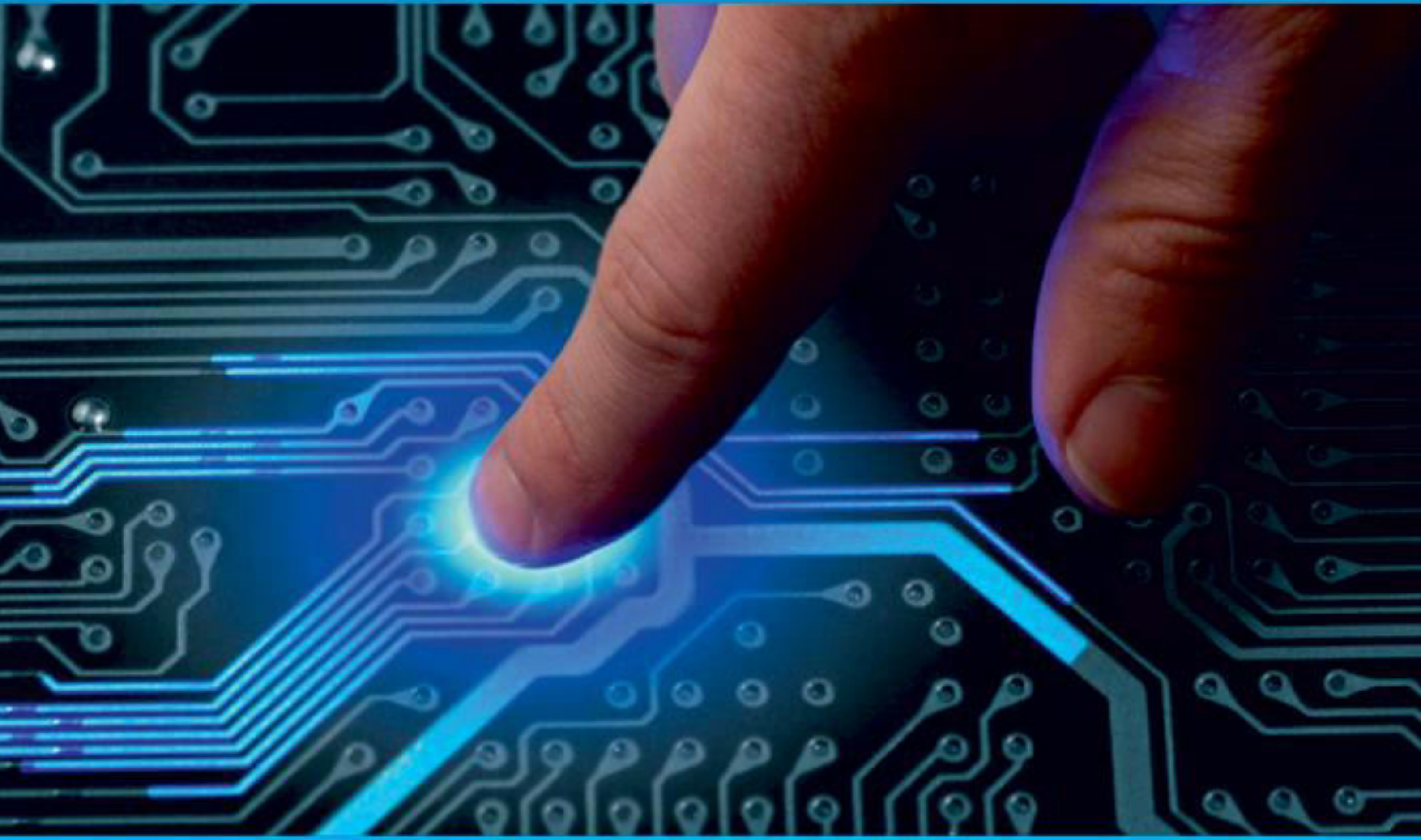
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 8, August 2022

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

Additional Security of Confidential Based Routing Algorithm for MANET

R. GAYATHRI, R. KIRUBA KUMARI,

M.Phil Scholar, Department of Computer Science, Padmavani Arts & Science College for Women,

opp. Periyar University, Kottagoundampatti, Salem, Tamil Nadu, India

Assistant Professor/HOD, Department of Computer Science, Padmavani Arts & Science College for Women,

opp. Periyar University, Kottagoundampatti, Salem, Tamil Nadu, India

ABSTRACT: MANET is very applicable for many crucial applications such as patient monitoring, environmental control, Battlefield environments or military, rescue or emergency operations, natural disaster relief operations, transport systems and conferences. So this MANET is best suited for sending specific or sensitive or confidential information to a specific person. But the security of information's in general is very low in wireless networks, and so in this advanced method uses a more satisfactory method for security in this category of environment, so, here TDES algorithm utilize for the security purpose. Generally, a lot of power is required for devices when utilizing the Network. If it wants to ameliorate the lifetime of Networks, need to diminish the energy consumption of the MANET. This presentation method uses the LDC algorithm to well planned and so lessen the energy. So this paper, MANET utilizes two very efficacious methods to maximize security purpose of salient news and diminish the energy consumption of the MANET. In this paper, those algorithms have successfully addressed the need for this proposed method.

KEYWORDS*:* MANET (Mobile Ad Hoc Network), security, energy consumption, TDES (Triple Data Encryption Standard), LDC (Low Duty Cycle)

I. INTRODUCTION

Ad-hoc networking allows new devices to maintain the connections of the network, and can add devices if needed and delete them if not needed. The MANET is a genre in this respect; But MANET's applications are a bit different. It is controlled by its power sources, from high-powered large-scale networks of small, fixed-networks.

One of the critical issues of Wireless is security and energy consumption. The main purpose of this proposed method is to improve the efficiency and operation of the MANET. Why energy consumption is so important in MANET's critical issues is that MANET nodes are powered by battery. So the focus of this researcher turned to issues of safety and energy consumption. If the power of the MANET node is low, the routing capacity of the MANET is reduced, thus, reducing the efficiency and longevity of the network. The advancement of technology at Battery has been far behind the development of semiconductor technology. Therefore, reducing the energy consumption at the nodes is essential here to improve the performance of the Network.

If MANET uses wireless transmissions, the protection of data is essential. From the node of each mobile, it is very difficult to implement a secure control center. So this paper, the solution to both of these problems is making the decision to solve.

Paper In [1], they have put forward some methods aimed at protecting the important data's used in MANET. For that purpose, the researcher had put forward some attacks. In it, Black hole called the attack very important. But there is no great benefit to it. When using the MANET Network, the power of the mobile phone is quickly exhausted due to the low battery in the nodes. In [2], focusing on this concept, they used the AODV protocol. This is a routing protocol, so by selecting routes for routing, they reduce the breakdown of the connection. But this AODV method did not improve that much.

In [3], they have proposed the process of enhancing the effectiveness of QOS and protections. Researchers have considered two solutions, using the CLD method to improve the performance of the QOS and the SSV method to increase the security. But this too is not used to that extent. In [4], the aim is to reduce the energy consumption in the nodes and increase the lifespan of the network. So the researchers decided to solve their problem using the method of EAODV. They have developed EAODV and differentiated it with AODV, DSDV and DSR, but security is limited.

In [5], each person using the MANET network, to security can must gave simply use their own address. For that they have used the DDH, DSR and HASH function, but this increases the energy. In [6], we show that when data transmission takes place, energy consumption depends on the data. Researchers in the sixth paper have therefore used the NS2 technique to reduce energy consumption, but this does not safety to data.

In [7], researchers focus on nodes because data is transmitted only by nodes. As they research those nodes, the nodes are exposed to some harmful attacks. So they used two methods, AODV and NS2, but it takes a lot of energy. In [8], we used the DSR because that the nodes are operate by battery. In addition, they have said that AODV is doing less than a DSR. In [9], data on the transmission of vulnerabilities, such as DOS, are affected, so the author of in this paper has tried to protect the MANET. So they used this IDS idea. But it did not succeed.

In [10], Next generations considering the high use of this MANET system, the editor of the 10th paper chose the REDEAR method. But there was very little security involved.

II. TDES / 3DES USED FOR SECURITY PURPOSE

Since the security of confidential data is very low in this MANET system, this proposed method uses the TDES/3DES method. This TDES system is based on DES. Therefore, it is very easy to change the software used before, to use Triple DES. It has high reliability; In addition, it uses a long key to prevent multiple attacks. If used correctly, this TDES method will keep data secure in effectively.

The key-K of the 3DES must be generated before using the 3DES. It contains three different types of keys: K1, K2 and K3. This means that, length of 3TDES key 3×56 = 168 bits. The concept of encryption can be found in:

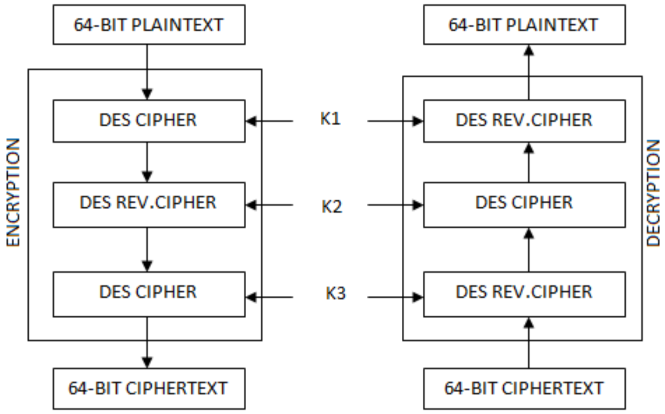


Fig.1: Encryption and Decryption

Encryption and Decryption is specified in the following steps:

1. To encrypt simple text modules, use single-DES with key K1.
2. To decrypt the output of step one, use a single DES with the key K2.
3. To re-encrypt the output of step two, use a single DES with key K3.
4. Finally, the release of Step Three is the Cipher Text.
5. To decrypt the cipher text again, first decrypt it using a key K3.
6. Then encrypt with K2 and finally decrypt with K1.

This TDES system has activities like encrypt-decrypt-encrypt. This process can be implemented by assigning the same value to K1, K2 and K3 in DES.

Encryption can be defined by the following mathematical equation:

$$\text{Cipher text} = \text{E-K3 (D-K2 (E-K1 (Plain text)))}$$

Decryption can be represented by the following equation:

$$\text{Plain text} = \text{D-K1 (E-K2 (D-K3 (Cipher text)))}$$

It is very easy to implement this 3DES method in both hardware and software and more secure compare with other cryptography algorithms.

III. LDC FOR ENERGY CONSUMPTION

The energy consumption is greatly enhanced by the use of the MANET system to exchange information here. In addition, we used 3DES in this paper to make data secure, It takes a lot of energy to protect data in a very efficient way. Therefore, this paper uses LDC to reduce this energy consumption potential. That means the goal of LDC is to put it to sleep when mobile nodes are out of work. What this means is that sleeping of the nodes will not make sense of unnecessary activity, reducing data storage and energy. In this case, a certain node can only sleep, and then other nodes can collect information.

In this paper use the Berkeley MAC type in LDC. B-MAC defines the waking period of the entire LPL structure, it call this the Check interval. The Check interval is denoted by T_i. The check interval consists of two parts, the listen interval and the sleep interval. The total number of important power consumers of the sensor node has five:

1) Transmitting energy E_{tx}
2) Receiving energy E_{rx}
3) Listening energy E_{listen}
4) Sampling sensor data energy E_{sensor}
5) Energy of sleeping E_{sleep}

Total energy E can be calculated by the following equation:

$$E = E_{tx} + E_{rx} + E_{listen} + E_{sensor} + E_{sleep}$$

The time it takes for each node to sensor the collect information and sample is 1100ms. The sampling rate can be as follows:

$$R_s = 1 / (T_s * 60)$$

Where,

R_s = sampling rate

T_s = Time to sensor

The sampling rate is chosen depending on the network conditions and the requirements of the application. The energy-related sample data, E_{sensor} is given below.

$$F_d = T_{sensor} * R_s$$

$$E_{sensor} = F_d * C_{sensor} V$$

Where,

F_d = Frequency of sample data

C_{sensor} = Current consumption of sample data

V = Supply voltage

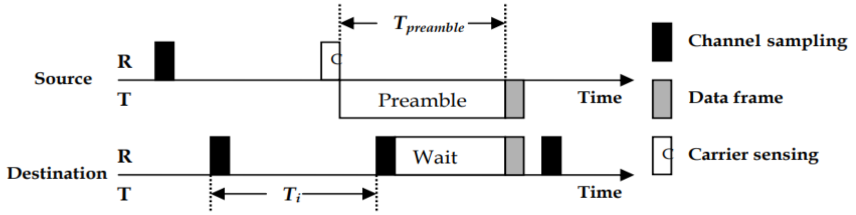


Fig.2: Operation of Berkeley MAC

The energy is consumed depending on the length of the preamble packet and data packets. Thus the energy of the exchange can be stated as:

$$F_{tx} = R_s * (N_{preamble} + N_{data}) * T_{txb}$$

$$E_{tx} = F_{tx} * C_{txb}V$$

Where,

F_{tx} = Frequency of packet transmission
$N_{preamble}$ = length of the preamble packet
N_{data} = Times of Data packet generated
T_{txb} = Time taken to exchange 1 byte
C_{txb} = the energy taken when exchanging 1 byte

The receiving power of a node is shaped by the reception of packets from its n neighbors, the power of that receives data is stated as follows:

$$F_{rx\,\leq}\ n * R_s * (N_{preamble} + N_{data}) * T_{rxb}$$

$$E_{rx} = F_{rx} * C_{rxb}V$$

Where,

F_{rx} = Frequency of received packet transmission
T_{rxb} = Time taken to received 1 byte
C_{rxb} = the energy taken when receiving 1 byte

The length of the preamble packet is,

$$N_{preamble} \geq [T_i / T_{rxb}]$$

The value of E_{sample} is 17.3 PJ. The energy consumed when the node is listening:

$$E_{listen} \leq E_{sample} * (1 / T_i)$$

The frequency of listening and transient timing can be specified as follows:

$$F_{listen} = (T_{rinit} + T_{ron} + T_{rx\,/\,tx} + T_{sr}) * (1 / T_i)$$

$$T_{transient} = T_{rinit} + T_{ron} + T_{rx\,/\,tx}$$

Where,

T_{rinit} = Time taken to start the radio
T_{ron} = time taken to turn on the radio and its oscillator
$T_{rx\,/\,tx}$ = time taken to switch the radio to the receive mode
T_{sr} = time taken to sample the channel.

Sleep time refers to the time remaining for each second. The energy consumed is as follows:

$$T_{sleep} = 1 – F_{rx} – F_{tx} – T_d – T_{listen}$$

$$E_{sleep} = T_{sleep} * C_{sleep}V$$

Where,

C_{sleep} = current consumed while a node is sleeping
T_{sleep} = time taken while a node is sleeping

Finally, the amount of energy consumed during the transmission of information was reduced and was calculated as less energy.

IV. RESULTS AND DISCUSSION

The main purpose of this study is to address the issues that come up when using MANET. It uses some methods, with the purpose of making it more efficient than the previous application. This study is based on the performance of the sensor nodes. Using these methods efficiently improves the lifetime of Network, reduces energy and provides greater security.

| DOI: 10.15680/IJIRCCE.2022.1008009 |

	DES	TRIPLE - DES
Key size (bits)	56	112 or 168
No. of rounds	16	48
No. of sub keys	16	48
Key generation	Shift permute	Shift permute
Block size (bits)	64	64
Mathematical operations	XOR, Fixed S - Boxes	XOR, Fixed S - Boxes
attack	Broken: Brute Force, 1998	No known attack
Memory used (KB)	18.2	20.7

Table 1: Comparison between DES and 3DES

In Table 1, the algorithms such as DES and 3DES are compared based on performance. In that, it is difficult to steal the data incorrectly, as the TDES algorithm is more than DES in key size. Because of the number of rounds and the number of sub keys of TDES is more than DES, So difficult to access in the application. Memory size of the TDES is also more than DES.

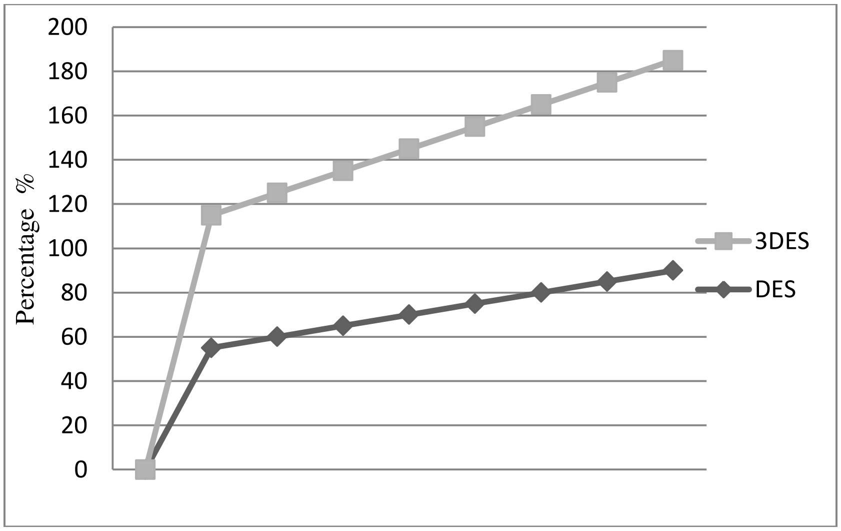


Fig.3: Comparison of Security Performance

In Fig.3, TDES's the efficiency of security is higher in percentage compared to the DES method. This has therefore increased the effectiveness of the protection of the MANET.

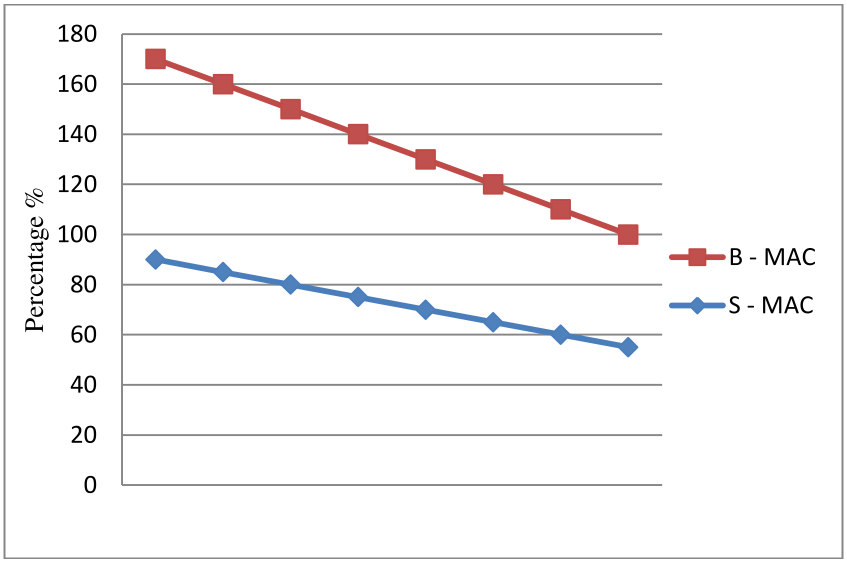


Fig.4: Comparison of Energy Consumption Performance

In Fig.4, the S-MAC is higher than the B-MAC compared to the energy consumption efficiency. Thus, B-MAC is considered to be the best at reducing energy consumption. Therefore, it can greatly reduce energy consumption when using MANET.

V. CONCLUSION

This current paper is developed with the intention of making it comfortable to use for all users of MANET without any harm. That goal is to increase safety and reduce the energy consumption. We used the TDES system to focus on security. This TDES system has given 95% percent of security efficiency. So this has proven to be the best. We then used the B-MAC with the aim of reducing the energy consumption. It transports the energy much less than the S-MAC. Therefore it is best suited to MANET. We implemented the performance of these two algorithms in the NS-2.3 (Network Simulator-version 2.3).

REFERENCES

1. Farhan Abdel-Fattah, Fadel AlTamimi, Khalid A. Farhan, Feras H. Al-Tarawneh, “Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs”, IEEE Jordon international joint conference on electrical engineering and information technology, 978-1-5386-7942-5/19/$31.00 ©2019 IEEE.
2. Muhammad Khalid Riaz, Fan Yangyu, Imran Akhtar, “Energy Aware Path Selection based Efficient AODV for MANETs”, Proceedings of 2019 16th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 8th – 12th January, 2019.
3. Manish Kumar, Rahul Bhandari, Ajay Rupani, Jakir Hussain Ansari, “Trust-based Performance Evaluation of Routing Protocol Design with Security and QoS over MANET”, 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE-2018) Paris, France 22-23 June 2018.
4. Reena Aggarwal, “QoS based Simulation Analysis of EAODV Routing Protocol for Improving Energy Consumption in Manet”, 2018 International Conference on Intelligent Circuits and Systems, 978-1-5386-6483-4/18/$31.00 ©2018 IEEE.
5. Milan Kumar Dholey, Manab Kumar Saha, “A Security Mechanism In DSR Routing For MANET”, Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018), IEEE Conference Record: # 42666; IEEE Explore ISBN: 978-1-5386-3570-4.

6. Saurabh Kumar, Debasrit Mohanty, Alisha Panda Lipsa, Sandeep Nigam Soumyashree S. Panda, Prakhar Golcha Srichandan Shobhanayak, " Energy Optimization for Cooperative Multipath Routing in MANETs using Network Coding", International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), ISBN:978-1-5386-4119-4/18/$31.00 ©2018IEEE
7. Gurveen Vaseer, Garima Ghai, Dhruva Ghai, "Distributed Trust-Based Multiple Attack Prevention for Secure MANETs", 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), 0-7695-6618-9/18/$31.00 ©2018 IEEE.
8. Mousami Vanjale, J. S. Chitode, Shilpa Gaikwad, "Residual Battery Capacity Based Routing Protocol for Extending Lifetime of Mobile Ad Hoc Network", 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), Amrutvahini College of Engineering, Sangamner, Ahmednagar, India. Feb 8-9, 2018.
9. Desai Rahul Babasaheb and Indhumathi Raman, "Survey on Fault Tolerance and Security in Mobile Ad Hoc Networks (MANETs)", 2018 3rd International Conference for Convergence in Technology (I2CT), The Gateway Hotel, XION Complex, Wakad Road, Pune, India. Apr 06-08, 2018.
10. Shreya Roy and Sonali Chouhan, "REDEAR: Relative Density Aware Routing Algorithm for Energy Efficiency in MANETs", 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 978-1-5386-8134-3/18/$31.00 ©2018 IEEE.
11. G. Boggia, P. Camarda, L. A. Grieco, and G. Piro, ``Extended EDCA for delay guarantees in wireless local area networks," Pervasive MobileComput., vol. 5, no. 5, pp. 402_418, 2009.
12. S. A. M. Tariq and F. Granelli, ``Performance analysis of wireless ad-hoc network based on EDCA IEEE802.11e," World Acad. Sci., Eng. Technol., vol. 4, no. 9, pp. 1322_1325, 2010.
13. P. K. Hazra and A. De, ``Performance analysis of IEEE 802.11e EDCA with QoS enhancements through TXOP based frame-concatenation and block-acknowledgement," Int. J. Adv. Tech, vol. 2, no. 4, pp. 542_560, 2011.
14. S. Rashwand and J. Mi²i¢, ``Stable operation of IEEE 802.11e EDCA: Interaction between offered load and MAC parameters," Ad Hoc Netw., vol. 10, no. 2, pp. 162_173, 2012.
15. D. Vassis and G. Kormentzas, ``Delay performance analysis and evaluation of IEEE 802.11e EDCA in _nite load conditions," Wireless Pers. Com- mun., vol. 34, nos. 1_2, pp. 29_43, 2005.
16. A. Banchs and L. Vollero, ``Throughput analysis and optimal conjuration of 802.11e EDCA," Comput. Netw., vol. 50, no. 11, pp. 1749_1768, 2006.
17. I. Koukoutsidis and V. A. Siris, ``802.11e EDCA protocol parameterization: A modeling and optimization study," in Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw., Jun. 2007, pp. 1_9.
18. C. Cano, B. Bellalta, A. Sfairopoulou, and J. Barceló, ``Tuning the EDCA parameters in WLANs with heterogeneous traf_c: A _ow-level analysis," Comput. Netw., vol. 54, no. 13, pp. 2199_2214, 2010.
19. K. Kosek-Szott, M. Natkaniec, and A. R. Pach, ``A simple but accurate throughput model for IEEE 802.11 EDCA in saturation and non-saturation conditions," Comput. Netw., vol. 55, no. 3, pp. 622_635, 2011.
20. F. Peng, B. Peng, and D. Qian, ``Performance analysis of IEEE 802.11e enhanced distributed channel access," IET Commun., vol. 4, no. 6, pp. 728_738, 2010.
21. A. L. Ruscelli, G. Cecchetti, A. Alifano, and G. Lipari, ``Enhancement of QoS support of HCCA schedulers using EDCA function in IEEE 802.11e networks," Ad Hoc Netw., vol. 10, no. 2, pp. 147_161, 2012.
22. S. Chakraborty, P. Swain, and S. Nandi, ``Proportional fairness in MAC layer channel access of IEEE 802.11s EDCA based wireless mesh networks," Ad Hoc Netw., vol. 11, no. 1, pp. 570_584, 2013.
23. S. Kim, R. Huang, and Y. Fang, ``Deterministic priority channel access scheme for QoS support in IEEE 802.11e wireless LANs," IEEE Trans.Veh. Technol., vol. 58, no. 2, pp. 855_864, Feb. 2009.
24. X. Liu and T. N. Saadawi, ``IEEE 802.11e (EDCA) analysis in the presence of hidden stations," J. Adv. Res., vol. 2, no. 3, pp. 219_225, 2011.
25. Z. Huang, C. C. Shen, C. Srisathapornphat, and C. Jaikaeo, ``A busy-tone based directional MAC protocol for ad hoc networks," in Proc. MILCOM, vol. 2, Oct. 2002, pp. 1233_1238.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi® crossref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com