International Journal of Hybrid Information Technology
Vol.8, No.9 (2015), pp.215-224
http://dx.doi.org/10.14257/ijhit.2015.8.9.20

A Fuzzy Logic System to Estimate ARP Poisoning Susceptibility of a Client in Wireless Networks

Jaideep Singh[1] and Vinit Grewal[2]

[1]*ECE Department, Lovely Professional University, Phagwara*
Jaideepsinghbawa@Gmail.Com
[2]*ECE Department, Guru Nanak Dev University, Regional Campus, Jalandhar*
Vinidhaliwal19@Gmail.Com

Abstract

Network Security is a supreme worry today for all computer users and organizations. It is the center of focus in all large and small networks. Extensively used internet protocols do not have promising mechanisms for protection against malicious activities. So the network attackers manage to shape and modify these protocols to launch various kinds of attacks on the legitimate clients. These attacks can have threatening effects on personal as well as professional aspects of clients. This paper proposes a fuzzy logic system to analyse and examine the susceptance of network clients towards various types of precarious attacks. The factors affecting the susceptibility have been carefully shortlisted by an extensive survey into journals, magazines and various research papers by leading authors in this field.

Keywords: *Fuzzy Logic; Susceptibility; Feedback Systems; Wireless Networks; ARP Spoofing Attack; Eavesdropping; Spoofing detection and prevention*

1. Introduction

Like any other feedback systems, networks assuredly need and deserve evaluation processes to accurately identify their strengths and weaknesses, so that improvements can be made in the areas lagging. Right now, there are no evaluation systems that provide high quality feedback about network security aspects and hence minimum paths to improvement. It is surely a daunting task to identify whether a client working in a wireless environment is safe enough to do his job without putting his security at stake. In a world, where information technology is essential for any individual or business organization to survive, the question seems indisputable. It is surely unfair for the clients performing confidential operations and secret communications wirelessly, while completely relying on the network administrators for their safety. So in order to analyse susceptibility of various clients towards getting eavesdropped, a fuzzy logic system using MATLAB™ can be setup with just the right number of parameters that may help in bringing out the general trend of security flaws and vulnerabilities prevailing in wireless networks. In most of the systems, we have factors affecting the performance that are higher at priority than others. So, fuzzy systems are more reliable and precise than any other setups to bring out the performance inferences. In this research, we are developing a fuzzy logic system to evaluate the susceptibility of a client towards attacks based on the parameters that have been identified by the most popular researchers. The factors shortlisted are considered as input variables to calculate the output. These input variables include

- Firewall Effectiveness
- Host Configuration

ISSN: 1738-9968 IJHIT

- Operating System
- User Awareness
- Network Scale

The paper is organized as follows: Section 2 describes introduction to fuzzy logic, Section 3 describes the fuzzy inference engine, Section 4 describes the simulation architecture and Section 5 concludes the paper.

2. Introduction to Fuzzy Logic

Fuzzy logic was proposed in 1965. It is a problem-solving control system methodology that can be put into effect in hardware, software or a combination of both. It is a form of multi-valued logic that deals with approximation rather than exact values. Fuzzy provides a much uncomplicated manner to bring out definite results out of very vague and non-specific information. In a sense, fuzzy logic resembles human decision making with its ability to work from approximate data and find precise solutions.[2] Fuzzy logic subsumes a straightforward, rule-based (IF X AND Y, THEN Z) technique to solve a control problem, rather than experimenting to model a system mathematically. Fuzzy logic variables may have a truth value that ranges between 0 and 1. It requires numerical parameters in order to function, such as what is considered significance error or significant rate-of-change-of-error. Precise values of these numbers are usually not crucial unless very responsive performance is required. The generalized fuzzy logic architecture has been depicted in Figure 1.

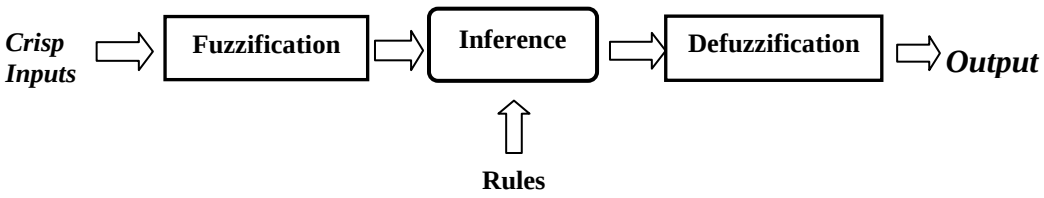

Figure 1. Fuzzy Logic Architecture

3. Fuzzy Inference Engine

A Fuzzy inference engine is an artificial intelligence tool based upon fuzzy set theory and if-then rules. Its basic structure consists of three conceptual components which are a rule base that contains selection of fuzzy rules, a data base which defines membership functions used in fuzzy rules and a reasoning mechanism performing inference procedures upon the rules and given facts to derive at a reasonable output. It is a way of mapping an input space onto an output space. [11] It is implemented in two phases given below.

3.1 Fuzzification

Fuzzification is a method of mapping measured input values to fuzzy membership functions. A membership function is a curve that describes how each position in the input space is mapped to a membership value within 0 and 1. There are distinct shapes of membership functions namely triangular, piecewise, trapezoid, gaussian, bell-shaped, *etc*. [3]

3.2 Defuzzification

Defuzzification is a conversion of internal fuzzy output variables into crisp values that can actually be used as output. It is done after the evaluation of inputs and applying them to the rule base.

4. Simulation Architecture

The simulation model is built up using the Fuzzy Logic Toolbox of Mathworks™. Fuzzification comprises the process of transforming crisp values into grade of memberships for linguistic terms in fuzzy sets. The first step involves identification of the parameters that are to be fuzzified and determining their respective range of values. The inference after the interaction is the value for each performance parameter. Five input parameters have been considered and an output is to be obtained from the FIS as shown in figure 2. The input parameters in hierarchy of their importance in the fuzzy system are as follows.

Host configuration is a very important parameter to decide the ARP poisoning susceptibility of a client. Static configuration is the most favoured type whereas dynamic configuration is least favoured in wireless networks from security point of view.

Firewall effectiveness is the next in importance in any particular wireless network. If a network is secured by some successful firewalling solutions such as Mikrotik or Cyberoam, the chances of ARP poisoning are very less as these firewalls implement latest measures to detect and prevent such attacks.

Network Scale also plays a major role in deciding the probability of occurrence of such attacks. The public networks are most vulnerable to ARP attacks if they lack inbuilt trusted firewall systems. Coffee shops, Shopping malls and other such places are soft targets of ARP poisoning attacks. Organizations, educational institutions and banks are less vulnerable to cyber attacks as they use more sophisticated hardware and better firewalls to curb attacks. The home networks are safest as there are less number of unknown users on the network and mostly trusted clients use the network. Furthermore, as home networks can be configured to meet personal needs by the clients they are less vulnerable.

Operating systems play a vital role in estimating the ARP poisoning susceptibility of a client. According to the recent research, Microsoft Windows™ is the most attacked operating system for session hijackings followed by Apple MAC™and UBUNTU™.

End User awareness is yet another important parameter that is essential to prevent a client from ARP poisoning attack. If a client keeps himself updated with the latest tips and tricks that hackers use to strip off the security out of wireless networks, there is always a less chance of getting trapped. A client must at least be able to differentiate between regular and phishing emails, create strong passwords and keep their computers locked for protection. More than 51% of the wireless networking clients according to the recent research do not know how to update anti-virus protection on company PCs'.

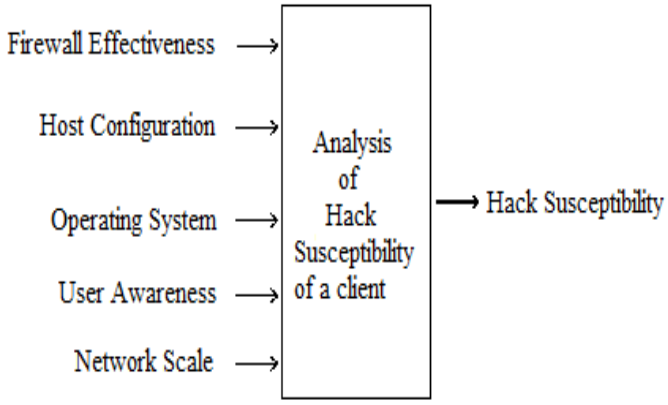

Figure 2. Simulation Architecture

4.1 Membership Functions

A membership function is a curve that describes how each position in an input space is mapped onto a membership value between 0 and 1. It is a graphical representation of magnitude of participation of each input and association with other inputs on the basis of weights. [10] The membership functions are built up using a membership function editor available in fuzzy logic toolbox of MATLAB™. The rules and membership functions together decide the result of a system.

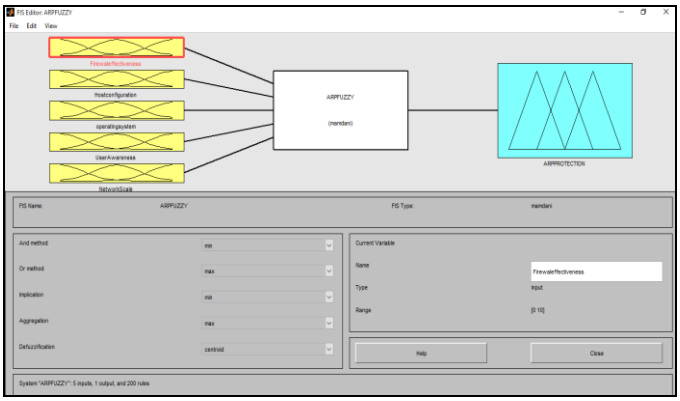

Figure 3. Membership Function Editor

Membership function editor for the ARPFUZZY system is shown in Figure 3. The five input parameters Firewall Effectiveness, Host Configuration, Operating system, User Awareness and Network Scale are shown on the left side, whereas the only output obtained from the system which is ARPPROTECTION is depicted at the right side of the system. The system processor is labeled as ARPFUZZY and is in the middle of the system. This contains all the necessary rules that combine with the membership functions to generate a single output.

The fuzzy rule bases used to train the system have been developed based on logical reasoning. The results obtained reflect that the proposed system can be used to estimate ARP poisoning susceptibility of a no-vice client in wireless networks. The various membership functions (Mf) defined for the Fuzzy Logic system have been tabulated with 5 input parameters in Table 1 and one output parameter as shown in Table 2.

Table 1. Membership Functions For Given Input Parameters

Input parameters	Mf1	Mf2	Mf3
Firewall Effectiveness	Poor	Good	Excellent
Host Configuration	Static	DHCP	Auto
Network Scale	Public	Organization	Private
Operating System	Windows	Apple MAC	Ubuntu
End User Awareness	Low	Medium	High

Table 2. Membership Functions For Given Output Parameters

Output parameter	Mf1	Mf2	Mf3
ARP Protection	Low	Medium	High

5. Rule Base

A fuzzy rule base is a collection of knowledge in the if-then format by experts. It describes the relationship between fuzzy input parameters and output. As per the input parameters fuzzified, rule base is generated by applying reasoning to estimate the overall output for protection parameter of a client. **200** rules have been generated to train the fuzzy system during this implementation.

While formulating the if-then rules, a specific hierarchy on the basis of priority has been followed. Among all the five parameters, host configuration has been given the top priority followed by firewall effectiveness and network scale based on the recent survey and researches. The end user awareness has been given the least importance in the rules. Sample rules from the fuzzy system have been shown as follows.

If (Firewalleffectiveness is GOOD*)* and (Hostconfiguration is DHCP) and (operating system is MAC) and (UserAwareness is bad) and (NetworkScale is Organisation) then (ARPSUSCEPTIBILITY is MEDIUM) is rule number 95 of fuzzy logic system.

If (Firewalleffectiveness is EXCELLENT) and (Hostconfiguration is Auto) and (operating system is WINDOWS) and (UserAwareness is good) and (NetworkScale is Organisation) then (ARPSUSCEPTIBILITY is LOW) is the rule number *115* of the fuzzy logic system.

If (Firewalleffectiveness is Poor) and (Hostconfiguration is STATIC) and (operating system is Windows) and (UserAwareness is bad) and (NetworkScale is Public) then (ARPSUSCEPTIBILITY is HIGH) is the rule number *1* of the fuzzy logic system.

Figure 4. shows the rule editor for the built up system. The various membership functions logically *AND* (connections) together to produce the output.

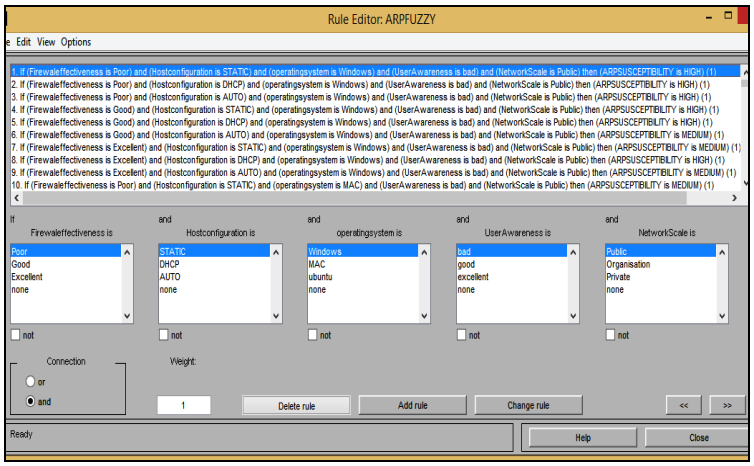

Figure 4. Rule Editor for ARPFUZZY System

The rule viewer for the system is shown in Figure 5. The red line in the middle of every membership function can be adjusted to obtain the corresponding change in output.

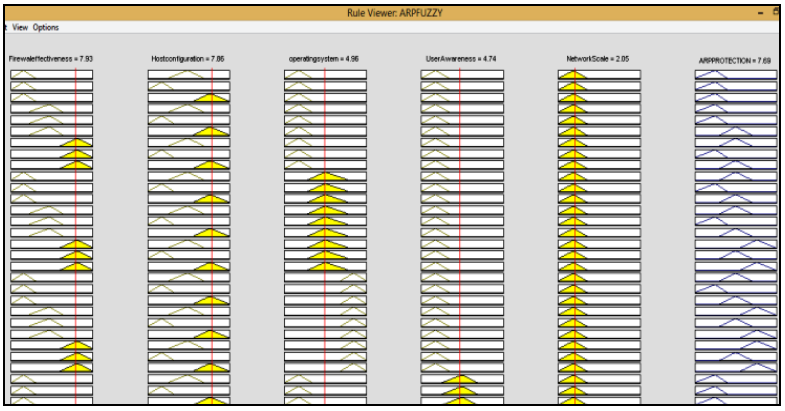

Figure 5. Rule Viewer for the ARP Fuzzy System

The surface viewer is yet another tool that can be used to see a three dimensional comparison between various parameters of the system. The entire area covered by the output set based upon the input area span can be viewed. A two as well as three dimensional surface view is possible using the fuzzy logic toolbar. At most, three membership functions can be used for obtaining a comparative plot, thus indicating dependencies on each other. The *Evaluate* button starts a calculation and a plot is generated . The surface view for ARPFUZZY system between Firewall Effectiveness, Operating Systems and ARP Protection has been shown in Figure 6.

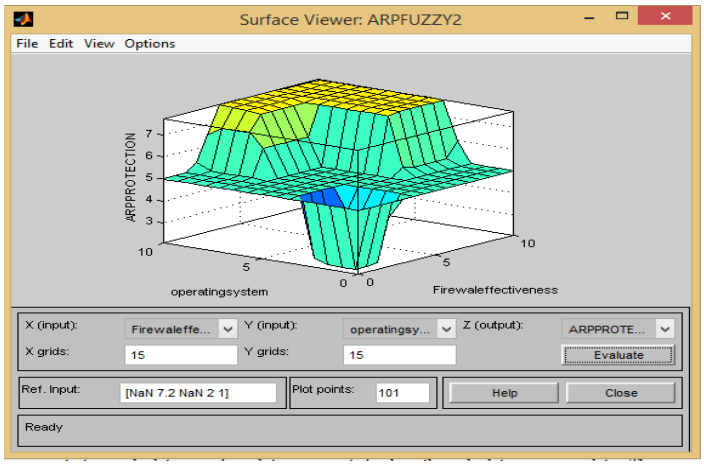

Figure 6. Surface Viewer for the ARPFUZZY System

The outputs calculated for varied values of inputs have been tabulated in Table 3.

Table 3. Results Obtained From ARPFUZZY System

INPUT VARIABLES					OUTPUT
FE	HC	OS	UA	NS	ARP Protection
1.2	2.2	4.2	3.2	2	2.04
3	2	4	3	2	3.29
7	7.2	4	3	2	7.71
8	7.2	6	2	1	7.70
8	7	2	1	1	5.02
7.2	8	6	3	2	6.46
2	3	3	3	3	2.91
8	7	4	6	7	7.75
6	8	6	6	6	7.72
4	6	4	6	5	7.70
1	2	3	4	5	2.82
1	2	4	1.2	2.3	2.09

It is evident from the results obtained that whenever there is a small change in the values of Firewall Effectiveness or Host configuration, which are high priority parameters among the input parameters chosen, the output is affected more. On the contrary, a considerable change in less important input parameters such as User awareness and Operating systems affect the output less. As a result, the system built caters to the expectations in an excellent manner.

6. Conclusion

The research findings reveal that the most important factor in deciding the probability of a client to get eavesdropped is firewall effectiveness followed by other factors. The

awareness of a novice user about various attacks also plays an important role in deciding the consequences. Even if a client notices a symptom of a cyber assault midway through it, a lot of essential information may be prevented from getting stolen. The fuzzy system of estimating ARP poisoning susceptibility of a client in wireless networks meets the feedback expectations in an effective manner. The model can invariably be used as a decision support system for implementing measures in the wireless networks that lack security in specific aspects, after gauging the output scores on the basis of network parameters in consideration. This research can later be extended by including more parameters in the fuzzy system after reaching into latest studies and surveys. Furthermore, the fuzzy system can be developed as a real world application, an embedded system consisting of a microcontroller, keypad and a small display device that can be used for conducting surveys and research among network administrators and general public.

References

[1] S. Whalen, "An Introduction to ARP spoofing," 2600: The Hacker Quarterly, vol. 18, no. 3, Fall **(2001)**, Available: http://www.ouah.org/intro_to_arp_spoofing.pdf
[2] Ekong Victor, Ekong Uyinomen and Uwadiae Enobakhare, "A Fuzzy Inference System for predicting depression risk levels", Emmanuel African Journal of Mathematics and Computer Science Research, Vol. 6(10) **(2013)**,pp 197-204.
[3] G.A Bhosle.and R.S. Kamath, "Fuzzy inference system for teaching staff performance appraisal", International journal of computer and information technology (ISSN 2279-0764) Vol. 02 **(2013),** pp 382-385**.**
[4] D. Plummer, "An ethernet address resolution protocol", **(2010)**, RFC 826.
[5] José Luis Aznarte M., José Manuel Benítez.and Juan Luis Castro., "Smooth transition autoregressive models and fuzzy rule-based systems: Functional equivalence and consequences",**(2007)**,Available:http://www.sciencedirect.com/science/article/pii/S0165011407001583.pdf
[6] J.-S.R.Jang., "Adaptive-Network-Based Fuzzy Inference System", In proceedings of IEEE Transactions on Systems, Man, and Cybernetics, Vol. 23, No. , **(1993)**, pp 665-684.
[7] Lazim Abudullah1.and Mohd Nordin Abd Rahman., "Employee likelihood of purchasing health insurance using fuzzy inference system", International Journal of Computer Science Issues. Vol 9, Issue 1, No. 2, **(2012)**, pp 112-116.
[8] Faisal Md, Abdur Rahman and Parves Kamal, "A Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm", International Journal of Advancements in Technology, (2014), pg 82-95, ISSN: 0976-4860.
[9] Cisco Systems, "Configuring Dynamic ARP Inspection", Catalyst 6500 Series Switch Cisco IOS Sofware Configuration Guide, Release 12.2SX, **(2012)**, chapter 39, pp 39:1–39:22.
[10] Jaideep Singh, Gurnoor Kaur and Goldendeep Kaur, " Determining best setup sites for cellular towers using fuzzy logic", In Proceedings of International Conference on Futuristic Trends in Computational Analysis and Knowledge Management (ABLAZE), IEEE (**2015**), pp. 256-260.
[11] Maedeh Rasoulzadeh, "Facial expression recognition using fuzzy inference system. International Journal of Engineering and Innovative Technology, Vol. 1, Issue 4, **(2012)**, pp 1-5.
[12] Steven D. Kaehler, "Fuzzy Logic Tutorial", Retrieved from: http://www.seattlerobotics.org/encoder/dec97/fuzzy.html
[13] Zalinda Othman, Khairanun Subari.and Norhashimah Morad, "Application of fuzzy inference systems and genetic algorithms in integrated process process planning and scheduling", Academin Staff Training Research, Research Grant No. 305/PTEKIND/622140.
[14] Larry Suto, "Analyzing The Effectiveness of Web Application Firewalls", by Larry Suto Application Security Consultant, San Francisco, **(2011)**.
[15] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen Center for Education and Research in Information Assurance and Security (CERIAS) Purdue University Analysis of Vulnerabilities in Internet Firewalls.
[16] Hadeel Tariq Al-Rayes, "Studying Main Differences Between Linux & Windows Operating Systems Lecturer/".
[17] Snort Project, "The. Snort: The open source network intrusion detection system", <http://www.snort.org>.
[18] Alfred Loo, "The myths & truths of wireless security", Communication of the ACM, Vol 51, No. 2, **(2008)**, pg 67-71.
[19] Jaideep Singh, Vinit Grewal, A Survey of Different Strategies to pacify ARP Poisoning Attacks in Wireless Networks", International Journal of Computer Applications, Volume 116. No. 11, **(2015)**.

[20] Cindy Broadie," The Importance of Security Awareness Training", SANS Institute Reading Room, © Sans Institute, **(2009)**.
[21] Cristian Florian, "Top Most Vulnerable Applications and Operating Systems in 2010", GFI Blog, **(2011)**, Retrieved from: http://www.gfi.com/blog/top-vulnerable-applications-operating-systems-2011.
[22] Goldendeep Kaur and Dr. Jyoteesh Malhotra, "ARP Spoofing Detection Algorithm an Effective Approach", American International Journal of Research in Science, Technology, Engineering and Mathematics, **(2015)**, pg 226-230, Available online at : http://www.iasir.net
[23] H. Neminath, S. Biswas, S Roopa, R. Ratti, R. Nandi, F.A. Barbhuiya, A. Sur, and V. Ramachandran, "A DES Approach to Intrusion Detection System foe ARP Spoofing Attacks", 18th Mediterranean Conference on Control & Automation (MED), ISBN: 978-1-4244-8091-3, IEEE **(2010)**.
[24] "ARP-Guard™," **(2013)**, [Online]. Available: http://www.arp-guard.com.
[25] Maltab™ User's Fuzzy Logic Toolbox™ Guide.
[26] V. Goyal and V. Abraham " An efficient Solution to the ARP cache poisoning problem", in Proceedings of 10th Australasian Conference on Information Security and Privacy, **(2013)**, pp 40-51.
[27] R Tripathy and V Goyal, "An efficient solution to the ARP cache poisoning problem", in Proc of Australasian Conference on Information Security and Privacy (ACISP), vol. 1. Brisbane, Australia, **(2011)**, pp. 40–51.
[28] Zouheir Trabelsi and Khaled Shuaib, "Spoofed ARP Packets Detection in Switched LAN Networks", J. Filipe and M.S. Obaidat (Eds.): ICETE, **(2013)**, CCIS 9, pp. 81– 91.
[29] H. Hwang, G. lung, K. Sohn, and S. Park, "A study on MITM (man in the middle) vulnerability in wireless network using 802.IX and EAP," in Proceedings of the 2008 International Conference on Information Science and Security, **(2008)**, pp. 164-170.

Authors

Jaideep Singh, was born in Amritsar, Punjab. He completed his M.Tech in Electronics and Communication Engineering from Guru Nanak Dev University, Regional Campus, Jalandhar in 2015 and received his B.Tech degree with distinction from Amritsar College of Engineering and Technology, Amritsar in 2013. He joined Lovely Professional University in 2015 for his doctorate and is currently carrying out research work in the field of Cyber Security and Wireless Networking. He has published and presented 8 research papers in scientific journals and International conferences.

Dr. Vinit Grewal, was born in Mumbai on 16/03/1980. She received her B.Tech degree in Electronics and Communications Engineering in 2002 from Gaini Zail Singh College of Engineering and Technology, Bathinda and M.E degree in Electronics and Communication from Thapar University, Patiala in 2005. She did her Ph.D from Department of Electronics and Communication at National Institute of Technology, Jalandhar in WiMax networks in 2013. Her research interests include digital communication, signal processing and wireless networking

She has 4 years research experience at National Institute of Technology, Jalandhar from February 2007 to July 2011. From August 2011 to June 2012, she worked as Assistant professor at LPU Phagwara. Currently, she is working as Assistant Professor in the Department of Electronics and Communication, GNDU regional campus, since July 2012. Till present, she has a total of 12 publications in various International Journals and conferences.