ISSN No. 0976-5697

Volume 5, No. 6, July-August 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A New Blowfish Secret-Key Block Cipher Based Cooperative Protocol Incentive Scheduler Algorithm for Wireless Network

A. Prakash
Associate Professor, Department of Master of Computer Applications, Hindusthan college of arts and science, Coimbatore, Tamilnadu, India

C. Deepika
Research scholar, Department of Computer Science, Hindusthan college of arts and science , Coimbatore, Tamilnadu, India

Abstarct: In wireless networks the coverage extension area is used to increase the network connectivity exclusive of escalating the infrastructure that is the one of main use of cooperative communication. The coverage extension concern wants the cooperation of border mobile nodes to transmit the packets of neighboring nodes which are positioned outside the base-station region. In this effort we suggest a new security based incentive scheduler algorithm that is able to expand the wireless coverage for potential mobile transmitting nodes. Certainly, in terms of QoS and energy consumption the cost of cooperation can be expensive that do not inspire the nodes to cooperate. Where the security based incentive approach returns the cooperative nodes. In the QoS management the percentage of cooperation is considered to facilitate stimulate the border nodes to cooperate and then to enlarge the wireless area. Here with the security can be improved by using Blowfish which is a variable-length key block cipher which is only suitable for applications where the key does not modify regularly, like a communications link or an automatic file encryptor. Furthermore, the monitoring mechanism is projected to suitably assess the cooperation rate of every node. The outcomes illustrate that not only the proposed solution permits the border nodes to cooperate exclusive of the negative impact but furthermore improve the QoS parameters.

Keywords: Incentive Scheduling, Coverage Extension, Cooperation, Quality of Service, Multipath Fading, Quality of Service (QOS), Selfish Nodes, Blowfish Secret-Key Block Cipher.

I. INTRODUCTION

The general procedure of estimation of coverage area for mobile adhoc network is to satisfy network connectivity not including growing the communications. These issues require best collaboration of boundary movable nodes in the direction of commune the packets of adjacent nodes by means of the principle of be situated external the base-station district. The mobility of communicate nodes has to be taken into explanation to be secure to certainty. Additional mechanism makes use of movable transmit nodes to make bigger the wireless coverage by means of throughput development [1], [2]. Conversely, no encouragement move toward is well thought-out in the concluding works. The communicate nodes be required to distribute their throughput by means of additional nearest nodes with the intention of can collision their have possession of packets' communication.

Consideration of energy utilization plays major important role for communicates nodes than the individual of further conventional nodes. They broadcast not merely their individual packets although the packets of additional nearest nodes because glowing. Consequently, the addict of prospective communicate nodes be able to put out of action the two-way functionality in the direction of maintain the show in conditions of QoS simply intended for it's be present in control of announcement. In this article, we regard as with the intention of movable communicate nodes are not measurement of the predetermined wireless communications. With the intention of is why the encouragement approach intended for prospective mobile communicate nodes have to be present full interested in explanation in the collaboration procedure propose. The most important motivation models converse in the reproduction are support on game theory [3],[4].

Conversely, it is durable to put into practice these models for the reason with the intention of several suppositions and for the reason with the intention of no achievement or show assessment is specified.

Furthermore, the development algorithms include previously be put into practice in the access point and routers, therefore make easy our learning. For illustration, the nodes positioned by the side of two hops beginning the services presented through communicate nodes such as the Internet. Several numbers of researches have been worked in earlier work to discover optimal path communication nodes to satisfy Quality of Services (QoS). Other works compact through the most favorable quantity of hops of communicate nodes. On the other hand, they suppose with the intention of the communicate nodes through characterization are predetermined and two-way in the case of a self-motivated process in wireless where each and every nodes in the networks progress without restraint and potentially self-interested. Consequently, the user of the achievable communicate node can disable the supportive functionality in order to preserve the results in terms of QoS simply for its individual statement. The most important involvement of effort is:

a. In this work first motivation move toward by means of QoS concern for the movable relayed nodes in regulate to make bigger the coverage area.
b. The method combines the different results of QOS constraints and estimate cross layer rate through communication mechanism with scheduling process.
c. The data transformation process for Pocket Brief uses the Blowfish Algorithm for Encryption and Decryption, respectively.
d. The experimentation results of proposed and existing solution measured in terms of delay, throughput, and

relaying effectiveness through diverse collaboration proportion of nodes.

The remaining study of this paper is as follows: In section II the existing works related to coverage extension using cooperation in wireless networks, incentive models, and scheduling algorithms. Section III provides a detailed description of the system under study and describes the proposed coverage extension protocol based on the security based incentive scheduler. The fourth section presents the obtained simulation results and their analysis. Finally, Section V concludes this paper and presents our future works.

II. BACKGROUND STUDY

The usual methods like Round Robin (RR) [5] are modified in the direction of the wireless background and make available underprivileged throughput. Additional in recent time's intensive investigate efforts include be through in arrange to suggest supplementary well-organized schedulers. Pleasing assistance of multiuser and regularity assortment in regulate to make the most of the structure throughput, each and every one these schemes robustly rely scheduled assortment designed for gift their high-quality accuracy results . It apportion the reserve by the side of a specified moment in time to the dynamic mobile in the midst of the maximum signal to noise ratio [6],[7]. These consequences in a rigorous punishment designed for them which do not optimistic two-way networks and exposure addition.

In earlier routing [8],[9], relying on the information of geographic position information of nodes to formulate restricted direction conclusion, is a capable direction-finding explanation to the command of mounting well-organized in MANET. In current years, by means of the important move forward of substantial cover communication procedure, two-way message designed for wireless networks have develop into an vigorous explore area appropriate in the direction of its capability in the direction of generate spatial assortment by means of node association. Present have been a variety of two-way assortment design in the earlier works [10],[11].

Optimization routing protocol methods also proposed in earlier works [12] [13] to decide the less power consumption with predetermined communication velocity assured and then implemented an less efficient path routing methods to accomplish basically Minimum Power Cooperative Routing (MPCR) [14] algorithm by means of certain throughput assured.

CoopGeo protocol was proposed in earlier work [15], for node to node communication with one hop and multi hop data transmission with less most favorable relay for routing schemas and subsequently by means of two-way communication to improve the association superiority. It may not take the coverage area in the MANET with cross layer estimation and it is different from normal process of protocol for scheduling process with routing protocols. The general procedure of the coverage estimation protocol methods was developed by earlier work [16] and it is implemented to each and every access point in mobile nodes with routers.

a. Blowfish Secret-Key Block Cipher Coverage Extension Protocol for Incentive Scheduler:

To perform security level of data transmission among mobile nodes along with access point with best cluster head selection in MANETs. Definitely, make the most of the organization capability is individual of the nearly everyone fundamental matter of wireless networks, and a central move toward is desirable to permit opportunistic development, which make available important structure throughput increase evaluate by means of a automatic decentralization basis distribution.

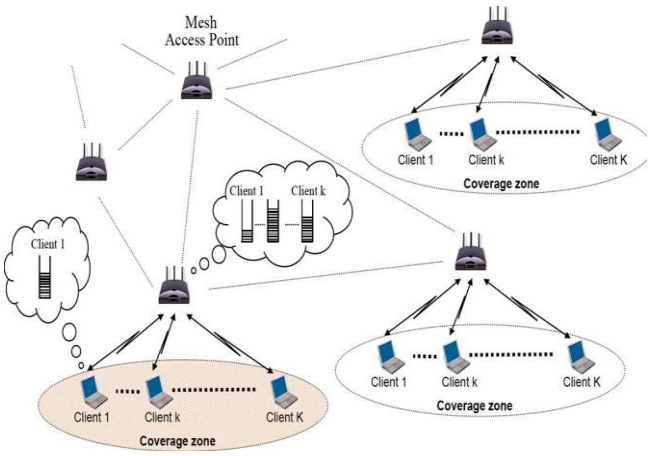

Figure.1. Allocation of radio resources among mobile nodes

The scheduler performs radio allocation process the mobile nodes transmit along with control condition, presently collaboration proportion, arrangement self-assurance proportion, interchange accumulation. The information of the direct condition is hypothetical in the direction of exist obtainable at the receiver [17]. The steps maximizes the results high transmission range and with more security. At each research period, the scheduler calculate the greatest amount of bit $m_{k,n}$ with the intention of know how to be broadcast in a point in time period of subcarrier n qualification allocate to a transportable k, designed for each and every one k and each and every one n. The symbol miscalculation opportunity and the position in time opening interval are unspecified to be present equivalent to time duration T_s is specified in [18]. The probability of the transmission range is defined in the power based allocation $P_r(q,k)$ with transmission range with bits values of q in each and every resource unit values in the nodes during transmission process in the access point with less $BER_{target,k}$ of mobile k is a purpose of the intonation category, its categorize. For each and every modulation type the nodes in the channel is defined as flat fading channel :

$$P_r(q,k) = \frac{2N_0}{3T_s}\left[\text{erfc}^{-1}\left(\frac{BER_{target,k}}{2}\right)\right]^2 (M-1)$$

Where $M = 2^q$ and erfc is the complementary error function. The results of $P_r(q,k)$ might moreover be strong-minded in perform support on BER account and modernized according to data collected from BER. The subcarrier results of transmission range of nodes are needed to satisfy following condition $P_{k,n} \le P_{max}$. It is measured with experienced node level $P_r(q,k) \le a_{k,n}P_{max}$. Consequently, the greatest integer of bits $q_{k,n}$ of mobile k which know how to be broadcast on a moment in time period of subcarrier n

at the same time as maintenance lower than its BER objective is: $q_{k,n} \le \left\lfloor \log_2\left(1 + \frac{3P_{max} \times T_s \times a_{k,n}}{2N_0\left[\mathrm{erfc}^{-1}\left(\frac{BER_{target,k}}{2}\right)\right]^2}\right)\right\rfloor$

Where $S = \{0, 2, 4, \ldots, q_{max}\}$. Consequently, the maximum number of bits $m_{k,n}$ RU is due to the mobile k is: $m_{k,n} = \max\{q \in S, q \le q_{k,n}\}$. MaxSNR base of each and every resource allocation process need to satisfy the : $m_{k,n}$ to the mobiles nodes in the networks . In order to expand more coverage area to each mobile sensor nodes in the simulation model methods throughput maximization, a novel parameter is introduced and applied to number of bits in the QAM model for efficient resource allocation process. This can be efficiently performed by using cross layer estimated to each node in the networks it is defined as Incentive Parameter (IP_k) along with cooperative allocation of resources ,it is measured as follows

$$IP_k = \frac{R_k}{D_k} = \frac{D_k + \sum_{i=0\ldots i=k}^{i} D_{ki}}{D_k}$$

where R_k best transmission results for mobile nodes k ,it is estimated based on summation of the data transmission D_k and D_{ki} ,it is simultaneously watched by access points in the coverage area network .it also estimate confidence level of nodes in the networks T_k depends on the communication among the make known cooperative ratio and the experiential promote ratio with values belongs to zero to one . If the nodes are watched by access point it is set one or else it becomes zero in scheduling process. The allocation of resources for mobile nodes based on time duration slot with queue based mobile allocation nodes with other nodes is strong-minded through the importance of its CEI parameter: $CEI_{k,n} = m_{k,n} \times \frac{R_k}{D_k} \times T_k$

This results in a well-organized scheme with the intention of certification enhanced association connectivity at the same time as keep away from substitution through the scheme capability. To improve the security level during data transmission process among one mobile nodes to another mobile nodes in the network, in this work we additionally add security level algorithm that adds that generates the key for each and every algorithm process in the network to improve security level of process .Initially firsts data are transmitted from one to another nodes along with bit allocation and confidence level of nodes in the network. Generally blowfish algorithm generates key using data transmitted with public and private keys. It follows general procedure of the Foisted Network, in iterative manner with a straightforward encryption purpose in several times. the size of the each and every blocks in the network consist of the 64 bits data during transmission process in mobile nodes with access point specification and length of key values upto multiplication of 7 into 64 bits values ,it is easily applied to any encryption data if it becomes high and low similarly. Generally it is defined as under the category of the variable length process and it is easily applied to data transmission process during mobile nodes or any node to node communication process .The structure of network for Feistel Network is shown in figure 2

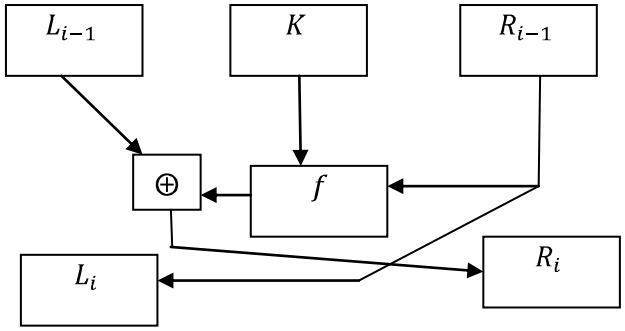

Figure 2: Feistel Network

The structure those mentioned above is used to design the efficient encryption scheme for during data transmission process in mobile nodes to another mobile nodes in the access points ,the L_{i-1} be number of mobile nodes in the wireless networks ,k be the number of keys generated to each nodes in the wireless networks , R_{i-1} be the data in the mobile nodes .The f combine all the data ,mobile nodes and keys generated to each nodes automatically using the above mentioned encryption process. Priority of mobile nodes during transmission with admiration to other nodes in the wireless sensor networks. There are two major characteristic in this methods to ensure security level of mobile nodes in wireless network, one of them is efficient structure of designing for nodes in the wireless network, and then other choice is to perform encryption with key generated from above figure 2 during data transmission process. Improve the security level of the wireless network in this work additionally sub key also generated for each and every data transmission Coverage Extension Protocol with efficient scheduling process in network .Sub key are generated to each nodes in the scheduling process with ensures of their entropy function . It is automatically generated distribution function with any distribution methods such as uniform, gamma and etc,Once key are generated it is efficient to perform scheduling task in coverage extension protocol, if the key are not satisfied it is not allowed to perform scheduling for that specific nodes. The encryption process of data transmission and sub key generation procedure for scheduling methods is shown in below:

Algorithm 1 : Blowfish

Separate the data into number of blocks during data transmission process

Each of the data in the mobile nodes have contains equal bit length 64-bit.

Otherwise it atleast contains 32 bit

Perform key generation for each data for mobile nodes and generates sub key

Perform number of iterations for each data in the mobile nodes

Finds the attacks in the network for best scheduling

Sub keys are generated in the following algorithm 2

a. Has no linear construction with the intention of decrease the complexity of comprehensive exploration.
b. Uses a propose with the intention of straightforward to understand.

The subkeys are calculated using the Blowfish algorithm:

Algorithm 2:Subkey generation

c. Define $P-$array of the data in the mobile nodes and then define S boxes
d. Initialize first the P-array and then the four S-boxes, in

order, with a fixed string.

e. Perform XOR operation for data transmission for mobile nodes with 32 bits ,similarly it is applied to four boxes of S
f. Encrypt the $P-$array, using the subkeys from above two steps
g. If it satisfied then replace $P1$ each array with another $P2$array values in the network
h. Then encrypt the mobile node data with subkeys.
i. If it satisfied then replace $P3$ each array with another $P4$ array values in the network
j. Repeat the steps all the $P-$array of the data in the mobile nodes completed

III. EXPERIMENTATION RESULTS

Evaluate the performance of the proposed Blowfish Secret-Key scheduling, and compare with normal cooperative allocation schemas .In this work mainly focus on two major parameter two estimate results of methods such as the mean packet delay and the represent throughput make available at each one mobile.

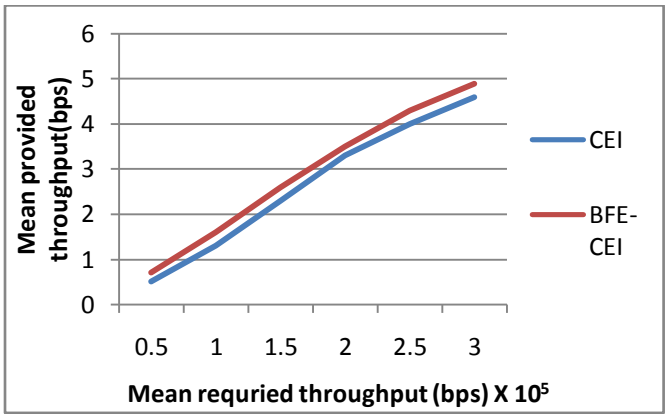

Figure 3. Relay efficiency

In the Figure 3 measures communicate effectiveness in terms of the entirety mean throughput with the intention of every scheduling algorithm has permissible to make available absent of the group. Then observation with the intention of existing methods results the bad compared with BFE-CIE when the system capability is reached. This is due to an inequitable and far above the position consequence of the most excellent two-way mobile which communicate in the direction of an elevated system addition capability.

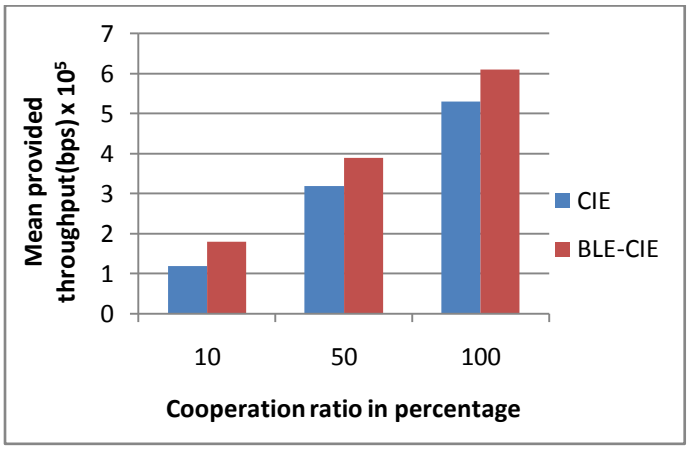

Figure 4: Provided Throughput Function of the Cooperation Ratio

The Figure 4 concludes throughput function of the cooperation ratio along performance estimation results, it consider the traffic results of 500 kb/s designed for every mobile, the behavior of nodes in the network have higher results when compared to cell value for each nodes in the network during the throughput according to their support proportion and with the intention of the full amount.

IV. CONCLUSION AND FUTURE WORK

In this paper, developed a new encryption based scheduling method to improve the security of mobile nodes during transmission process. Here with the security can be improved by using Blowfish which is a variable-length key block cipher which is only suitable for applications where the key does not modify regularly, like a communications link or an automatic file encryptor. In the QoS management the percentage of cooperation is considered to facilitate stimulate the border nodes to cooperate and then to enlarge the wireless area. Additionally, the monitoring machine is predictable to correctly evaluate the collaboration velocity of all nodes. The conclusion demonstrate with the intention of not merely the proposed explanation authorize the boundary nodes in the direction of work together restricted of the unconstructive collision but additionally progress the QoS parameters with the intention of be of assistance the structure accomplish a disinterested situation.

V. REFERENCES

[1]. L. Xiao, T. E. Fuja, and D. J. Costello, "Mobile relaying: Coverage extension and throughput enhancement," IEEE Trans. Commun., vol. 58, no. 9, pp. 2709–2717, Sep. 2010.

[2]. B. Bakaimis and T. Lestable, "Connectivity investigation of mobile relays for the next generation wireless systems," in Proc. 61th IEEE VTC, Stockholm, Sweden, Nov. 2005, pp. 2192–2195.

[3]. L. Chen, L. Libman, and J. Leneutre, "Conflicts and incentives in wireless cooperative relaying: A distributed market pricing framework," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 758–772, May 2011.

[4]. L. Dapeng, L. Youyun, X. Jing, W. Xinbing, and M. Guizani, "A spatial game for access points placement in cognitive radio networks with multi-type service," in Proc. IEEE Global Telecommun. Conf., 2010, pp. 1–5.

[5]. J. Nagle, "On packet switches with infinite storage," IEEE Transactions on Communications, vol. 35, no. 4, pp. 435 – 438, April 1987.

[6]. C. Y. Wong and R. S. Cheng, "Multiuser OFDM with adaptive subcarrier, bit, and power allocation," IEEE J. Sel. Areas Commun., 1999.

[7]. X. Wang and W. Xiang, "An OFDM-TDMA/SA MAC protocol with QoS constraints for broadband wireless LANs," ACM/Springer Wireless Networks, vol. 12, no. 2, pp. 159 – 170, 2006.

[8]. I. Stojmenovic, "Position-based routing in ad hoc network," IEEE Commun. Mag., vol. 40, no. 7, pp. 128–134, July 2002.

[9]. J. A. Sanchez, P. M. Ruiz, and R. Marin-Perez, "Beaconless geographic routing made practical: challenges, design

guidelines, and protocols," IEEE Commun. Mag., vol. 47, no. 8, pp. 85–91, Aug. 2009.

[10]. J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[11]. C.-L. Wang and S.-J. Syue, "An efficient relay selection protocol in cooperative wireless sensor networks," in Proc. 2009 IEEE Wireless Commun. and Networking Conf., Budapest, Hungary, April 2009.

[12]. Z. Yang and A. Host-Madsen, "Routing and power allocation in asynchronous gaussian multiple-relay channels," EURASIP J. Wireless Commun. Netw., vol. 44, pp. 181–217, Jan. 2006.

[13]. F. Li, K. Wu, and A. Lippman, "Energy-efficient cooperative routing in multi-hop wireless ad hoc networks," in Proc. IEEE International Performance, Computing, and Communications Conference (IPCCC 2006), April 2006, pp. 215–222.

[14]. D. Brennan, "Linear diversity combining techniques," Proc. IEEE, vol. 91, no. 2, pp. 331–356, Feb. 2003.

[15]. T. Aguilar, M. C. Ghedira, S.-J. Syue, V. Gauthier, H. Afifi, and C.- L. Wang, "A cross-layer design based on geographic information for cooperative wireless networks," in Proc. 2010 IEEE Vehic. Tech. Conf. (VTC 2010-Spring), Taipei, Taiwan, May 2010, pp. 1–5.

[16]. A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," IEEE Commun. Lett., vol. 42, no. 10, pp. 74–80, Oct. 2004.

[17]. Y. G. Li, N. Seshadri, and S. Ariyavisitakul, "Channel estimation for OFDM systems with transmitter diversity in mobile wireless channels," IEEE J. Sel. Areas Commun., vol. 17, no. 3, pp. 461–471, Mar. 1999.

[18]. C. Y. Wong and R. S. Cheng, "Multiuser OFDM with adaptive subcarrier, bit, and power allocation," IEEE J. Sel. Areas Commun., vol. 17, no. 10, pp. 1747–1758, Oct. 1999.

