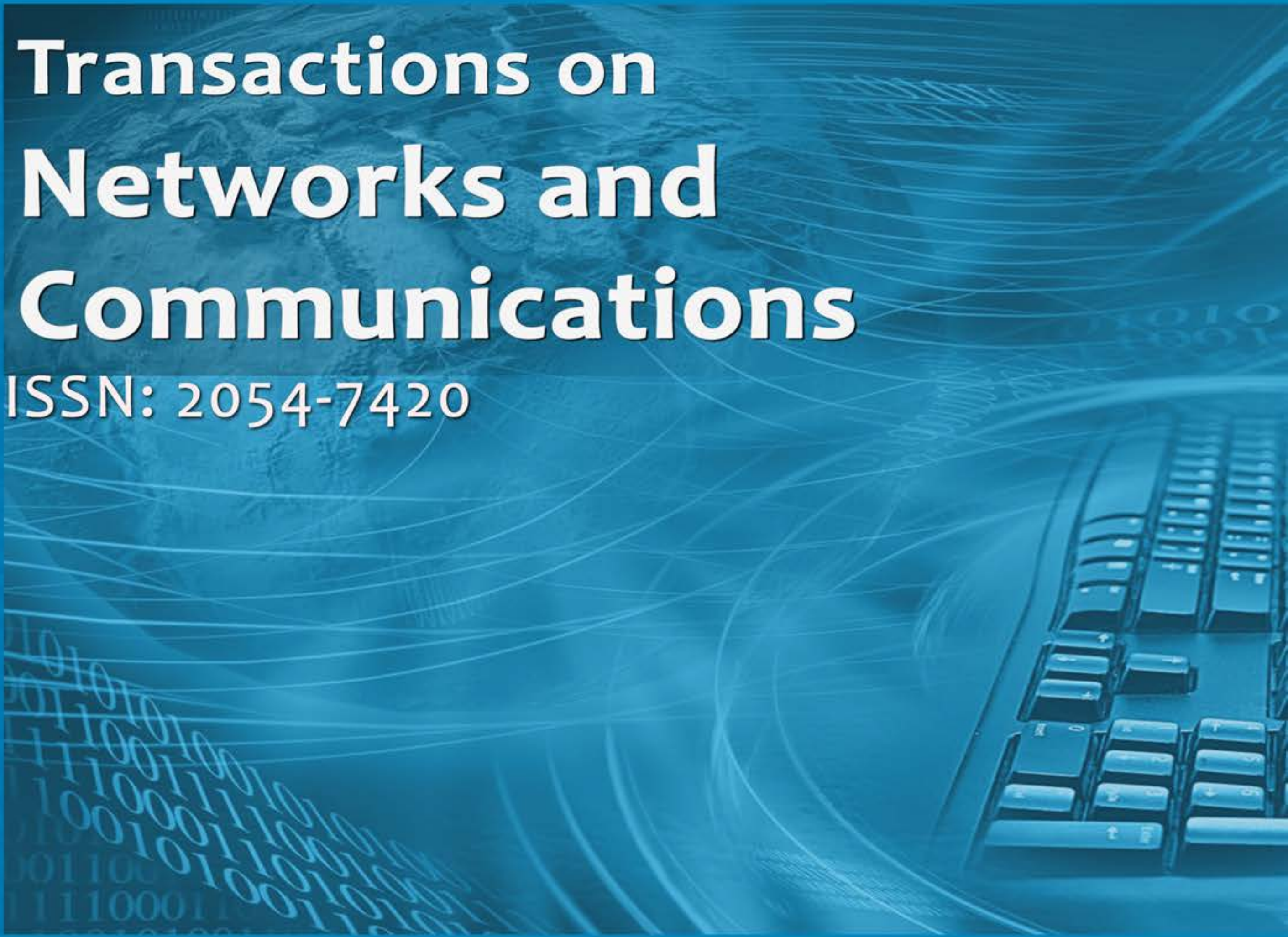
VOLUME 5 NO. 2, APRIL 2017

Transactions on Networks and Communications

ISSN: 2054-7420



Society for Sciences and Education - United Kingdom

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone’s views or feelings etc.

SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 5, NO. 2
ISSN: 2054 -7420

Quantitative Analysis of the Fault-Tolerance of Pragmatic General Multicast (PGM) and Elastic Reliable Multicast (ERM) Protocols

Okonkwo O. Raphael Okonkwo[1], Akpojaro Jackson[2] and Anthony Achuenu[3]
[1]Department of Computer Science, Nnamdi Azikwe University, Awka, Anambra State, Nigeria
[2]Department of Mathematical and Physical Sciences, College of Basic and Applied Sciences, Samuel Adegboyega University, Ogwa, Edo State, Nigeria
[3]Department of Computer Science, Auchi Polytechnic, Auchi, Edo State, Nigeria
jakpojaro@yahoo.com; tonynayou2003@yahoo.com

ABSTRACT

Multicast communication protocols are not immune from failures as a result of packets being dropped due to a broken link or time out processes. Therefore, it is essential to understand how these failures can affect the overall performance of multicast protocols over the Internet. This paper compares the fault-tolerance effect of two reliable multicast protocols: pragmatic general multicast (PGM) and elastic reliable multicast (ERM) in a situation where a multicast-aware node fails and the sub-nodes will have to request a repaired packet. A simulation model is developed in such a way that faults are randomly created on nodes and link for a specified period of time and the fault-tolerance effect on the two multicast protocols is analyzed. The model developed for this paper repeats the simulation for different network size, the results obtained show that the ERM protocol is better than the PGM as the size of the network increases. This finding is key while considering the improvement (or upgrade) of existing multicast protocols. The result is also significant at the early stage of designing new multicast protocols as it provides useful information in allocating scarce resource that can be appropriated to improve other infrastructure in the network.

Keywords: Multicast, pragmatic general multicast, elastic reliable multicast, multicast-aware node, fault-tolerance

1 Introduction

Multicasting has made group communication easier and cheaper. Examples include teleconferencing, video on demand, Internet TV, etc. The quality of multicasting can be enhanced if the fault-tolerance nature of the multicast protocols is studied and characterized such that its effect does not overwhelm and slow down the network. Multicast can be classified into two types, reliable and unreliable multicast. This paper focuses on reliable multicast such as the PGM and ERM, unreliable multicast is studied in another paper. Reliable multicast transport protocol are used by applications that required ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. However, they can also be used in one-to-many group communication.

DOI: 10.14738/tnc.52.2822
Publication Date: 25th March 2017
URL: http://dx.doi.org/10.14738/tnc.52.2822

The advantages of group communication include [1]; less bandwidth is consumed for instance if a real-time feed of data packets from a source to various destinations is instantiated. As the number of destination increases less bandwidth is consumed while the reverse is the case with unicast model. Also, the server load (network load) is greatly reduced in a multicast model since the server has to send a packet once. Since only one packet is sent across the network, cost is greatly reduced compared to unicast model, which sends packets based on the number of receivers.

One of the salient advantages of reliable multicast protocols over traditional multicast protocols is that it guarantees that a receiver in the group either receives all data packets transmitted and retransmitted, or is able to detect unrecoverable data packet loss. Fault-tolerant computer systems are systems designed to be able to continue working to a certain level of satisfaction in the presence of faults. Therefore, the end to end delay and the amount of control bandwidth overhead (CBO) utilized when a fault occurs are studied and evaluated to provide useful information to the network community, particularly multicast designers, network integrators and users.

2 Related Work

The proliferation of group communication applications over the Internet has accelerated a stream of research in this field. Strigel and Manimaran [2] investigated the various issues and solutions for handling group dynamics and node failure in QoS-aware multicast models. In this work, the cost of maintaining dynamic multicast distribution trees with respect to changes in network topology as member join/leave the group was analysed and future research directions suggested.

In [3], the authors described E-Cast as a uniform causal-total-order multicast protocol designed to implement fault tolerant, highly elastic, yet strongly consistent database engines in the cloud. The work provides a rigorous formalization of routing problem, show how partial replication with strong consistency is guaranteed. Mir et al., evaluated the fault tolerance on protocol independent multicast (PIM) and core base tree (CBT) both of which are unreliable multicast protocols [4]. Performance evaluation parameters used included the end-to-end delay, network source usage and the overhead bandwidth cost. Their results showed that PIM performed better than CBT as the network size increases. Read carried out a multicast performance evaluation between PGM and multicast dissemination protocol with congestion control (MDP-CC) under different network conditions and concluded that PGM was superior to MDP-CC [5].

In [6], the authors investigated the technology which provides ubiquitous high bandwidth access for a large number of users in a wireless mesh network. The reliability of such network can significantly be degraded as broadcast traffic which is not solicited for by the participating nodes in the network. The work designed a self-pruning mechanism to control and reduce the broadcast traffic forwarding. The scheme defined two behaviours to manage the broadcasting operation while routing packets are managed differently from data broadcast messages to avoid afflicting the routing process. Simulated results show that the CBF ameliorates the network capacity by reducing considerably the number of redundant packets, thereby improving the end to end delay and providing high reachability and packet delivery.

In [7], the work surveyed multicast routing protocols with interest in ad-hoc networks. A general overview of multicast protocols and their performance was discussed. In particular, the work analysed the Ad-Hoc On-Demand Distance Vector (MAODV) [8], Adaptive Demand- Driven Multicast Routing protocol (ADMR) [9] and Core-Assisted Mesh Protocol (CAMP) [10]. It described how they work and showed reasons for developing these protocols. The work compared these protocols to explain their advantages and limitations.

An efficient approach for fault-tolerant capability for mobile multicast was presented in [11]. In multicast communication, packets can be concurrently sent from a source node to all members by multicast delivery tree. The main goal of the paper is that it makes multicast members immune from failure of nodes affection. The proposal contains two schemes. The first scheme uses the redundant resources of a mobile network to reconnect all the disconnected subtrees. The first scheme does not generate loops. In addition, it can control the maximum delivery delay of the new reconnected multicast delivery tree. The second scheme is initiated when the first scheme cannot reconnect all the subtrees. It extracts the failure-free part of the faulty multicast tree to form a safe multicast subtree. Then, multicast packets are only delivered along the safe multicast subtree to all the members. Unlike the first scheme, the second scheme is not based on the network topology support to achieve fault tolerance. Finally, simulations are performed to compare the proposed approach and previous approaches in terms of the fault-tolerant capability and various performance overheads.

3 Methodology

In this paper the end-to-end delay, the stress level of the source and the cost of control bandwidth overhead (CBO) for maintaining the multicast distribution trees were evaluated. The model is such that the source node floods the multicast routes with a control message and interested nodes indicate interest. A simulator program was designed to simulate the network. Faults were introduced randomly to signify dropped packets and the amount of CBO utilized were obtained for the two different protocols. The total amount of CBO utilized to repair broken distribution subtrees was calculated. The process was repeated for different network sizes.

A video stream from the source to the rendezvous point source (RPS) was sent by the RPS to connected receivers using the PRM and ERM protocols as shown in Figure 1. Faults were generated at random along some receivers (receivers are those with arrows) and the stress level at the RPS was computed based on the number of Negative Acknowledgement (NAK) and repair data that was sent between the RPS and the receivers.

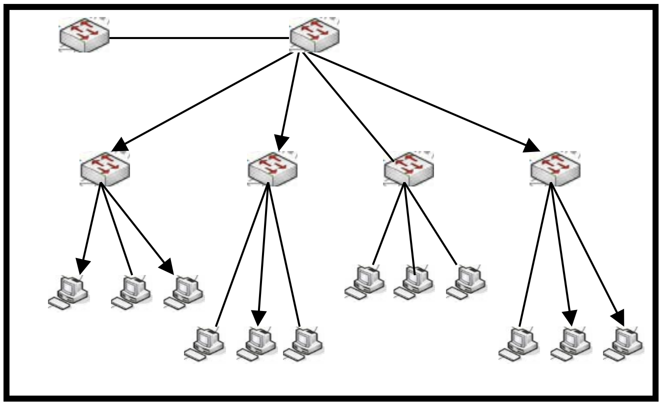


Figure 1: A hierarchical network showing multicast distribution tree

4 Analysis of Results

Following from the above description, the stress level at the RPS for both PGM and ERM protocols were computed and the results presented in Table1. The receivers range was plotted against the stress level as shown in Figure 2. It is clearly shown that the stress level was more in the PGM protocol than in the ERM protocol. This shows that the ERM protocol more efficient than the PGM protocol since less CBO was used as the RPS performed less work in ERM protocol than in PGM protocol.

Table 1: Stress level at the RPS for PGM and ERM protocols

Range of connected leafs	Stress level for PGM	Stress Level for ERM
1-10	46	22
11-20	203	135
21-30	323	274
31-40	495	397
41-50	634	499
Above 50	795	674

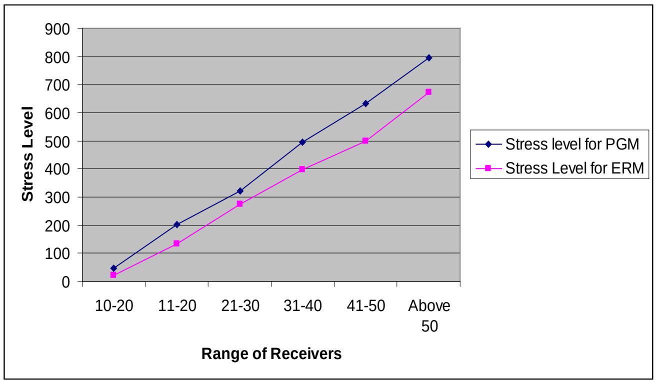


Figure 2: A graph showing the stress level at the RPS for PGM and ERM protocols.

Table 2 measures the cost of bandwidth overhead utilized at all level (source, RPS, studs and receivers' leaf routers). The size of receivers range was plotted against the overall control bandwidth overhead utilized as shown in Figure 3. The results show that the PGM protocol consistently consumed more CBO than the ERM protocol (Table 2). This implies that the distribution tree of the PGM protocol is more expensive to construct and maintain than that of the ERM distribution tree.

Table 2: Comparison of CBO for PGM and ERM protocols

Range of connected leafs	CBO for PGM	CBO for ERM
1-10	44	36
11-20	603	550
21-30	1666	1400
31-40	3249	2774
41-50	5568	4536
Above 50	8610	7370

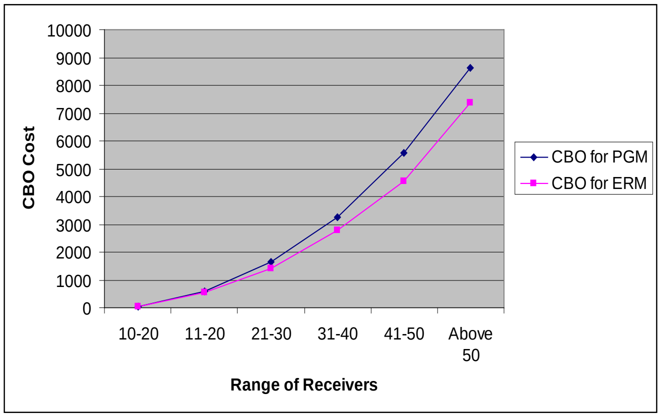


Figure 3: A graph showing the CBO utilized by both PGM and ERM protocols

5 Conclusion

This paper compares the fault-tolerance behaviour between PGM and ERM protocols using CBO utilized to construct and maintain their distribution trees. Findings show that the stress level at the RPS for ERM protocol is less than that of PGM protocol. This implies that the overall CBO for maintaining ERM protocol is less than that of PGM protocol. This means that the ERM protocol is more efficient than the PGM for the different sizes of multicast groups considered. This characterization is very important to the network community, particularly multicast designers, network integrators and users. This information is key while considering the improvement (or upgrade) of existing multicast protocols. The result is also significant at the early stage of designing new multicast protocols as it provides useful information in allocating scarce resource that can be appropriated to improve other infrastructure in the network.

REFERENCES

[1] Kaur, K, and Sachdeva, M., Performance matrices for evaluation of multicast routing. International Conference on Advances in Engineering, Science and Management (ICAESM), 2012, 582-587.

[2] Strigel, A., and Manimaran, G., *Managing Group Dynamics and failures in QOS Multicasting.* IEEE communications, 2002. 40(6): 82-87.

[3] Unterbrunner, P., Alonso, D., and Kossmann, G., E-Cast: Elastic Multicast. Technical Report, 2011. Available at https://www.researchgate.net/publication/275716927.

[4] Mir, N., Musa, S., Torresand, R., and Swamy, S., *Evaluation of PIM and CBT Multicast Protocols on Fault-Tolerance.* International Journal of Computing and Networking Technology, 2014. 2(2): 59-64.

[5] Read, N., *A Multicast performance evaluation between PGM and MDP-CC under varying Network Conditions*, 2006. Available at https://vlebb.leeds.ac.uk/bbcswebdav/orgs/SCH_Computing/FYProj/reports/0506/Read.pdf

[6] Youssef, S., Bouchaib, N., Soufiane, J., and Abdelkrim, H., *Wireless Mesh Networks Capacity Improvement Using CBF.* International Journal of Wireless & Mobile Networks (IJWMN), 2015. 7(3): 1-15.

[7] Baker, R. M., and Akcayol, A. A. 2011. *A Survey of Multicast Routing Protocols in Ad-Hoc Networks.* Gazi University Journal of Science, GU J Sci., 2011. 24(3): 451-462.

[8] Royer, E. R., and Perkins, C. E., *Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol.* In Proc. of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 1999. 207-218.

[9] Jetcheva, J. G., and Johnson, D. B., *Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks.* In Proceeding of the 2nd ACM International Symposium on Mobile and Ad-hoc Networking & Computing, 2001. 33-44.

[10] Garcia-Luna-Aceves, J. J., and E. L. Madruga, E. L., *The Core Assisted Mesh Protocol.* IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, 1999. 17: 1380-1394.

[11] Lin, J., *An Integrated Approach to Efficiently Providing Fault Tolerance for Mobile Multicast*. Journal of Information Science and Engineering, 2005, 21: 153-179

Society for Science and Education
United Kingdom

TNC Transactions on Networks and Communications

Volume 5, No. 2
ISSN: 2054 -7420

Achieving Scalability with Data Owner Anonymity in Cloud Access Control

Abdulqader A. Bahaj, and Ahmed M. Abouollo
King Fahd University of Petroleum & Minerals, Computer Networks, Saudia Arabia
abdulqader.bahaj@gmail.com

ABSTRACT

Cloud computing is a trending technology that enables subscribing organizations to outsource computations and storage, and eliminates the need of purchasing and maintaining the equipment by the organizations themselves. However, it is very challenging to maintain the privacy and security of data especially when the number of users grows dramatically. This paper focuses on achieving a high level of scalability to the cloud, allowing fine-grained access control, preserving the anonymity of the data owner and enabling the end user to verify the integrity of the data uploaded to the cloud. In order to achieve this, this paper proposes an effective scheme that uses Ciphertext Policy Attribute Based Encryption (CP-ABE) combined with identity-based encryption (IBE), and introduces a security mediator which signs files on behalf of the data owner to preserve the data owner's anonymity from the cloud. This scheme allows the end user to check the integrity of the data on the cloud.

1 Introduction

Cloud computing paradigm has been and will continue to be one of the most effective techniques to outsource computation and storage. Despite the great advantage cloud computing provides, it suffers from data security and privacy risks. Since the outsourced data is usually out of the trusted domain servers, counter precautions need to be taken to avoid any external or internal risk such as unauthorized access to data by users who obtain more access than they should be granted, intruders who gain access to the system without being given permission to start with, or even the cloud administrators getting paid to leak user data.

Every user of a system has a set of privileges that might not necessarily be appropriate for others. Well defined access to each piece of data must be managed for each user to ensure privacy and security. A possible technique to target this in cloud computing is to encrypt data and share keys with the privileged users accordingly. This technique becomes a hassle when the number of cloud users booms and when fine-grained data access is needed.

Therefore, it is crucial to find a solution that achieves high level of scalability while maintaining the security of data and the privacy of cloud users.

DOI: 10.14738/tnc.52.2764
Publication Date: 30th March 2017
URL: http://dx.doi.org/10.14738/tnc.52.2764

2 Problem Statement

This paper targets preserving the privacy and anonymity of the data owner in a cloud environment's access control scheme. The scheme must be highly scalable, provides fine-grained access and enables data users to verify the integrity of the data uploaded to the cloud.

3 Background and Terminology

Access control is concerned with regulating who can view, edit and use resources in a computing environment. Most customers require the cloud environment to support fine grained access control, which specifies precisely in a good level of details the characteristics of whoever is granted access, the properties to grant access to, and the level of authority for each user.

Anonymity of data owner in a cloud environment is sometimes crucial. This property can be achieved by introducing a security mediator (SEM), which is a server that is responsible for generating the signature on outsourced data on behalf of the data owner. However, this SEM is not supposed to have visibility to the data that needs to be signed by itself. Therefore, blinding techniques are needed to be introduced. Blinding techniques are meant to allow an agent to provide a service such as signing messages to a client in an encoded form without being able to see the real input or output.

4 Related work

There are many schemes that can be used to encrypt data over a cloud environment. Some of them are more efficient than the others. It should be noted that there are two main points that need to be provided by each scheme to be qualified as a potential scalable choice: Fine-Grained Access and Key Delegation. The following is a presentation of some of the possible access control schemes. It is noteworthy here that none of these schemes provides anonymity of the data owner except the Traditional Symmetric Key cryptosystem, since it uses one shared key between several users.

4.1 Traditional Symmetric Key Cryptosystem Scheme

In the Traditional Symmetric Key scheme pointed out in [3], the sender uses one shared key with all the recipients to encrypt a file and store it in the cloud so that the recipients are able to get the encrypted file from the cloud and decrypt it with the shared key.

This scheme does not qualify to be scalable according to the two points we mentioned earlier. It doesn't provide fine-grained access to the encrypted files as every authorized user has the same shared key, as well as it does not support key delegation.

It is worth mentioning that if the data owner wishes to stop access to a certain file for a certain user who was granted access before, he needs to change the key, re-encrypt the file and re-distribute the key to all other users. As such, the Traditional Symmetric Key Cryptosystem is not an efficient scheme to be used for cloud environments.

4.2 Traditional Public Key Cryptosystem Scheme

In this scheme described in [3], the data owner encrypts the file that is desired to be shared with recipients by using every recipient's pubic key so that every one of them is able to decrypt the file with the recipient's own private key. This approach creates a big problem, which is the need of having a different encrypted copy for every recipient. This is very costly in terms of space and computational power.

Accordingly, this scheme does not qualify to be scalable, as it does not provide fine-grained access to the encrypted files and does not support key delegation.

4.3 Broadcast Encryption Scheme

The broadcast encryption scheme in [1] divides all system users into subsets. The data owner in this scheme assigns keys to the users so that every member of a subset S has the same key as the other members of the same subset. The data owner then encrypts the data and broadcasts it to the intended recipients, and they will be able to decrypt it using their own common keys.

This scheme is not efficient as the data owner needs to maintain and refer back to a database for user authorization in order to specify who can access the broadcast channel. Fine-grained access and key delegation are not supported in this scheme, and thus it does not qualify to be scalable.

4.4 Identity Based Encryption Scheme

Every recipient in the Identity Based Encryption Scheme (IBE) pointed out in [3] is assigned a string (could be the user ID) that works as a public key for that recipient. A trusted third party computes a private key derived from that public key. Introducing this third party and delegating the key management to it makes this scheme more scalable. This scheme no longer requires matching the user to his public key, since the user ID is typically the string used as the public key. Key delegation to a trusted third party is achieved in this scheme, but fine-grained access is still a persistent problem.

4.5 Hierarchical Identity Based Encryption Scheme

To take off the high load from the trusted third party in the Identity Based Scheme which performs a very costly task, an implementation has been proposed in [4] to offer two levels of private key generators (PKG): The first level has one Root PKG and the second level has many Domain PKGs. Every domain PKG computes private keys for its corresponding users after it gets its domain secret key from the root PKG, which owns the master secret. Other implementations took this further and offered arbitrary numbers of levels of PKGs. Having more than one level of PGK enhanced the key delegation of the Identity Based Scheme, but didn’t provide fine-grained access as well.

4.6 Attribute Based Encryption Scheme

Reference [5] points out a relatively advanced scheme called Attribute Based Encryption scheme (ABE). ABE is considered a generalization of the previously mentioned Identity Based Encryption, in which the user ID is the only attribute used. In ABE, the data owner encrypts a file and specifies a set of attributes for that file and a threshold n. Any recipient needs to have at least n attributes from the file’s attribute set to be able to decrypt the file. Other improved implementations support “And” and “OR” logic structures to decrypt the files.

There are two main types of ABE: Key-Policy Attribute-Based Encryption (KP-ABE) where the private key specifies the access structure while the ciphertext is associated with attributes that have to satisfy the access structure in order to enable the user to decrypt the ciphertext, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) where the private key is associated with a subset of the universe of attributes and the access structure is specified in the ciphertext. The user will only be able to decrypt a ciphertext if the attributes associated with his private key satisfy the access structure specified in the ciphertext. ABE provides a good level of fine-grained access to data shared by data owner, but does not support key delegation.

4.7 CP-ABE and IBE Hybrid Scheme

The scheme proposed in [9] provides high level of scalability, user privacy, and effective data sharing in the cloud by combining the CP-ABE with IBE. It enables data owners to assign various access privileges for users to the data as well as carry out dynamic requests to adding and revoking access privileges to them. At the same time, the cloud is unable to read any files shared by data owners and saved on the cloud. This scheme is qualified to be scalable as it provides fine-grained access to the encrypted files and supports key delegation.

In this scheme, the data owner specifies an access structure for each file based on a set of meaningful attributes. This access structure can be expressed by an access tree with attributes at leaves and logic gates such as AND and OR as internal nodes. The data owner also assigns an appropriate set of attributes to every user. If the set of attributes for a certain user match with the access structure of the file, the user is granted access to it. Every attribute is assigned a pair of keys: public and private. The private key of an attribute is used along with a user's public key (i.e. user's ID) to generate a secret key component for that user. Combining all the secret key components for a user makes his secret key. This way, we ensure that all system users have different keys. The secret key of the user is used to decrypt the file stored in the cloud if the user's assigned attributes satisfy the access structure of the file. Public key components of the attributes along with the access structure of a file are used to encrypt data files. Figure 1 describes a simplified workflow of the hybrid scheme starting from the system initialization, when the public and private keys of system users are generated and distributed. After that, files are encrypted by the data owner and uploaded to the cloud server. Then, the data owner generates secret keys and delivers them to the corresponding users. At the end, the user will be able to decrypt the files if his attributes match the files attributes and the access structure.

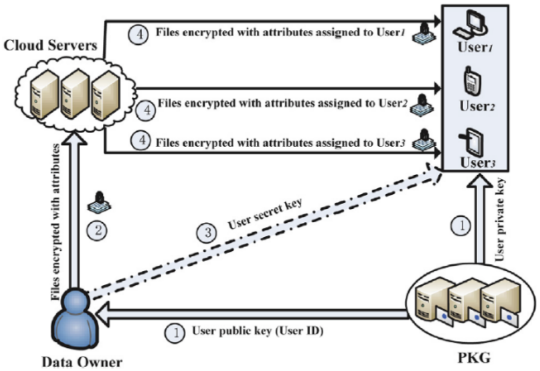

Cloud Servers
4 Files encrypted with attributes assigned to User1
4 Files encrypted with attributes assigned to User2
4 Files encrypted with attributes assigned to User3
User1
User2
User3
Files encrypted with attributes
2
3 User secret key
1 User private key
1 User public key (User ID)
Data Owner
PKG

Figure 1. A simplified Workflow of the Hybrid Scheme.

Table I summarizes the criteria that were considered in comparing the techniques stated earlier, including: Fine-grained access, key delegation and anonymity.

Table 1: Comparison between Schemes

Scheme	Fine-Grained Access	Key Delegation	Anonymity
Traditional Symmetric Key cryptosystem	Not Satisfied	Not Satisfied	Satisfied
Traditional Public Key cryptosystem	Not Satisfied	Not Satisfied	Not Satisfied
Broadcast Encryption	Not Satisfied	Not Satisfied	Not Satisfied
Identity Based Encryption	Not Satisfied	Satisfied	Not Satisfied
Hierarchical Identity Based Encryption	Not Satisfied	Satisfied	Not Satisfied
Attribute Based Encryption	Satisfied	Not Satisfied	Not Satisfied
CP-ABE and IBE Hybrid Scheme	Satisfied	Satisfied	Not Satisfied

5 Proposed Solution

The CP-ABE and IBE Hybrid Scheme is considered the most scalable schemes among the previously mention schemes. However, this scheme does not provide data owner anonymity as the identity of data owner is revealed to the cloud during authentication. For example, a hospital patient might be willing to share his health records with his doctor, but doesn't want the cloud to be able to identify that these records belong to this certain patient.

The model presented in [2] introduces a new party to the scene, which is the Security Mediator (SEM). The role of the SEM is to make sure that the data owner is authenticated to the cloud without revealing his identity. This is achieved by delegating signing the file to the SEM instead of the data owner. The SEM can be any typical server from the same organization as the data owner. This model protects the files which the data owner needs to upload, and hides them from the SEM using blinding techniques to enable the SEM to sign the files without knowing their contents.

As shown in Figure 2, the data owner obtains signature on a file he needs to upload to the cloud with the help of the SEM. This is accomplished by first dividing the file into smaller blocks, applying a blinding technique to these blocks, and sending them to the SEM. The SEM in turn signs the blinded blocks using its private key, then sends back the signed blind blocks to the data owner. Upon receiving the singed blocks, the data owner un-blinds them to get the SEM signature on the original block, then the data owner uploads the file singed by the SEM to the cloud server. The cloud server will accept the signature of the SEM since it is part of the same organization. The data user can check the integrity of the uploaded files by sending a challenge that consists of the ID's of the data blocks the data user want to verify along with random numbers to the cloud, and the cloud calculates a response based on this challenge. Based on this response, the data user will be able to determine the integrity of the data blocks.

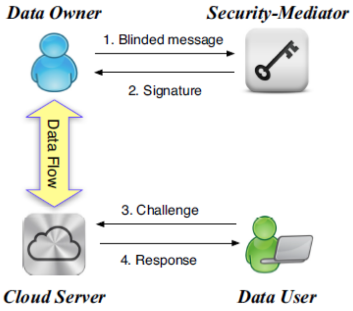


Figure 2. The Security Mediator Model.

Incorporating the highly secure CP-ABE and IBE Hybrid Scheme proposed in [9] with the SEM, we come up with a solution that combines the scalability of the former scheme with the data owner anonymity of the latter model. As shown in Figure 3, the proposed solution is achieved by the following five algorithms:

5.1 Public and private keys generation and distribution

Every data user is assigned a private key and a corresponding public key by a trusted third party called Private Key Generator (PKG). The PKG shares the private key securely with the data user to be able to decrypt the encrypted secret key that will be sent to her by the data owner. The PKG also shares the public key of the same data user with the data owner to be able to use it with the attributes' private keys to create the secret key, encrypt it and send it to the data user.

5.2 Secret key generation and distribution

Every user is assigned a set of attributes by the data owner that need to satisfy the attributes and access structure associated with a file in order to be able to decrypt this file. Every attribute is assigned a pair of keys by the data owner: public and private. The data owner uses the private key of attributes along with the user's public key to generate secret key components for that user. These components combined consist the secret key of the user. Combining the private keys of the attributes with the public key of the user ensures that no users will ever have the same shared key even if they have the same attributes. The data owner encrypts the secret key of the data user with the data user's public key before sending the secret key to her.

5.3 File encryption

The data owner encrypts the file using the public key components of the file attributes along with the access structure of a file as described earlier in the CP-ABE and IBE Hybrid Scheme.

5.4 File signing and uploading

The data owner divides the ciphertext into blocks. Then the data owner applies a blinding technique to the blocks of the ciphertext obtained during the file encryption phase, and send it to the SEM. Applying the blinding technique to the ciphertext prevents the SEM from learning about the content of the data blocks even if the SEM gets hold of any of the authorized users' secret keys. SEM signs the received blocks of ciphertext with its private key, and sends them back to the data owner. The data owner un-blinds the signed blinded block of ciphertext and obtains the original block of ciphertext with the signature of SEM, then uploads them to the cloud. The cloud verifies that the received signature belongs to the SEM. As a result, the cloud will be able to tell that the user came from a certain organization, but will not be able to identify the data user.

5.5 Checking integrity

To check the integrity of the files uploaded to the cloud, the data user sends a challenge to the cloud specifying the blocks the data user wants to verify along with random numbers. These inputs enable the cloud server to calculate a valid response to the challenge if the file has not been changed. The data user compares the response from the cloud with the values the data user calculates locally based on the random numbers chosen. If the calculated values match at both ends, the data user considers the files to be unmodified.

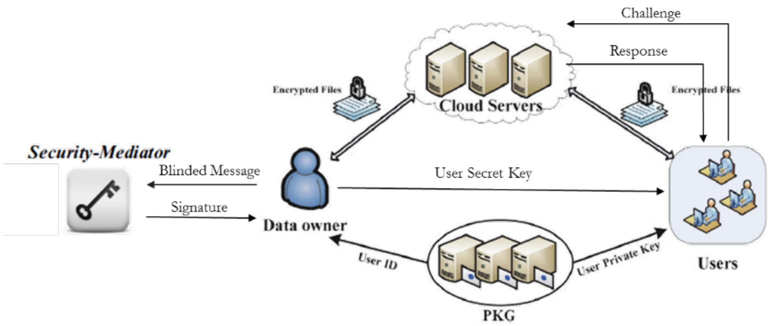


Figure 3. The Proposed Scheme.

6 Advantages of the proposed scheme

The proposed scheme provides a high level of scalability since it supports delegation of key generation and distribution as well as it provides fine-grained access to the data on the cloud. This scheme also preserves the anonymity of the data owner from the cloud server since the cloud is only able to verify that the user belongs to certain organization that is subscribed to the service, but cannot find out the identity of this specific data owner.

The SEM is unable to learn any content from the data it needs to sign after using blinding techniques, which minimizes the requirement of trust on the SEM. The data user can always verify the integrity of the data blocks it needs to verify to be unchanged. This scheme provides less overhead for integrity checking as it enables the data user to choose random blocks of data to verify instead of the entire files, and achieves a very high probability of confidence of the results.

7 Conclusion and Future Work

Many access control schemes have been proposed for managing cloud servers. This paper discussed one of the most secure and scalable schemes which achieves fine grained access control along with key delegation. Since this highly scalable technique does not preserve the data owner anonymity, it is beneficial to integrate this scheme with a model that hides the identity of the data owner by introducing a third party that signs the files on behalf of the data owner. By doing this, the scheme proposed in this paper combines the scalability of the access scheme along with data owner anonymity. It also enables the data user to efficiently verify the integrity of the data uploaded to the cloud.

This paper proposes a new problem for researchers to work on, which is the ability of the scheme not only to support the anonymity of the data owner from the cloud server, but also from the end user. This would be a great future move especially for researchers. For instance, a patient might allow a medical researcher to view her records stored on the cloud, but does not want to reveal her real identity to the researcher.

REFERENCES

[1] Amos Fiat and Moni Naor. Broadcast encryption. In *Advances in Cryptology CRYPTO93*, pages 480–491. Springer, 1994.

[2] Boyang Wang, Sherman SM Chow, Ming Li, and Hui Li. Storing shared data on the cloud via security-mediator. In *Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on*, pages 124–133. IEEE, 2013.

[3] GuojunWang, Qin Liu, and JieWu. Achieving fine-grained access control for secure data sharing on cloud servers. *Concurrency and Computation: Practice and Experience*, 23(12):1443–1464, 2011.

[4] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-based encryption. In *Advances in Cryptology EUROCRYPT 2002*, pages 466–481. Springer, 2002.

[5] Jin-Shu Su, Dan Cao, Xiao-Feng Wang, Yi-Pin Sun, and Qiao-Lin Hu. Attribute based encryption schemes. *Journal of Software*, 22(6):1299–1315, 2011.

[6] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *Parallel and Distributed Systems, IEEE Transactions on*, 24(1):131–143, 2013.

[7] Santanu Chatterjee, Amit Kumar Gupta, and GV Sudhakar. An efficient dynamic fine grained access control scheme for secure data access in cloud networks. In *Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on*, pages 1–8. IEEE, 2015.

[8] Song Lingwei, Yu Fang, Zhang Ru, and Niu Xinxin. Method of secure, scalable, and fine-grained data access control with efficient revocation in untrusted cloud. *The Journal of China Universities of Posts and Telecommunications*, 22(2):38–43, 2015.

[9] Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, and Minglu Li. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. *Computers & security*, 42:151–164, 2014.

SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 5, NO. 2
ISSN: 2054 -7420

A 1-5Ghz, Hybrid Mic Wideband LNA utilizing Microstrip Geometric Structure Variety for Performance Improvement

[1]Pramod K B Rangaiah, [2]Kumaraswamy H V
[1]PhD Student of JAIN University, Bangalore, India;
[1]Assistant Professor at EXTC Dept., MCT's RGIT, Mumbai, India;
[2]Dean CAT, Dept. of Telecommunication, RVCE, Bangalore, India;
pramod63putta@gmail.com; pramod.kb@mctrgit.ac.in; kumaraswamyhv@rvce.edu.in

ABSTRACT

A wideband LNA is design and developed utilizing Hybrid Microwave Integrated Circuit (HMIC) technology for the 1-5GHz bandwidth employing the microstrip line geometric variation. For the performance enhancements in the LNA as for Gain, Noise figure and return loss attributes novel procedures are utilized. The circuit is designed using both lumped elements and distributed components and simulated in AWR microwave office.

The LNA design include optimum biasing circuit and microstrip geometric varieties with two distinct renditioned versions. The first version as the geometric structure with radial stubs and second one as linear stubs and whose basic changes were given in the simulation measurements. This paper likewise gives the reasonable strides in insights with respect to hardware implementations. The proposed design especially helpful in the communication systems working under IEEE L and S bands applications. To be more particular it is having more prominent degree application in the radars and defense receiver systems.

Keywords: LNA, Microwave, Microstrip Lines, biasing Circuit and HMIC.

1 Introduction

Expanding interest to associate more devices wirelessly with higher data rates pushes the industry to adjust new models and send new frequency groups [1]. For the most part all the advanced electronic gadgets, for example, mobiles, portable PCs conceive wireless applications and wireless standards. Each wireless application needs its own front end [2, 3]. A wideband receiver design ought to have the capacity to get an extensive variety of frequency guidelines. This imperative is popular in light of the fact that it grants to diminish the chip region, spare expenses and decrease the RF front-end multifaceted nature [4,9].

Significant requirements on a wideband LNA are to give wideband input matching, high gain with flatness, low NF and adequately high linearity over a vast band of frequencies while keeping power utilization low. The linearity decides how much tolerant is the LNA towards possible solid meddling blockers in the range [11-13].

DOI: 10.14738/tnc.52.3039
Publication Date: 27th Apr 2017
URL: http://dx.doi.org/10.14738/tnc.52.3039

2 Collected Research Background

This segment portrays the work in late related s which gives the reasonable support to comprehend what is required to be done to achieve the objectives. D. Bierbuesse,. et.al [5], composed the wideband LNA utilizing all the noise cancellation and a linearization method is exhibited. The outlined LNA comprises of a cross-coupled common-gate topology for wideband matching and noise cancellation. The LNA is planned in a 130 nm CMOS innovation. It has a simulated gain of 14 dB in the frequency run from 100 MHz to 4.7 GHz. The NF is between 3 dB and 4 dB over this frequency band. H. Cruz, et.al [6], presents a wide band LNA for the IEEE 802.11 WLAN. The LNA utilizes two input ways to improve linearity and in-band gain increased. The - 3dB BW is 4 GHz with focus recurrence of 4.7 GHz. The current reuse strategy is used to lessen the power utilization and the NF. Post-Layout design comes about show that the achievable IIP3 is - 2 dBm, and the NF breaks even with 3.07 dB. Peigen Zhou,et.al [7] displayed the outline and usage of a scaled down ultra-wideband LNA reasonable for RF framework. The LNA depends on negative feedback topology and lessens the measure of the circuit enormously. By utilizing a 4.7 Ω resistance in arrangement with the deplete of every transistor, the design output excellent stability at a wideband frequency. The LNA is created on a Rogers RO4003C board with size of 91.5mm*25mm. Over the wide working recurrence band of 2-10GHz, the deliberate outcomes show an astounding execution with the gain of higher than 34dB, in-band evenness of under 3.37dB, S11 of not as much as - 10.95dB, S22 of not as much as - 11.04dB, a low NF of under 3.49dB and a low power utilization. X. Zhang et.al, [8] the proposed LNA indicates enhanced execution parameters including Gain, NF, 1dB P1dB, and information alluded IIP3, especially for wideband LNA outline. The LNA is manufactured in TSMC 0.13-gm prepare. From 0.3 to 6GHz, demonstrate a high-Gain of 20 dB, a predominant NF of 1.6dB at 3GHz, input control at P1dB of - 19.2dBm at 2GHz.

3 The Proposed LNA Design

3.1 The Proposed design flow

This design flow will explore the design parameters space of integrated inductively-low noise amplifiers (LNA), under the constraint of matched input impedance, is presented. It is based on AWR microwave simulation tool and can be easily automated. The approach of the design is shown clearly with details in the flow diagram figure 1 will explore the design parameter space of integrated low noise amplifiers (LNA), under the constraint of matched input impedance.

3.2 The Proposed LNA Design

The design of microwave wideband low noise amplifier operating from 1-5GHz uses Enhancement Mode Psuedomorphic HEMT "ATF54143" 4V and 80mA from Avago Technologies. Lumped elements are used to implement the matching networks. The 2-stage configuration provides required gain. Input and output matching networks are designed to produce 50Ω impedance for maximum power transfer. The achieved specifications are variable gain 17 dB to 30dB, noise figure (NF) of <2dB throughout the band 1 -5GHz, with very good return loss and unconditionally stable condition.

The above figure 2 is the entire schematic diagram of the proposed design of the wideband LNA. It has obviously indicated schematic comprises of the sub block which is having name (net) from left side to be specific "Input Matching Stubs”, “Total Ckt”, MLIN, Capacitor and MTRACE2, “Total Ckt” and “Output

Matching Stubs". Every last square will be examined obviously one by one with schematic and designs. The reason, limit and capacity of every sub-square will be examined and analyzed in detail advance.

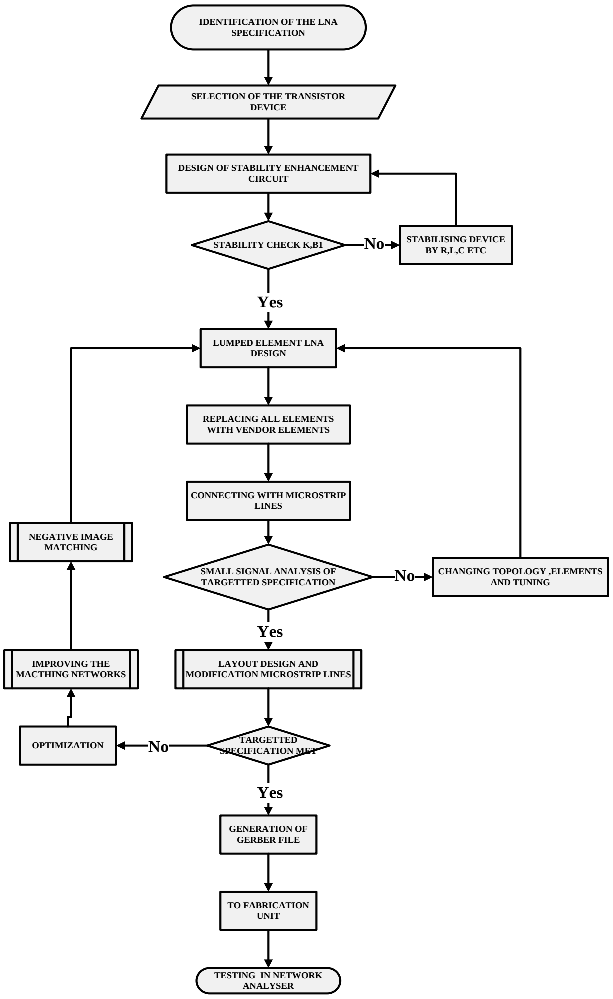

IDENTIFICATION OF THE LNA SPECIFICATION
SELECTION OF THE TRANSISTOR DEVICE
DESIGN OF STABILITY ENHANCEMENT CIRCUIT
STABILITY CHECK K,B1
No
STABILISING DEVICE BY R,L,C ETC
Yes
LUMPED ELEMENT LNA DESIGN
REPLACING ALL ELEMENTS WITH VENDOR ELEMENTS
CONNECTING WITH MICROSTRIP LINES
NEGATIVE IMAGE MATCHING
SMALL SIGNAL ANALYSIS OF TARGETTED SPECIFICATION
No
CHANGING TOPOLOGY ,ELEMENTS AND TUNING
Yes
IMPROVING THE MACTHING NETWORKS
LAYOUT DESIGN AND MODIFICATION MICROSTRIP LINES
OPTIMIZATION
No
TARGETTED SPECIFICATION MET
Yes
GENERATION OF GERBER FILE
TO FABRICATION UNIT
TESTING IN NETWORK ANALYSER

Figure 1 Shows complete work and methodology followed in design of the LNA.

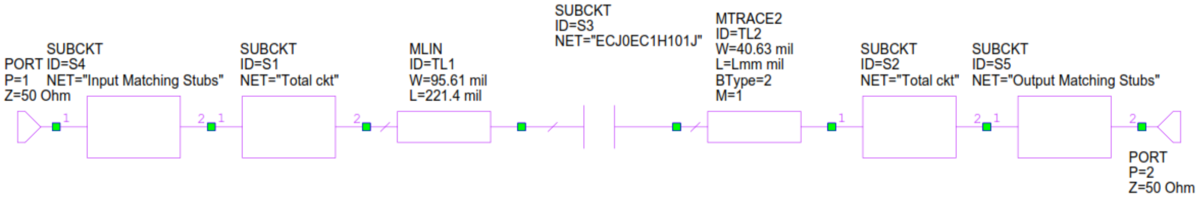


Figure 2 The proposed LNA design Schematic in block form

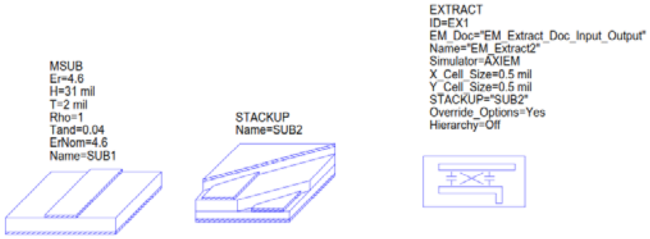


Figure 3 Shows the substrate MODEL, STACKUP AND EXTRACT used in the design

In the figure 3 the square called "MSUB" is utilized to characterize the miniaturized micro strip line in the general circuit design. Er is the permittivity of the substrate material with respect to the permittivity of free space ω0 = 8.85e-12 F/M2, ErNom speaks to the ostensible dielectric steady of the substrate in respect to free space and is utilized just by X-Models where all EM information is gathered at Er_Nom and a variationally approach is utilized to assess the execution for little varieties in Er about Er_Nom or in general nominal dielectric constant. Tand is the dielectric loss digression of the substrate material: Tand = εr″/εr′ where εr = εr′ -jεr″, Rho is the mass resistivity of channel metal standardized to gold (that is, to 2.44 x 10 - 8ω*m). So, real metal mass resistivity = 2.44 x 10 - 8Ω*Rho*m. H and T are cross sectional dimensional factors given in default length units.

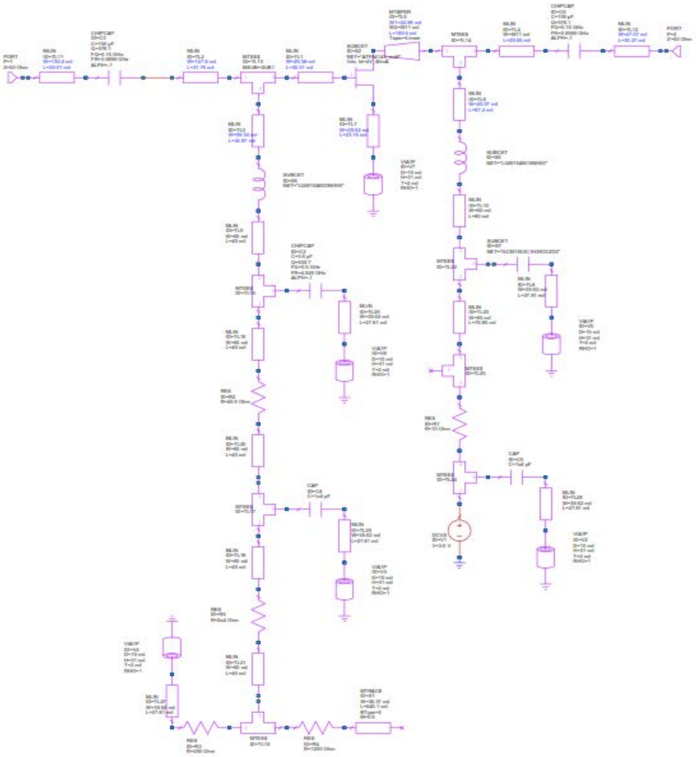


Figure 4 Shows the Sub Block "Total Ckt" of the complete schematic in detail

The sub square "STACKUP" is the Element Options-(Schematic) STACKUP Properties discourse box Material definition which permits to add new materials to structures, determine their properties, and alter and erase these layers. The Conductor and Impedance Definitions characterize the electrical properties of a conduit. For Conductor Definitions, which indicate the conductivity and after that the thickness is determined to the Materials tab. For Impedance Definitions, the thickness is as of now represented in the qualities entered (ohms/sqr). There are two strategies, as now and again you know your material conductivity (gold, copper, and so forth) and now and then it is known dielectric material's impedance (thin film resistors, and so on) [14-16]. The accompanying names are held and can't be utilized: Air, Perfect Conductor, Approx Open, and Input waveguide. It can't include things with these names.

In the figure 3 the sub piece called EXTRACT square is a simulation control that permits a gathering of related schematic components to be electrically displayed by means of a physical reproduction (EM simulation, parasitic extraction, and so forth.) of the format of these segments. After reproducing, the design cells of the majority of the related segments are ported to an EM sight and simulation. After this reproduction is finished the electrical results are naturally converged once more into the schematic and simulation of the whole schematic is performed.

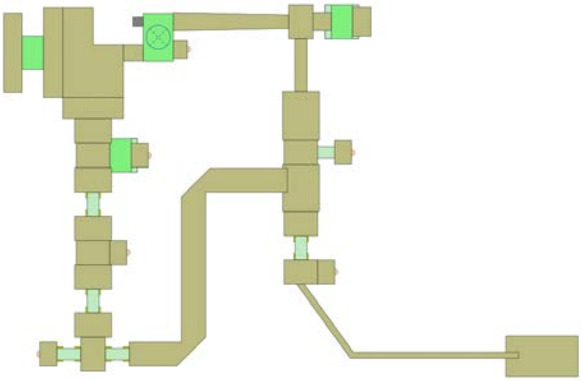


Figure 5 The 2D layout of the sub block "Total Ckt"

The above figure 5 is the sub block of the main circuit schematic figure 2. In order to make cascaded LNA is it good practices by the designer to make first single stage LNA circuit and then followed by that same circuit will be duplicated and connected in series side by side. The cascaded 2 stage amplifier will be done by using 2 "Total Ckt" with intermediate matching by using capacitor "ID S3", "MLIN" and "MTRACE2" which is shown in figure 2. LNA parameters are mainly depend on S parameters which varies with respect to frequency. Also Γin depends on Zin and ΓL, ΓL depends on ZL and ΓIN . Zin and ZL will be different for different biasing components. Effects of biasing components is also frequency dependent

The above figure 5 which is the layout formed for the single stage LNA "Total Ckt". The layout id formed by taking foot prints of each components from the vendors and it is connected by using the micro strip lines. After that high impedance line with patch for soldering the biasing input.

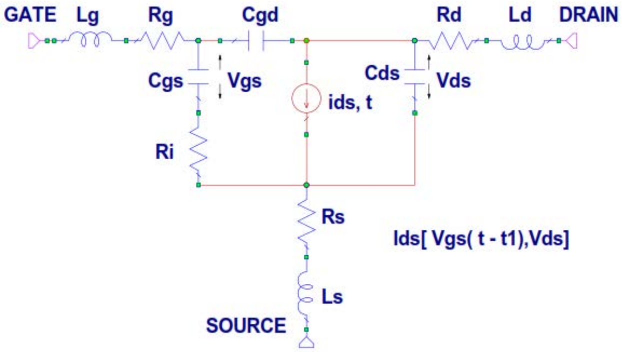


Figure 6 The small signal model of a pHEMT

Cgs and Cgd depends on the biasing voltage because the depletion region changes with the bias.

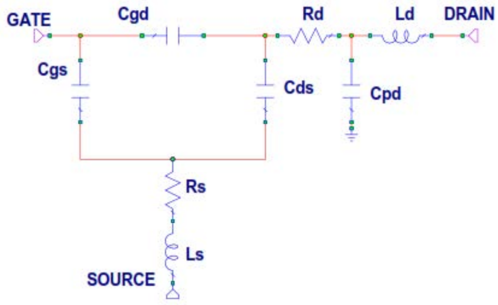


Figure 7 The small signal model of a pHEMT at zero drain bias and gate voltage below pinch-off

The three capacitances Cg, Cs and Cd are given by triangle-star transformation as given below

$$C_g = C_{gs} + C_{gd} + [(C_{gs}* C_{gd})/ C_{ds}] \quad (1)$$

$$C_s = C_{gs} + C_{ds} + [(C_{gs}* C_{ds})/ C_{gd}] \quad (2)$$

$$C_d = C_{ds} + C_{gd} + [(C_{gd}* C_{ds})/ C_{gs}] \quad (3)$$

Input port and output port impedances can be expressed using

$Z_{11} = R_g +R_s + j * [\omega(L_g + L_s) – (1/ \omega) \{ (1/C_g)+ (1/C_s)\}]$ (4)

$Z_{22} = R_d +R_s + j * [\omega(L_d + L_s) – (1/ \omega) \{ (1/C_d)+ (1/C_s)\}]$ (5)

Input reflection coefficient and output reflection coefficient

$$\Gamma_{in} = (Z_{in} – Z_0)/(Z_{in} + Z_0) \quad (6)$$

$$\Gamma_L = (Z_L – Z_0)/(Z_L + Z_0) \quad (7)$$

Equivalent input and output impedances can be expressed in terms of two port Z parameters.

$$Z_{in} = Z_{11} – [(Z_{12}* Z_{21})/(Z_L + Z_{22})] \quad (8)$$

$$Z_L = Z_{22} – [(Z_{12}* Z_{21})/(Z_G + Z_{11})] \quad (9)$$

On the premise of the above arrangement numerical conditions unmistakably reliance of Γin and ΓL furthermore Zin and ZL on Cg, Cs and Cd which changes because of progress in biasing conditions. For the effective outcome, even after fabrication implementations this proposed configuration will be conveyed into two unique forms of the micro strip lines structure.

4 Microstrip Variant Design versions

4.1 Version

This version is done by using negative image matching techniques for the same circuit which is show figure 8. The input matching stubs is prepared for optimizing the input return loss and corresponding gain flatness. The schematic is shown in figure 6.7 and corresponding layout in figure 6.8.

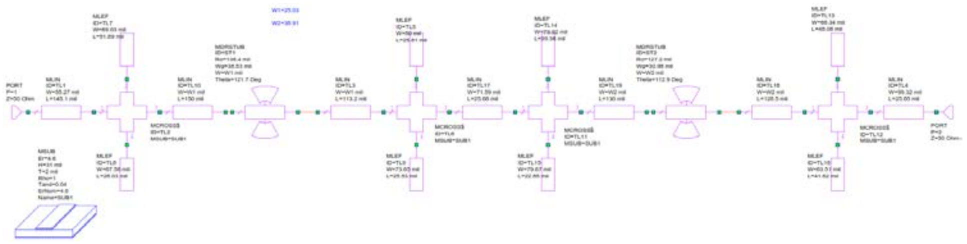


Figure 8 Shows the schematic of the sub block “Input Matching Stubs” of the version 1

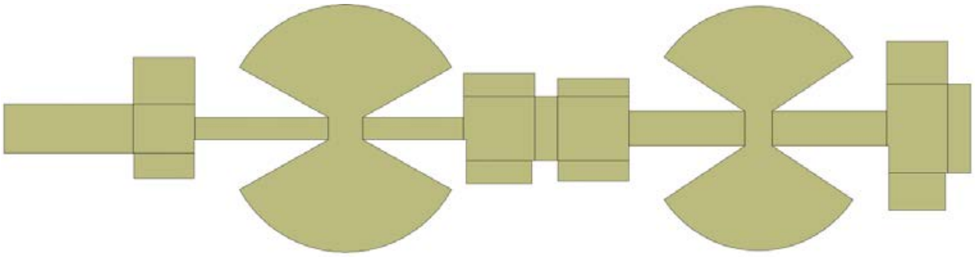


Figure 9 Shows the layout of the sub block “Input Matching Stubs” of the version 1

It is clearly visible that the circuit is prepared by using the micro strip lines structures like “MLIN”, “MCROSS”, “MLEF” and “MDRSTUB” which means in turn it is linear line, four port junctions, open stub line and radial stubs.

4.1.1 Output Matching Stubs

In this version, output micro strip matching is done by using negative image matching techniques for the same circuit which is shown in figure 2. The input matching stubs is prepared for optimizing the input return loss and corresponding gain flatness. The schematic is shown in figure 10 and corresponding layout in figure 11.

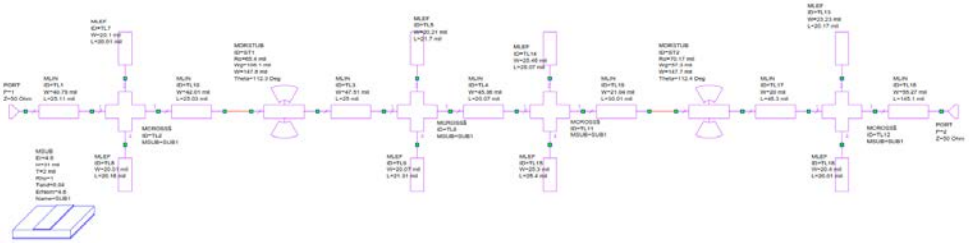


Figure 10 Shows the schematic of the sub block “Output Matching Stubs” of the version 1

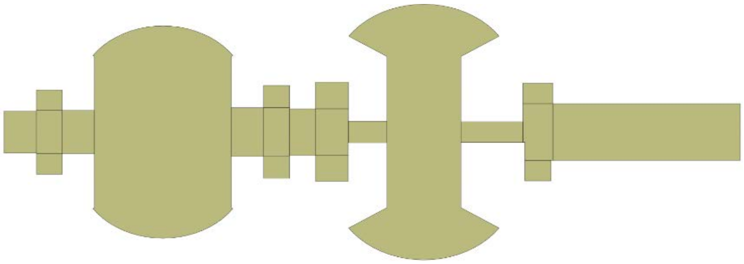


Figure 11 Shows the layout of the sub block “Output Matching Stubs” of the version 1

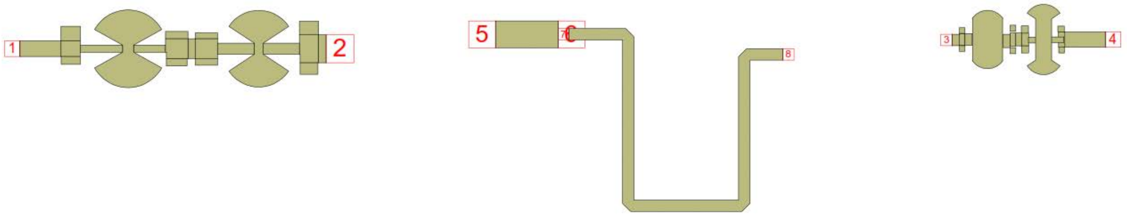


Figure 12 EM Structure circuit for the version 1 circuit

Electromagnetic (EM) test systems is done utilize Maxwell's conditions to process the reaction of a structure from its physical geometry the micro strip line with substrate data and stack up. EM simulation are perfect since they can re-enact exceedingly self-assertive structures and still give extremely exact outcomes. Furthermore, EM test systems are not subject to a large portion of the limitations of circuit models since they utilize key conditions to figure the reaction. One confinement of EM test systems is that reproduction time develops exponentially with the extent of the issue, hence it is critical to minimize issue unpredictability to accomplish opportune outcomes.

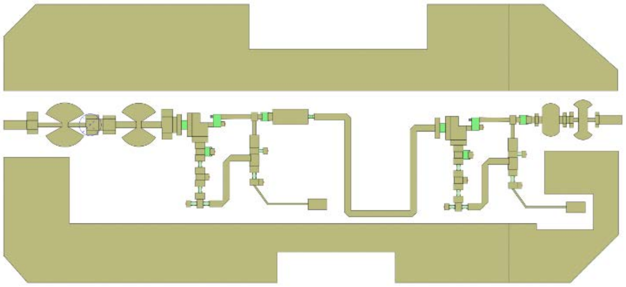


Figure 13 Shows the 2D layout of the complete proposed LNA design version 1

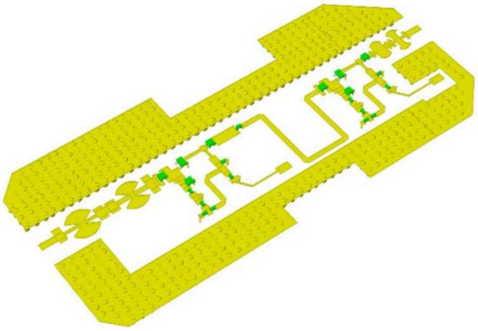


Figure 14 Shows the 3D layout of the complete proposed LNA design version 1

This above figure 13 shows the complete 2D layout and figure 14 shows 3D layout. This is the layout of version 1 changes in input matching stubs and output matching stubs for the complete circuit which has displayed in figure 2. To avoid the parasitic fringing effects the metal outer shape has been provided and series vias are provided to remove or unnecessary charges will be grounded immediately.

4.1.2 Results

The AWRDE features extensive post-processing capabilities, allowing the display of computed data known as "Measurements" on rectangular graphs, polar grids, Smith Charts, histograms, constellation graphs, tabular graphs, Antenna plots and 3D graphs. There exist an extensive number of the potential electrical and mechanical measurements that are pertinent for the microwave LNA. In any case, there are number of the particulars however all around acknowledged estimations are talked about further.

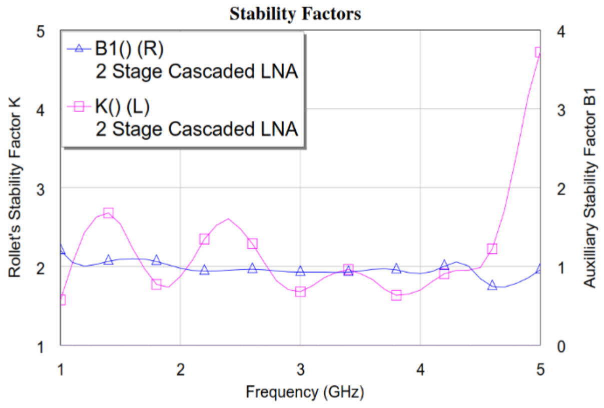


Figure 15 Shows Stability factors: Rollet Factor K and B1 of the proposed LNA design version 1

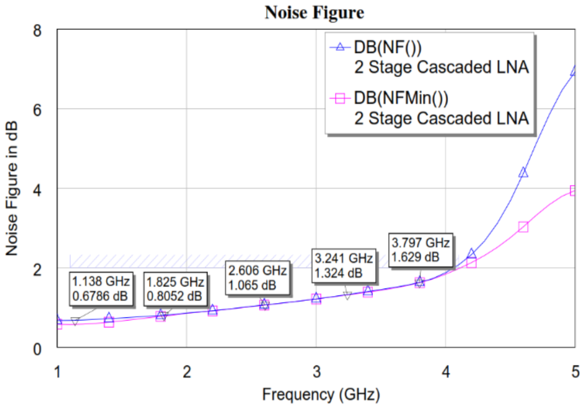
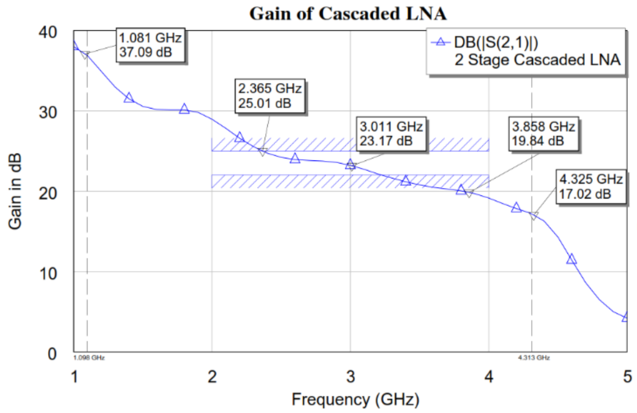


Figure 16 Shows Noise Figure characteristics of the proposed LNA design version 1

The above demonstrated figure 15 shows the stability factors which incorporates Rollet Factors K should greater than 1 and B1 auxiliary factors greater than 0 which is prevailing through the band 1-5GHz. In the figure 16 which is plotted the Noise Figure measurements which is less than 2dB up to 4GHz.



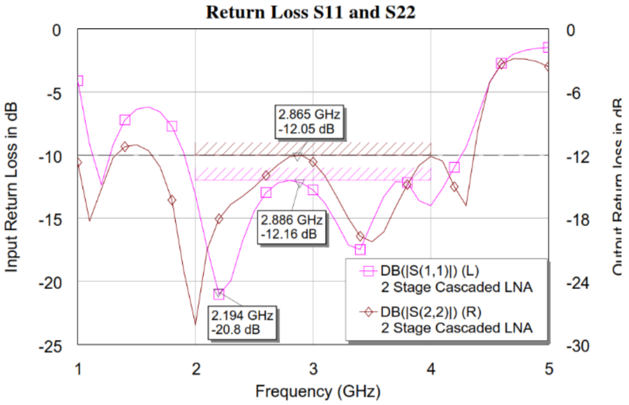


Figure 17 Shows Gain in dB of complete design of the proposed LNA design version 1

Figure 18 Shows Return loss at both Input and Output Port of the proposed LNA design version 1

In the above figure 17 demonstrates the transducer gain (S21) which is having preferred esteem having more over 20dB up to 4GHz however it is differing from 20dB to 38dB. In the region of the interest between 2-4GHz it is having average of 23dB. Same lines figure 18 shows the very good return loss (S11 and S22) is less than -12dB between 2-4GHz.

4.2 Version 2

This version is done by using negative image matching techniques for the same circuit which is show figure 23. The input matching stubs is prepared for optimizing the input return loss and corresponding gain flatness. The schematic is shown in figure 19 and corresponding layout in figure 20.

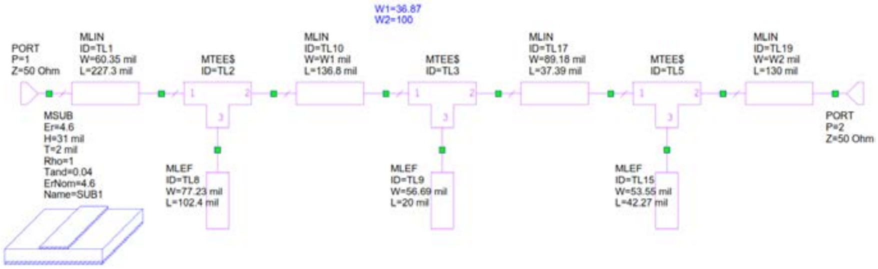


Figure 19 Shows the schematic of the sub block "Input Matching Stubs" of the version 2

4.2.1 Input Match stubs

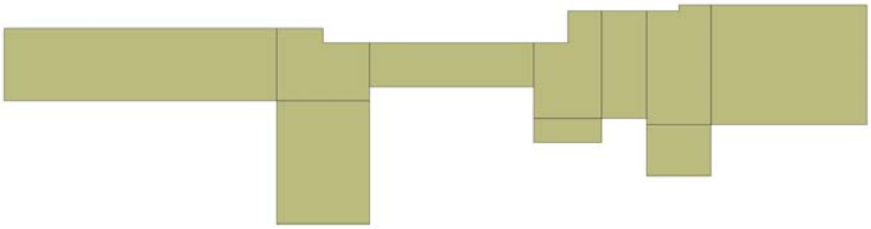


Figure 20 Shows the layout of the sub block "Input Matching Stubs" of the version 2

It is clearly visible that the circuit is prepared by using the micro strip lines structures like "MLIN", "MCROSS", "MLEF" and "MDRSTUB" which means in turn it is linear line, four port junctions, open stub line and radial stubs. In this version, output micro strip matching is done by using negative image matching techniques for the same circuit which is show figure 2. The input matching stubs is prepared for optimizing the input return loss and corresponding gain flatness. The schematic is shown in figure 19 and corresponding layout in figure 20.

4.2.1 Output Match Stubs

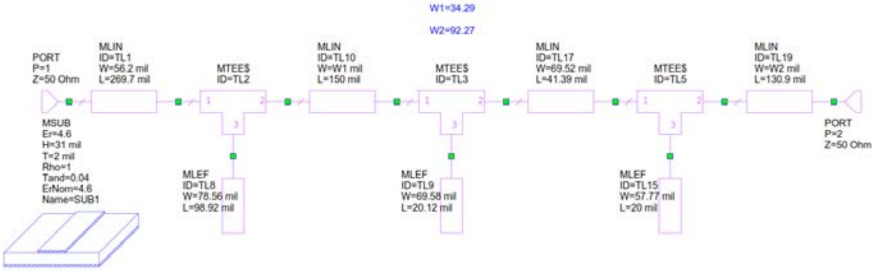


Figure 21 Shows the schematic of the sub block "Output Matching Stubs" of the version 2

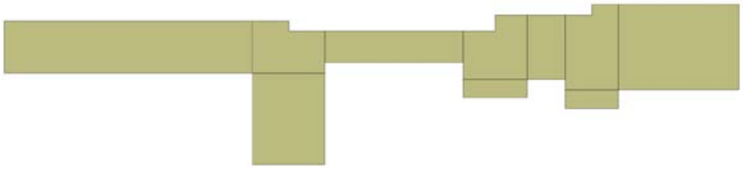


Figure 22 Shows the layout of the sub block "Output Matching Stubs" of the version 2

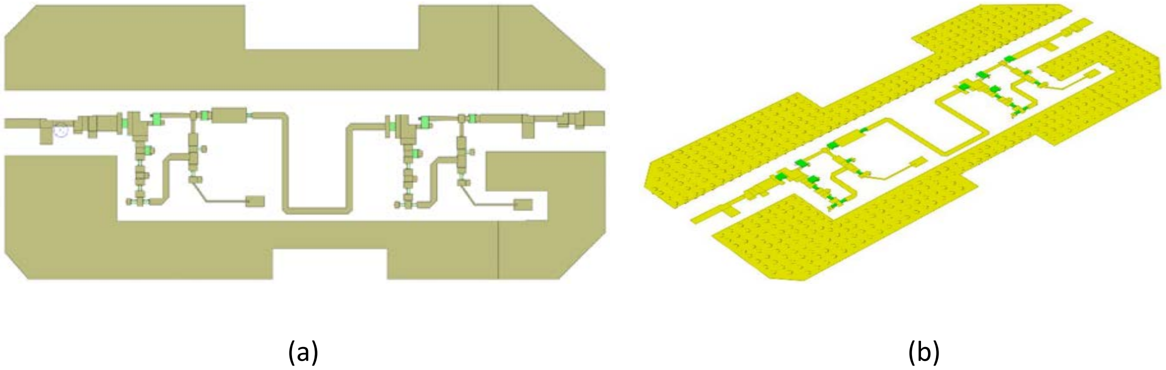


Figure 23 Shows the (a) 2D layout (b) 3D layout of the complete proposed LNA design version 2

4.2.2 Results

The AWRDE features extensive post-processing capabilities, allowing the display of computed data known as "Measurements" on rectangular graphs, polar grids, Smith Charts, histograms, constellation graphs, tabular graphs, Antenna plots and 3D graphs.

There exist an extensive number of the potential electrical and mechanical measurements that are pertinent for the microwave LNA. In any case, there are number of the particulars however all around acknowledged estimations are talked about further.

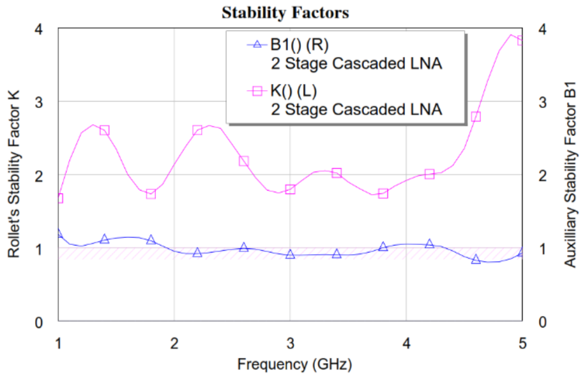


Figure 24 Shows Stability factors: Rollet Factor K and B1 of the proposed LNA design version 2

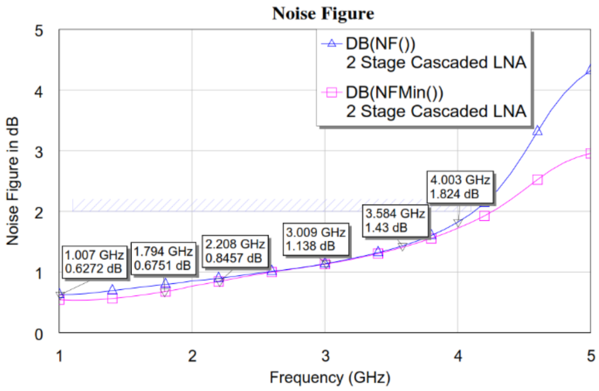


Figure 25 Shows Noise Figure characteristics of the proposed LNA design version 2

The above demonstrated figure 25 shows the stability factors which incorporates Rollet Factors K should greater than 1 and B1 auxiliary factors greater than 0 which is prevailing through the band 1-5GHz. In the figure 26 which is plotted the Noise Figure measurements which is less than 2dB up to 4GHz.

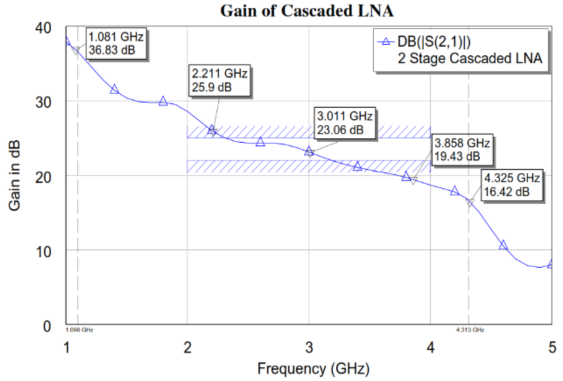


Figure 26 Shows Gain in dB of complete design of the proposed LNA design version 2

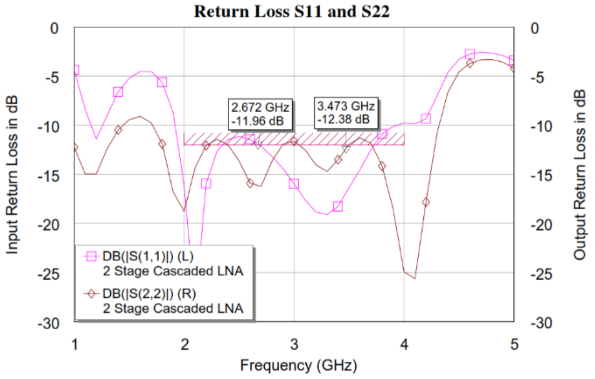


Figure 27 Shows Return loss at both Input and Output Port of the proposed LNA design version 2

In the above figure 27 demonstrates the transducer gain (S21) which is having preferred esteem having more over 20dB up to 4GHz however it is differing from 20dB to 38dB. In the region of the interest between 2-4GHz it is having average of 23dB. Same lines figure 28 shows the very good return loss (S11 and S22) is less than -12dB between 2-4GHz.

5 Theoretical Research Development on the Microstrip Geometric

5.1 Design with Linear Microstrip Line

Figure 29 shows Linear Microstrip Line prototype from AWR tool having length 1600 um width 200 um Port 1and Port 2 are Input and Output Port of Microstrip Line. Layout Design set up by taken care of certain convention. MLIN is used to connect components (Inductor, Capacitor, Transistor), MTEE is used to connect three-point intersection of components and MTAPER is used for smooth tapering between ports by utilising library of AWR Microwave Office Simulation Tool [13]. For transmission power PT from the source and the reflected power PR the return loss in dB as shown in Figure 8 and is given by[4],

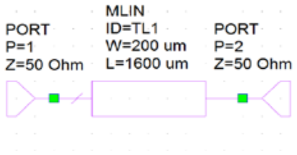


Figure 28 Microstrip Line (MLIN)

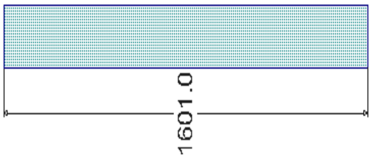


Figure 29 Layout of Microstrip Line (MLIN)

$$\text{RL (dB)} = 10\, log_{10} \left(\frac{P_T}{P_R}\right) \tag{10}$$

For unconditional stability [14],

$$K = \frac{1-|S_{11}|^2-|S_{22}|^2+|\Delta|^2}{2|S_{12}S_{21}|} > 1 \tag{11}$$

$$|\Delta| = |S_{11}S_{22} - S_{12}S_{21}| \ < 1 \tag{12}$$

$$F_{\text{total}} = F_1 + \frac{F_2-1}{G_1} + \frac{F_3-1}{G_1G_2} + \frac{F_4-1}{G_1G_2G_3} + \ldots \tag{13}$$

where, Fn are the noise factor and Gn are available power gain, individually of the nth phase. Note that both magnitudes need aid communicated as ratios, not clinched alongside decibels

5.2 Design with Mitered (U-bend) Microstrip Line

For Mitering Microstrip Line, Meander Line 2 closed form (MTRACE2) is used instead of Microstrip Line (MLIN) in AWR Microwave Office with Miter Length to Width ratio = 1. Whole Design remains same with same Matching Networks.

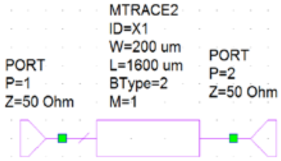


Figure 30 Meander Line 2 closed form (MTRACE2)

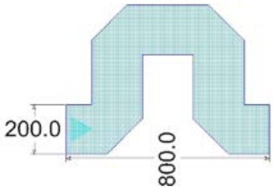


Figure 31 Layout of Meander Line 2 closed form (MTRACE2)

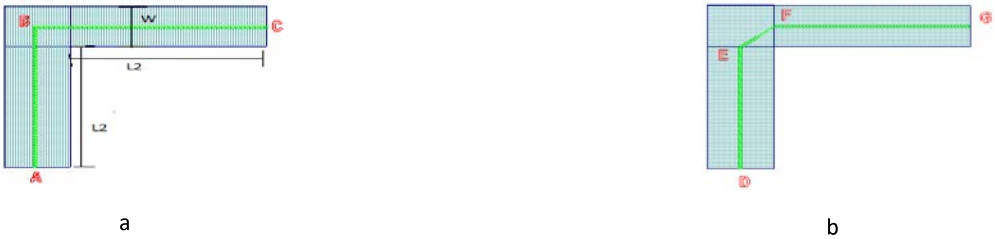


Figure 32 Determination of equivalent length for unmetered right-angled bend. a) Centreline approach. b) Modified centreline approach.

Figure 33.a shows centreline approach and the equivalent length (L_{eq}) is equal to length **ABC** will be given by[12],

$$L_{eq} = 2L_2 + W \tag{14}$$

Figure 33.b shows Modified centreline approach and the equivalent length (L_{eq}) is equal to length **DEFG** which shows actual current flow will be given by [12],

$$L_{eq} = 2L_2 + \frac{\sqrt{2}}{2}W \tag{15}$$

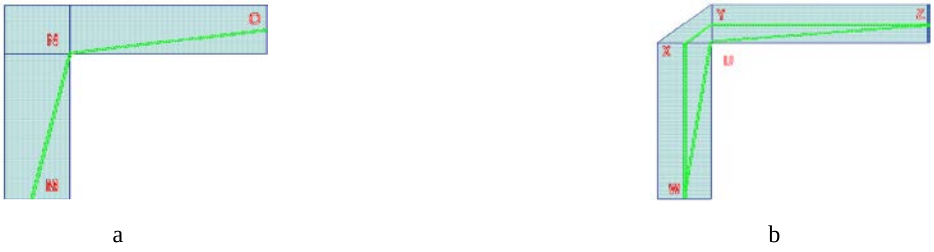


Figure 33 Current path approximations. a) Shortest path. b) Shortest path and modified centerline path.

According to figure 34.a, Due to deviation in current density that is high current density at edges and low current density at center of Microstrip Line current path will not follow the centreline path (**ABC**), but deviates towards the shortest path (**MNO**). For the unmitered right-angled bend the corrected current path by modifying the centreline path, equation (5), into a path following the inner edge more closely (**DEFG**) given by equation (6). The shortest path length, L_{shrt} (**MNO**), follows from figure 34.a,

$$L_{short} = \sqrt{\left(\left(\frac{W}{2}\right)^2 + (L_2)^2\right)} \tag{16}$$

The equivalent length of the 50% mitered right-angled microstrip bend, L_{eqmit2} (**WXYZ**) , is now calculated as[12],

$$L_{eqmit2} = \sqrt{L_{Short} \cdot L_{eq2}} \tag{17}$$

Where, L_{eq2} is given by equation (5).

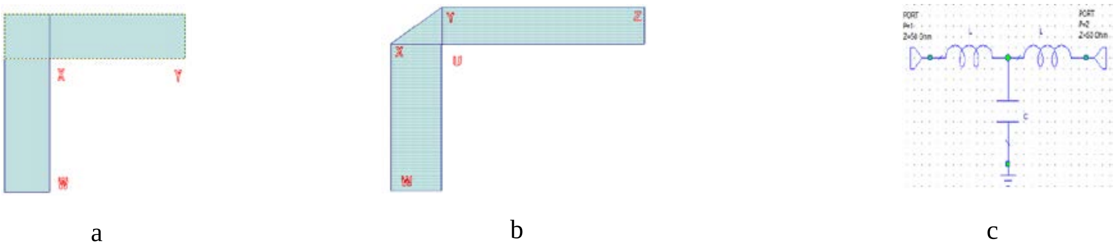
Optimum miter is given by [16],

$$\frac{X}{D} = 0.52 + (0.65 * e^{\left(-1.35*\left(\frac{W}{H}\right)\right)}) \tag{18}$$

Range of Usage,

$0.5 \leq \frac{W}{H} \leq 2.75$ and $2.5 \leq \varepsilon_r \leq 25$

Where, ε_r = dielectric constant (from associated Substrate), H = substrate thickness (from associated Substrate), W = conductor width, in specified units W ≥ 0 for layout



a

b

c

Figure 34 A) Microstrip corner B) Mitered corner C) Equivalent circuit

The equivalent circuit of a microstrip corner is shown in fig. 35 .a. The values of the components are as follows [11].

$$C\,[pF] = W\,.\,[(10.35 * \varepsilon_r + 2.5) * (\frac{W}{h}) + (2.6 * \varepsilon_r + 5.64)] \tag{19}$$

$$L\,[nH] = 220 * h * [1\text{-}1.35 * \exp(-0.18 * (\frac{W}{h})^{\,1.39})] \tag{20}$$

The values for a 50% mitered bend are [11].

$$C\,[pF] = W\,.\,[(3.93 * \varepsilon_r + 0.62) * (\frac{W}{h}) + (7.6 * \varepsilon_r + 3.80)] \tag{21}$$

$$L\,[nH] = 440 * h * [1\text{-}1.062 * \exp(-0.177 * (\frac{W}{h})^{\,0.947})] \tag{22}$$

With W constantly width of the Microstrip accordance Furthermore h stature the height of the substrate. The Z-parameters to those provided for proportional little sign out might make composed Similarly as underneath mathematical statement What's more would simple to change over with to scattering parameters [10].

$$Z = \begin{bmatrix} j\omega L + \left(\frac{1}{j\omega C}\right) & \frac{1}{j\omega C} \\ \frac{1}{j\omega C} & j\omega L + \left(\frac{1}{j\omega C}\right) \end{bmatrix} \tag{14}$$

6 Prime novelty Statement

The proposed design of the LNA is carried using negative image matching technique at the input and output of the circuit using microstrip line with two different versions to understand how major parameters of the LNA to be identify, distinguish and characterized. The prime novelty of the research is on biasing technique, negative image matching and Microstrip line geometric structure variations for particular application context. Expecting that LNA design processing problems are resolved and integrating the lumped elements with Microstrip lines using HMIC manufacturing technique.

1. Special Design of LNA which covers the applications of IEEE Bands L and S.

2. Experimented optimum biasing circuits, micro strip lines and variation towards the LNA frequency measurements.

3. Negative Image Matching techniques are applied for both input and output matching circuits.

5. To have good performance with the sensitivity of the circuit, this research provided effect on biasing circuit on the small signal analysis.

The novelty dwells in a unified approach that deals with the interpretation, design, analysis and optimization of the LNA parameters in their mutual relevant requirements to improve the imperatives LNA performance.

7 Conclusion

This research work includes design, measurement, analysis of microwave low noise amplifier over the IEEE frequency bands L and S. Furthermore, investigating of Linearity, Gain, Stability and Return Loss which also demonstrates low noise amplifier schemes to enhance efficiency and linearity by controlling the number of amplifiers parameters in operation. This paper gives clear thought regarding the geometric varieties of the microstrip lines execution as for LNA estimations. In like manner, the design as two renditions versions which is having same design with various microstrip line components model variety.

REFERENCES

[1]. A. Abdelhamid, M. T. Ozgun and H. Dogan, "A highly integrated wideband LNA with multiple inputs for multi-band mobile devices," 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), Abu Dhabi, United Arab Emirates, 2016, pp. 1-4. doi: 10.1109/MWSCAS.2016.7870076.

[2]. A. Pandey, M. Pusalkar and P. Dwaramwar, "A 0.1–3 GHz, 90nm CMOS wideband LNA employing positive negative feedback for gain, NF and linearity improvement," 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, 2016, pp. 147-152. doi: 10.1109/ICACCCT.2016.7831618.

[3]. M. Pusalkar, A. Pandey and P. Dwaramwar, "A 0.3–3.3GHz low power, low noise figure, high gain inductor-less wideband CMOS LNA," 2016 International Conference on Advanced Communication Control and

Computing Technologies (ICACCCT), Ramanathapuram, 2016, pp. 196-201. doi: 10.1109/ICACCCT.2016.7831629.

[4]. P. Bousseaud, M. A. Khan and R. Negra, "Inductorless wideband LNA with improved input matching using feedforward technique," 2016 46th European Microwave Conference (EuMC), London, 2016, pp. 1027-1030. doi: 10.1109/EuMC.2016.7824521.

[5]. D. Bierbuesse, P. Bousseaud and R. Negra, "Inductorless and cross-coupled wideband LNA with high linearity," 2015 Nordic Circuits and Systems Conference (NORCAS): NORCHIP & International Symposium on System-on-Chip (SoC), Oslo, 2015, pp. 1-4. doi: 10.1109/NORCHIP.2015.7364391.

[6]. H. Cruz, S. Y. Lee and C. H. Luo, "A 3-to-7GHz wideband LNA with IIP3 of −2dBm and 0.5dB in-band gain ripple," 2015 IEEE International Wireless Symposium (IWS 2015), Shenzhen, 2015, pp. 1-4. doi: 10.1109/IEEE-IWS.2015.7164627.

[7]. Peigen Zhou, Daxu Zhang and Jixin Chen, "A 2–10GHz ultra-wideband high gain negative feedback low-noise amplifier," 2016 IEEE International Conference on Microwave and Millimeter Wave Technology (ICMMT), Beijing, 2016, pp. 58-60. doi: 10.1109/ICMMT.2016.7761676

[8]. X. Zhang, L. Yang and F. Huang, "A 0.3–6GHz broadband noise cancelling low noise amplifier," 2016 International Conference on Integrated Circuits and Microsystems (ICICM), Chengdu, 2016, pp. 144-148. doi: 10.1109/ICAM.2016.7813581

[9]. A. K. Ray and R. C. Shit, "Design of ultra-low noise, wideband low-noise amplifier for highly survival radar receiver," in IET Circuits, Devices & Systems, vol. 10, no. 6, pp. 473-480, 11 2016. doi: 10.1049/iet-cds.2016.0065

[10]. M. Kirschning, R. H. Jansen, and N. H. L. Koster, ``Measurement and Computer-Aided Modeling of Microstrip Discontinuities by an Improved Resonator Method,'' IEEE MTT-S International Microwave Symposium Digest, pp. 495-497, May 1983.

[11]. L. Pantoli, A. Barigelli, G. Leuzzi and F. Vitulli, "Analysis and design of a Q/V-band low-noise amplifier in GaAs-based 0.1 µm pHEMT technology," in IET Microwaves, Antennas & Propagation, vol. 10, no. 14, pp. 1500-1506, 11 19 2016. doi: 10.1049/iet-map.2016.0422

[12]. A. K. Ray and R. C. Shit, "Design of ultra-low noise, wideband low-noise amplifier for highly survival radar receiver," in IET Circuits, Devices & Systems, vol. 10, no. 6, pp. 473-480, 11 2016. doi: 10.1049/iet-cds.2016.0065

[13]. F. Ma, X. W. Zhang and B. Y. Chi, "A 100M–1.5 GHz harmonic-rejection SDR receiver front-end," 2015 IEEE 11th International Conference on ASIC (ASICON), Chengdu, 2015, pp. 1-4. doi: 10.1109/ASICON.2015.7516892

[14]. M. N. Karim and P. K. Saha, "Optimal design of a low power UWB LNA for 5–10 GHz application," 2015 18th International Conference on Computer and Information Technology (ICCIT), Dhaka, 2015, pp. 213-216. doi: 10.1109/ICCITechn.2015.7488070

[15]. B. Adhikari, P. Jain and Jamadagni H. S., "An ultra-wideband frequency Domain receiver for software defined radio applications," 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, 2015, pp. 1-6. doi: 10.1109/CONECCT.2015.7383934

[16]. G. de Streel, D. Flandre, C. Dehollain and D. Bol, "Towards ultra-low-voltage wideband noise-cancelling LNAs in 28nm FDSOI," 2015 IEEE SOI-3D-Subthreshold Microelectronics Technology Unified Conference (S3S), Rohnert Park, CA, 2015, pp. 1-2. doi: 10.1109/S3S.2015.7333487

[17]. L. Ma, Z. Wang, J. Xu and O. Zhang, "A 500 kHz-1.4 GHz push-pull differential noise cancellation LNA," 2015 IEEE International Conference on Communication Software and Networks (ICCSN), Chengdu, 2015, pp. 182-185. doi: 10.1109/ICCSN.2015.7296150

[18]. S. Lee, D. Jeong, H. Jin and B. Kim, "Reconfigurable 4 channel carrier aggregation receiver using harmonic recombination technique," 2016 11th European Microwave Integrated Circuits Conference (EuMIC), London, 2016, pp. 1-4. doi: 10.1109/EuMIC.2016.7777473

[19]. Z. Hong-min, Z. Ying, Y. Ying and D. Ke-ke, "Analysis and design of a 3.1–10.6 GHz wideband low-noise amplifier using resistive feedback," 2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Nanjing, 2016, pp. 1-3. doi: 10.1109/ICUWB.2016.7790609

[20]. A. Mattamana, W. Gouty, W. Khalil, P. Watson and V. J. Patel, "Multi-Octave and Frequency-Agile LNAs Covering S-C Band Using 0.25 µm GaN Technology," 2016 IEEE Compound Semiconductor Integrated Circuit Symposium (CSICS), Austin, TX, 2016, pp. 1-5. doi: 10.1109/CSICS.2016.7751057