MAC Layer Distributed Jammer Network Using Markovian Model DCF

[1] Dhanasekaran R, [2] Kesavamoorthy A

[1 & 2] *Assistant Professor of Computer Applications*
[1 & 2] *K.S.Rangasamy College of Arts and Science (Autonomous)*
[1 & 2] *Tiruchengode, India.*

Abstract

In wireless sensor networks that use the Distributed Coordinated Function (DCF) of the MAC protocol, a collision may occur when two or more devices transmit simultaneously. When a collision results in failed reception of a packet, the stations involved increase their backoff window which decreases the probability of transmission. A jammer trying to disrupt the communications can take advantage of this behavior to reduce the throughput of the system significantly with little energy expense. In this behavior of the stations is analyzed by deriving the expressions for throughput and jammer's power expenditure as a function of probability of jamming. These results are experimentally verified with the help of a jammer built in the lab. Under the standard DCF, the jammer's power expenditure decreases with an increase in jamming probability beyond a threshold. A simple modification to the standard DCF can make jamming more power expensive for the jammer. A Markovin model detection scheme is proposed to detect the presence of a jammer and its performance characteristics are determined.

Keywords: Medium Access Control, Jammer, Distributed Coordinated Function

1. Introduction

Wireless communications are highly susceptible to interference and hence are vulnerable to jamming attacks. Unlicensed bands are used for a large number of applications including the extremely popular IEEE 802.11-based wireless local area networks. To facilitate an efficient medium access, a number of Medium Access Control protocols are put forward of which Carrier Sense Multiple Access/Collision Avoidance is widely implemented and is included in IEEE 802.11 standards. A trivial method of jamming is to continuously transmit a signal in the operational frequency band. This can be easily demonstrated in the lab by using an inexpensive analog cordless phone that operates in the 2.4GHz band. When the phone is switched ON, it continuously transmits, which forces other devices to wait, as they see a busy channel, and hence the data transfer rate is zero. However, this requires the jammer to spend a lot of energy. By understanding the MAC protocol being used to control channel access, more energy-efficient ways of jamming can be developed.

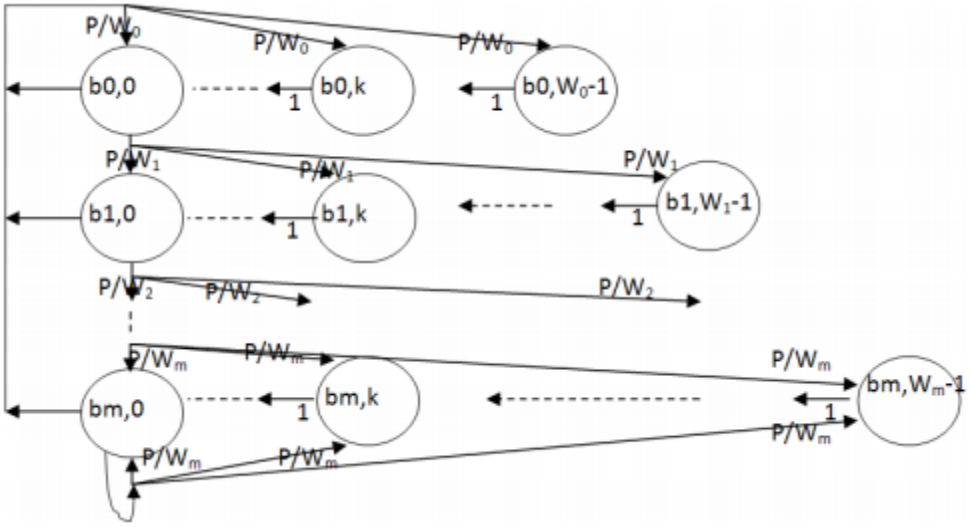

Figure 1: Standard DCF

Classical jamming consists of injecting an interfering signal that corrupts the desired signal at the receiver. Resistance to jamming is traditionally achieved by tuning various parameters such as transmission power, directional antennas and receiver communication bandwidth. By increasing the transmission power level, the signal-to-interference ratio can be increased, but is not a very efficient technique. The most commonly used anti-jamming technique is spread spectrum, in which a signal is spread across a very large frequency band with the help of a spreading sequence, typically a pseudo-random noise.

2. Literature Survey

Author	Method	Advantages
T.X. Brown, J.E. James, and A. Sethi,	Proposed this jamming and sensing technique makes the misuse of AODV and TCP protocols at transport /network layer very efficiently. With the help of this protocols attacker sense the victim packets, but as the whole packet is encrypted attacker can sense only packet size, timing and sequence	As network is encrypted so only packet size and start time can be measured. By doing the selfish use of AODV and TCP protocols attacker achieves advantages like it requires less energy, targeted jamming can be done and reduced probability of detected. Jamming to specific part of network, nodes can be done by attacker.
W. Xu, W.	Proposed failed packet	Authentication can be used to address such

Trappe and Y. Zhang	reception times are used to build the timing channel. Failed packet events can be detected against the jamming. A low-rate overlay link-layer can be (is) constructed using single sender and multi-sender timing channel. There are many strategies that may be applied to halt wireless connectivity. Some network-oriented attacks such as dissociation attacks have been applied against the wireless systems (e.g. 802.11).	powerful threats. Directly interfering with communications by jamming the communication channel is an alternative strategy to mess up wireless communications. To reconstructs network connectivity in the presence of interference, certain defense (or resistive) strategies have been proposed.
P. Tague, M. Li, and R. Poovendran	Availability of service in wireless networks depends on the ability for network users to establish and maintain Communication channels. Jamming the communication channels used to exchange control messages. Spread spectrum techniques used to detect an external adversary from such control channel jamming attacks.	Efficient communication in mobile networks requires the use of multiple access protocols allowing mobile users to share the wireless medium by separating user data in any combination of time, frequency, signal space, and physical space in the network. Allocation of access and resources to mobile users must be periodically updated in order to maintain the efficiency of the multiple access protocol.
The RC6TMBlock Cipher Ronald L. Rivest, M.J.B. Robshaw, R.	Proposed RC6 algorithm is an extension to RC5.RC6 uses an extra multiplication operation which is not present in RC5 in order to make the rotation dependent on every bit in a	RC6 Block Cipher designed to use four 32-bit registers rather than two 64-bit registers. This has one advantage that we are doing two rotations per round rather than the one round in a half-round of RC5.

Sidney, and Y.L. Yin	word, and not just the least significant few bits.	

3. Proposed Methodology

The standard Distributed Coordination Function can be modeled as a Markov chain. As shown in Figure 2, when a packet arrives at a station for transmission, it first needs to sense that the channel is idle for at least a time equal to Distributed Inter-Frame Space, which is typically 50μs. After this, a countdown timer is choosen as a uniform random variable on (0, W0 − 1) and is counted down to zero. W0 is the contention window size of the first backoff state. The backoff counter stops when the station senses a busy channel and resumes after sensing an idle channel for at least a duration of DIFS. The station spends a time equal to aSlotTime, typically 20μs, in each state, bi,k, k 6= 0 until it reaches bi,0. When the backoff counter reaches zero (k = 0), it sends a packet. If the destination receives the packet correctly, it waits for a time equal to Short Inter-Frame Space (SIFS), which is typically 10μs.

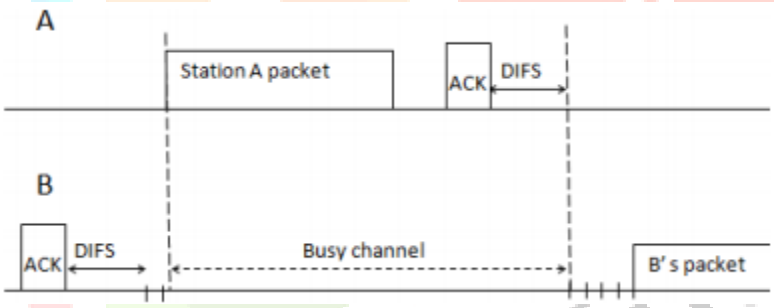

Figure 2: Access Mechanism

A packet is considered a failure when the source station does not receive an acknowledgement (ACK). Should the packet fail, the station increases its contention window size to W1 and chooses a number uniformly between (0, W1 − 1) and repeats the above process by increasing its window size with subsequent failures. When exponential backoff is used, Wi = 2iW0. When a station reaches the last backoff state, it stays in that state until the packet is successful or the maximum allowed number of transmissions is reached, in which case the packet is dropped. When the packet is successful, DCF returns to the zero backoff state.

4. Experimental Results

Throughput

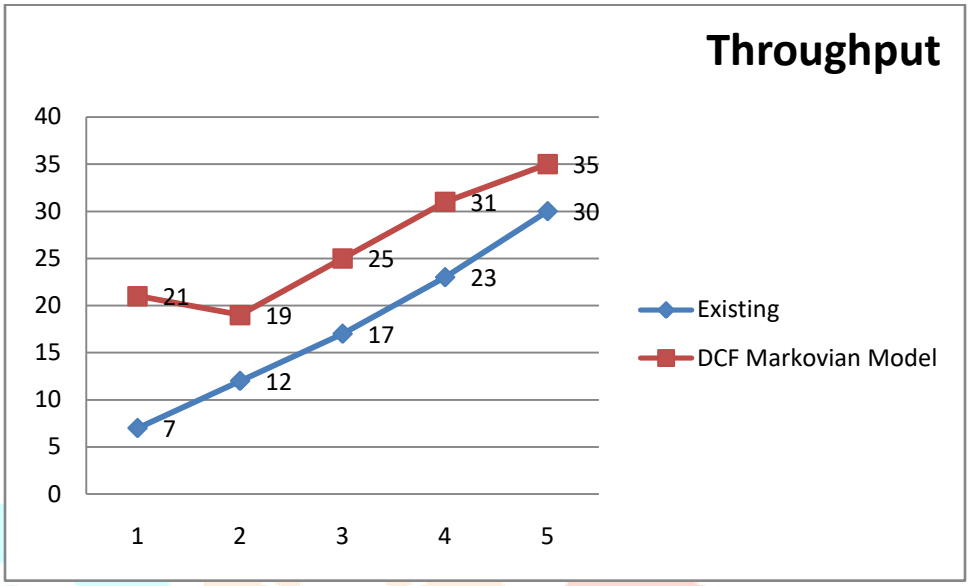

Figure 3: Throughput

Throughput (bits/sec) of a network or device is the total amount of data traffic that was successfully received and forwarded to the higher layer by the WLAN Media Access Control (MAC). It is the rate of successful message delivery of the network communication channel. For example, assume two nodes are transmitting data in a network. If the average data delivery in this network is 100 bits/sec, the throughput of the network is 100 bits/sec.

Load

Load (in bits/sec) of a network or a device is the average rate submitted to the wireless LAN MAC by its higher layers in this node. It is a measure of the amount of data networks or devices are transmitting in the system.

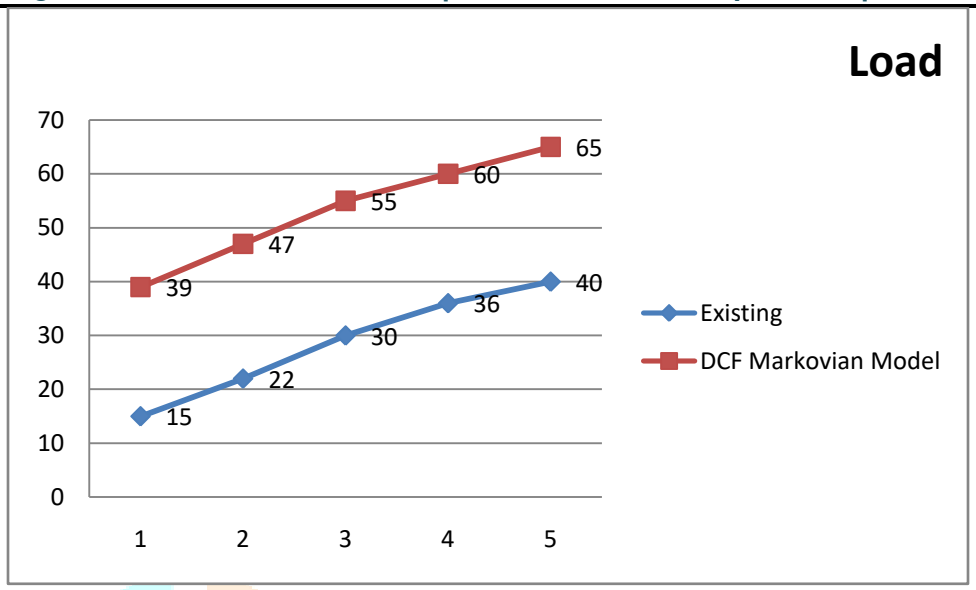

Figure 4: Load

Delay

Delay (sec) represents the end-to-end delay of all the data packets that are successfully received by the WLAN MAC and forwarded to the higher layer. This delay includes the delays at the source, reception of all the individual fragments, and the delay of the frame via access point (AP). In the case of the source and destination, MACs are not AP MACs of the same infrastructure BSS.

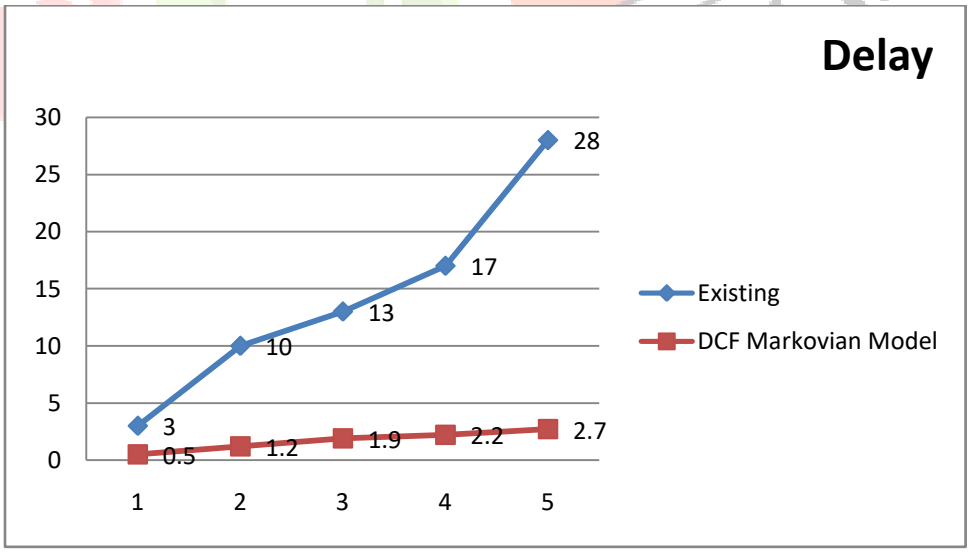

Figure 5: Delay

Data Traffic Sent

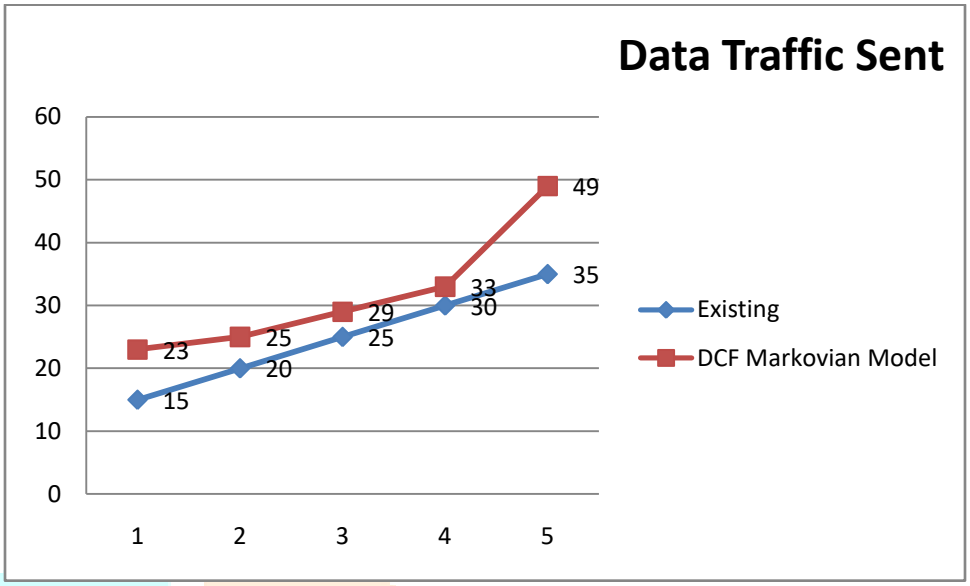

Figure 6: Data Traffic Sent

Data traffic sent (bits/sec) presents WLAN data traffic transmitted by the MAC. Data traffic of a network is the rate of traffic transmitted by all the nodes. The data traffic sent from a node is the rate of data traffic transmitted by this single node.

Data Traffic Received

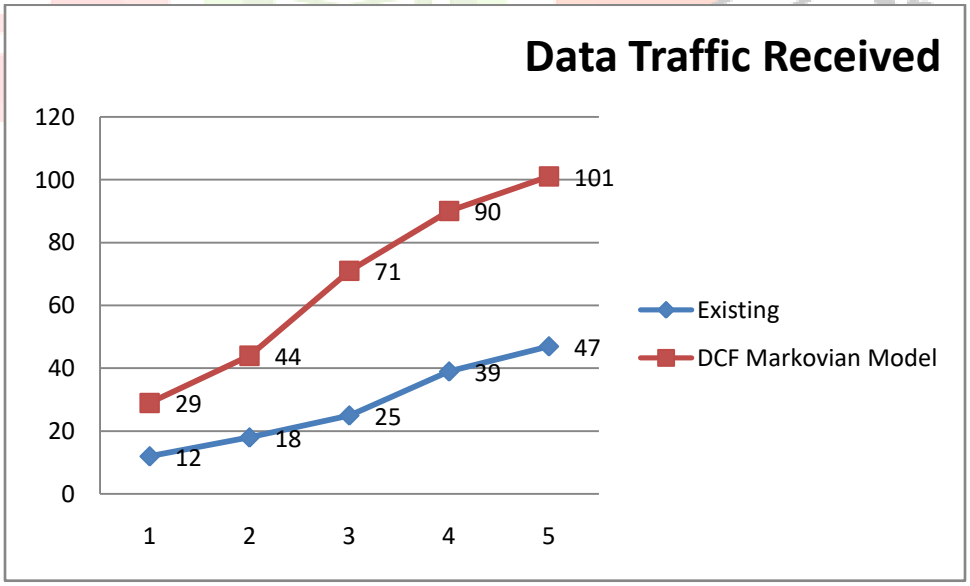

Figure 7: Data Traffic Received

Data traffic received (bits/sec) in WLAN refers to the data traffic successfully received by the MAC from the physical layer. This statistic includes all data traffic received regardless of the destination of the received frames.

Data Dropped

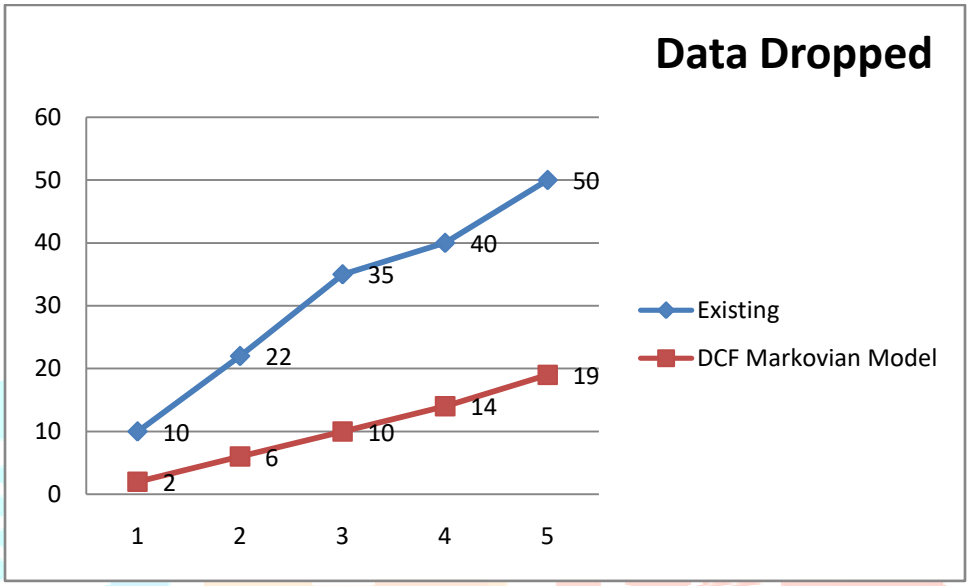

Figure 7: Data Dropped

Data dropped (bits/sec) is the data traffic in higher layer dropped by the WLAN MAC due to consistently failing retransmissions. This statistic reports the number of the higher layer packets that are dropped because the MAC cannot receive any ACKs of those packets or their fragments for the (re)transmissions.

Conclusion

A simple jamming device with limited processing capability, is sufficient to bring the throughput of a network to zero at very little energy expense. The jammer achieves this by pushing the stations to use the largest contention window, which increases the delay between transmissions and reduces the number of packets for the jammer to interfere as explained. proposed a simple modification to DCF that makes the stations transmit more often with an increase in jamming probability. This exhausts a jammer's energy at a faster rate and will be effective with jammers that are energy constrained. This is particularly true with small jamming devices with little batteries that are easy to deploy across network. By burning the batteries of these devices quickly, the network gets restored to its normal operation.

References

[1] T.X. Brown, J.E. James, and A. Sethi,"Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACMInt'l Symp. Mobile Ad Hoc Networking andComputing (MobiHoc), pp. 120-130,2006.

[2] W. Xu, W. Trappe and Y. Zhang, "Anti-Jamming Timing Channels for WirelessNetworks," Proc. ACM Co n f .WirelessNetwork Security (WiSec), pp. 203-213, 2008.

[3] P. Tague, M. Li, and R. Poovendran,"Mitigation of Control Channel Jammingunder Node Capture Attacks," IEEE Trans.Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009.

[4]] The RC6TMBlock Cipher Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge , MA 02139, USA rivest@theory.lcs.mit.edu2 RSA Laboratories, 2955 Campus Drive, Suite 400, San Mateo, CA 94403.

[5] D. J. Theunte and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proceedings of the 25th IEEE Communication Society Military Communications Conference (MILCOM 2006), vol. 7, 2006.

[6] G. Lin and G. Noubir, "On link layer denial of service in data wireless lans," Wireless Communications and Mobile Computing, vol. 5, pp. 273 – 284, 2004.

[7] S. Amuru and R. M. Buehrer, "Optimal jamming in digital communication - impact of modulation," in Proc. Global Commun. Conf., Austin, TX, Dec. 2014.

[8] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 10, pp. 2212-2224, Oct. 2015.

[9] S. Amuru and R. M. Buehrer, "On jamming power allocation against OFDM signals in fading channels," submitted to IEEE Trans. Inf. Forensics and Security, available at www.buehrer.ece.vt.edu/papers/FadingJamming.pdf, 2015.

[10] S. Amuru and R. M. Buehrer, "Optimal jamming using delayed learning", in Proc. Military Commun. Conf., Baltimore, MD, Oct. 2014, pp. 1528-1533.

[11] S. Srinivasa and M. Haenggi, "Modeling Interference in Finite Uniformly Random Networks," in Proc. Intern. Workshop on Inf. Theory Sensor Netw. (WITS), Santa Fe, NM, Jun. 2007, pp. 1-12.

[12] M. Abramowitz and I. A. Stegun, "Handbook of Mathematical Functions with Formulas, Graphs, Mathematical Tables." 9th edn, New York, NY, Dover Publications, 1972.

[13] G. Tauchen and R. Hussey, "Quadrature-based methods for obtaining approximate solutions to nonlinear asset pricing models," Econometrica, vol. 59, no. 2, pp. 371-396, Mar. 1991.

[14] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," Proc. IEEE, vol. 97, no. 2, pp. 205-230, Feb. 2009.

[15] M. Di Renzo and W. Lu, "The equivalent-in-distribution (EiD)-based approach: On the analysis of cellular networks using stochastic geometry," IEEE Commun. Lett., vol. 18, no. 5, pp. 761-764, May 2014.

[16] L. Afify, H. ElSawy, T. Y. Al-Naffouri, and M. S. Alouini, "Error Performance Analysis in Uplink Cellular Networks using a Stochastic Geometric Approach," in Proc. Intern. Conf. Commun. (ICC) Workshops, London, UK, 2015.

[17] M. Di Renzo and P. Guan, "A mathematical framework to the computation of the error probability of downlink MIMO cellular networks by using stochastic geometry," IEEE Trans. Commun., vol. 62, no. 8, pp. 2860-2879, Jul. 2014.

[18] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," IEEE Trans. Commun., vol. 59, no. 11, pp. 3122-3134, Nov. 2011.

Dr.R.Dhanasekaran received his Bachelor of Science degree in Computer Science from Bharathiyar University in the year 2003 and Master degree in Computer Applications from Bharathiyar University in the year 2007. He has received his Ph.D in the field of Computer Networks from Anna University in the year 2017.

Mr.A.Kesavamoorthy received his Master degree in Software Science from Periyar University in the year 2008. He has received his Master Philosophy in the field of Computer Networks from Prist University in the year 2010.