

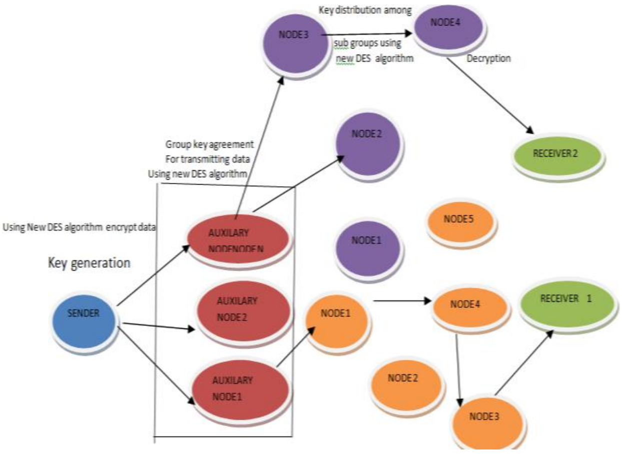

Fig5: Architecture of proposed method

As we mentioned new Data Encryption Algorithm the working functionality is given below. Where sender will send data to auxiliary nodes those will encrypt data as given in figure.6.

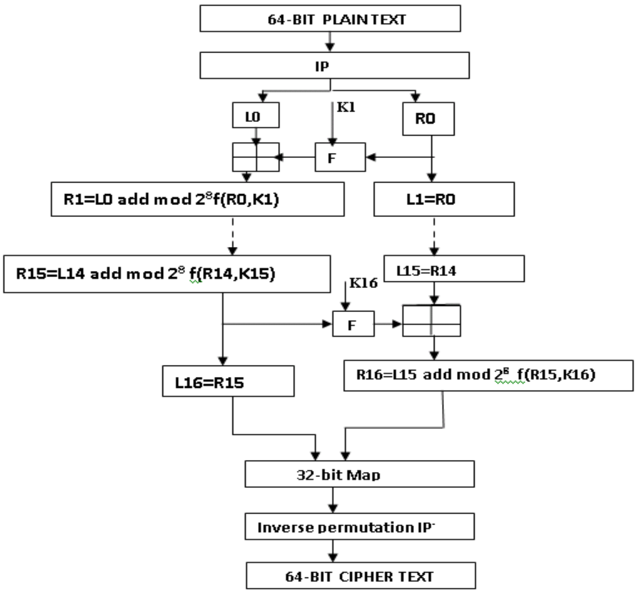

Fig 6: Functionality of New DES Algorithm

here which makes the use of the new operation known as addition modulo (+).it takes two inputs and performs Addition and resulting output assume like x. later perform x mod 2^w Where w is the number of bits that depends on given input.

Example: x and y are the Inputs

X=1100 1000

Y=1000 1111

X'1 is obtained by performing x+y

X1= 1 0101 0111

Carry can be thrown off (or) perform modulo 2^8

X1 is converted to decimal number

X1= 343 mod 2^8 = 87

Binary equivalent of x1 is 0101 0111

To find original x value perform following operation

X=x1+(-y)

To obtain (-y) = 28-y =>256-143=113

Perform X1+ (-y) which results

Original x

0111 0001

0101 0111

1100 1000 original x value

Likewise data will be encrypted. Our main intention is to give better security and reducing energy levels. Security levels are increased due to introducing S-boxes's and addition modulo which is difficult for intruder to encrypt the data. Consumption of energy levels are decreased as compared to key distribution algorithm.

IV SIMULATIONS

Here we used Network simulator -2 for simulating energy levels of key management algorithm and existed Data Encryption Standard and Proposed DES algorithm.

Simulation tool	NS-2
Network area size	100*100
Network size(number of nodes)	100
Speed of nodes	2 meters/sec
Standard	IEEE 802.11g
Data rate	11Mbps
Transmission power	0.005w
Simulation Time	100s
Routing Protocols	AODV
Mobility	Default Random Waypoint
Node Placement	Random

Energy consumption is showed in different ways where Figure 7 shows energy consumption over encryption Figure 8 shows over decryption and figure 9 shows over transmission.

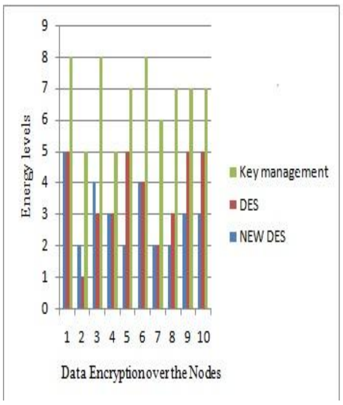

Fig 7: Energy levels consumption

Encryption

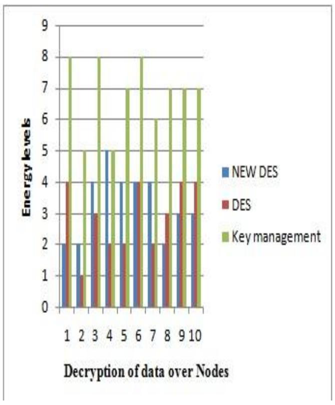

Fig 8: Energy levels consumption over Decryption

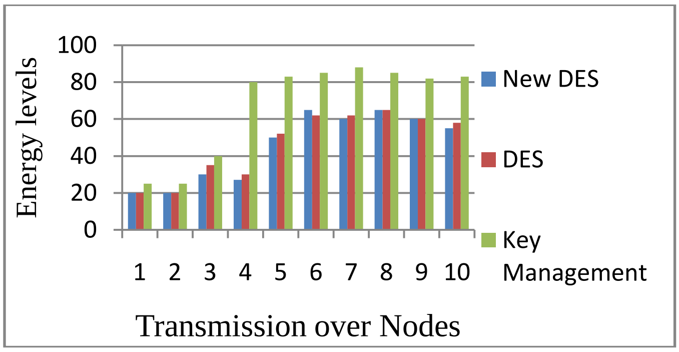

Fig 9: Energy levels consumption over Transmission

V CONCLUSION

In MANETS fast transmission of data to a remote cooperative groups facing problem with security and energy level consumption to overcome these problems we used a new Data Encryption Standard. Due to this it is difficult to hack the data by the intruder and it reduces the energy consumption levels as shown in simulations.

VI ACKNOWLEDGMENT

They take this opportunity to acknowledge those who have been great support and inspiration through the research work.

VII REFERENCES

[1]. Fast Transmission to Remote Cooperative Groups:A New Key Management Paradigm Qianhong Wu, *Member*, *IEEE*, Bo Qin, Lei Zhang,Josep omingo-Ferrer, *Fellow*, *EEE*, Jes´us A. Manj´on

[2]. Y. Zhang and Y. Fang, “ARSA: An Attack-ResilientSecurity Architecture for Multi-Hop Wireless Mesh Networks,” *IEEE J. Sel. Areas Commun.*, vol. 24, no.10, pp. 1916-1928, Oct. 2006.

[3]. K. Ren, S. Yu, W. Lou and Y. Zhang, “PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no.2, pp. 203-215, Feb. 2010.

[4]. B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu and S. Guizani, “A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study,” *IEEE Trans.Veh. Technol.*, vol. 58, no. 1, pp. 398-408, Jan. 2009.

[5]. M. Burmester and Y. Desmedt, “A Secure and Efficient Conference Key Distribution System,” in *Advances in Cryptology–EUROCRYPT’94*,LNCS, vol. 950, pp. 275-286, 1995.

[6]. M. Waldvogel, G. Caronni, D. Sun, N. Weiler and B. Plattner, “The VersaKey Framework: Versatile Group Key Management,” *IEEE J. Sel. Areas Commun.*, vol. 17, no. 9, pp. 1614-1631, Sept. 1999.

[7]. M. Steiner, G. Tsudik and M. Waidner, “Key Agreement in Dynamic Peer Groups,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 8, pp.769-780, Aug. 2000.

[8]. A. Sherman and D. McGrew, “Key Establishment in Large Dynamic Groups Using One- way Function Trees,” *IEEE Trans. Software Eng.*,vol. 29, no. 5, pp. 444-458, May 2003.

[9] .Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G.Tsudik, “Secure Group Communication Using Robust Contributory Key Agreement,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, no. 5, pp. 468-480, May 2004.

[10]. Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, “Asymmetric Group Key Agreement,” in *Advances in Cryptology–EUROCRYPT’09*,LNCS, vol. 5479, pp. 153-170, 2009.

[11].Y-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, “Constructing Secure Group Communication over Wireless Ad Hoc Networks Based on a Virtual Subnet Model,” *IEEE Wireless Comm.*, vol. 14, no. 5, pp.71-75, Oct. 2007.

[12]. Y. Sun, W. Trappe and K.J.R. Liu, “A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks,” *IEEE/ACM Trans.Netw.*, vol. 12, no. 4, pp. 653-666, Aug. 2004.

[13]. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013 “A Novel Approach for Data Encryption Standard Algorithm” Prashanti.G, Deepthi.S, Sandhya Rani.K

[14]. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 ISSN: 2277 128X**”** Study of MANET: Characteristics, Challenges, Application and Security Attacks”

[15]. International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 www.ijesi.org ||Volume 3 || Issue 6 || June 2014 || PP.52-56 “Secure Transmission over Co-operative Groups: A New Key Management Archetype and Data Leakage Prevention”, Ms. Soji Charles, Mr. Scaria Alex

[16]. International Journal of Computer Science (IIJCS) Volume 2, Issue 1, January 2014 ISSN 2321-5992 Secure Transmission Over Remote Group: A New Key Management Prototype Mrs.K.Sudha 1, Mr. J.Prem Ranjith2, Mr. S.Ganapathy3, Mr.S.Ranjith Sasidharan4