QUEST OF ROGUE ACCESS POINT IN BLUETOOTH NETWORKS USING NEURAL NETWORK

Menal Dahiya

Department of Computer Science, Maharaja Surajmal Institute,
C-4, Janakpuri, Delhi-110058, India
meenaldahiya@msi-ggsip.org

Abstract

Bluetooth networking has been developed to provide connectivity between wide ranges of wireless devices. Wireless communication is the driving force behind the development of new technologies and standards. Bluetooth is one of the emerging standards that fulfill the concept of mobility, flexibility, connectivity and scalability. The security issues in Bluetooth network are different types of external & internal attacks; entries of unauthorized devices, viruses may corrupt the wireless devices etc. Entry through rogue access point is one of the main security issues which we discuss in this paper. In This paper we will project a approach which help in detecting the RAP in Bluetooth network. We apply Back propagation network algorithm for achieving the results.

***Keywords*:** Bluetooth; Back Propagation Algorithm; Detection; Rogue Access Point; Wireless Communication.

1. Introduction

With the advent of network technology, the demand for wireless communication and mobile computing devices are increasing. Mobile devices like laptop, smart phones, PDA and other digital devices exchange information in faster and smoother fashion. There are many types of wireless networks that help in transferring information from source to destination like Wi-Fi, WLAN, Wi-Max, and Bluetooth. Among all, Bluetooth is a popular technology that link cell phones to their peripherals and other accessories. Bluetooth is a low last technology, simple and works on low power. Bluetooth provides a short range cable free environment for sharing information between devices and operates in the open 2.4 GHz ISM band [Menal (2016)]. The Bluetooth radio system provides connectivity between fixed and portable devices. During connectivity to different types of hardware platforms, its security has been considered as a serious problem. To enhance the security and privacy in Bluetooth, wireless communication impetus new standards and security features. For finding actual weaknesses or vulnerability against Bluetooth, proper implementation steps can be taken to accelerate the faith of user in the communication.

Security of Bluetooth can be breached by many ways, there are number of attacks which continue to be problematic in Bluetooth communication, the rogue access points or rogue devices is considered to be the another attack on Bluetooth present technology. Rogue access point is an unauthorized access point in any network. Rogue access point is introduced with the known of an authorized access point and after that it has been used to obtain secret information from the organizations [Kui (2003)]. This valuable information or credentials are used to initiate serious attacks and also create mess with other users. Unauthorized Bluetooth devices or rogue devices can disguise him as an authorized user through address and link key spoofing.

2. Bluetooth

Bluetooth system working is based on point-to-point or point to multipoint connection. When two or more nodes share a common channel they form a piconet. In a piconet, one unit acts as the master and other unit works as slave. Some slaves known as parked slaves and they cannot be active on the channel, but synchronized to the master. Multiple piconet together sharing the coverage area from a scatter net. Each piconet has its own frequency hopping channel and is determined by the Bluetooth device address of the master. The minimal hop rate is 1600 hop/sec.

Every Bluetooth device, includes four entities that are used for maintain the security at the link level [Ma (2010)]. These includes a secret key for authentication and for encryption, third a psendo random number which is unique for each new transaction and the fourth entity is Bluetooth device address which is 48 bit long and unique to the device. Bluetooth authentication scheme uses a challenge response strategy i.e. both the parties shared symmetric keys for successful authentication [Yeh (2012)]. Bluetooth standards are basically for wireless personal area network (WPAN) which is a short range radio frequency communication. Bluetooth technology is very much reliable for ad-hoc networks and integrated number of business devices like cell phone, keyboard, pagers, headsets, etc.

Bluetooth technology provides many benefits like cable replacement, ease of file distribution, internet connectivity and automatic synchronization between Bluetooth enabled devices. Apart from these services, maintaining security in Bluetooth devices is a big challenge. Like any wireless technology, Bluetooth has a number of security vulnerabilities. Some of the well known Bluetooth attacks are: Identity detection, location tracking, denial of service, unauthorized access point (RAP) etc. Strength of the Bluetooth network security mainly based on the length and random generation of the passkeys used for connection establishments. These setting play a vital role in maintaining the security of Bluetooth networking. Also optional user authorization concept for connection setup provides an extra security level.

3. Experimental Setup

For simulation purpose, let us consider a scenario, where a Bluetooth enabled device B (master) communicates on regular basis with another authorized devices (slaves) in a piconet. For authentication and encryption purpose, their unit keys serve as link keys i.e. device B store the link keys of all the slaves. When an unauthorized device, say X take initiative to attack, it requires the address and unit key of one of the slaves say S1. The requirement of address is fulfilled by capturing the device and then by programming it. Unit key of device S1 is obtained by the unauthorized device X by establishing a communication link with device S1. Now device X is ready to enter in the network with authorized information. Figure 1 shows the Bluetooth network having one master device, two slave devices and a rogue device which wants to enter into the network.

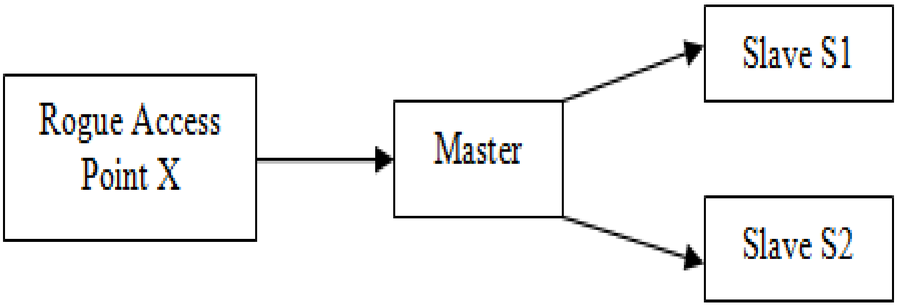

Fig.1: Bluetooth Network having two Slaves and a Rogue Device.

We take two inputs, 56 bits each means the address and unit key of two Bluetooth devices that stores in the memory of master device. Our approach to detect the rogue access point in Bluetooth networks is that we store both the basic requirements of the device in the form of network parameters in the master's device memory. Using supervised Back propagation algorithm of neural network, we trained the network by neural network tool with the given inputs and store the result in the form of weight matrices [Demuth (2012)]. These weight matrices are hard to crack and thus safe for the Bluetooth network. Back Propagation algorithm is widely adaptable approach in neural networks used for many applications. We take 56 input neurons, 28 hidden neurons and 56 output neurons. The primary goal of training the network is to achieve a correlation between the ability to respond positive to the input data that are used for training and the ability to provide good results to the input that were similar. The total squared error of the output computed by network is minimized by a gradient descent method known as Back Propagation or Generalized Delta Learning Rule [Sivanandam (2008)]. Network trained in 4 iterations and the acceptable mean square error was 0.001. Figure 2 shows network performance during memorized pattern set of Feed Forward Network trained by Back Propagation algorithm.

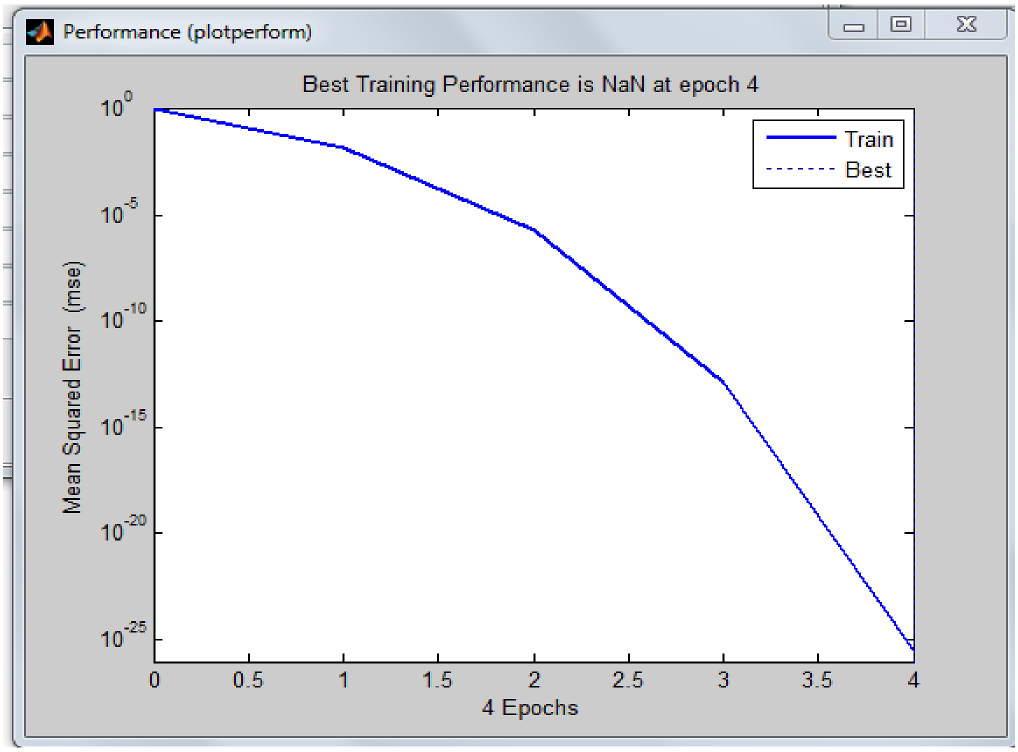

Fig. 2: Performance Graph of Feed Forward Network (56-28-56).

4. Conclusion

Unauthorized Bluetooth devices enter into the authorized network through hacking the address and link key of the legitimate device. These types of rogue devices or rogue access points are big worry for the growth of an organization. The proposed neural network mechanism based on supervised Back propagation learning algorithm. This mechanism makes the system strong and helps in intrusion detection. The authentic Bluetooth device addresses along with their unit keys are stored in the form of training parameters. These training parameters are harder to crack even if the hacker captures and programming the device too. Because by seeing the training parameters no one can find what algorithm you used or what kind of network you used for the training parameters. So this mechanism provides security to the Bluetooth devices and help in detecting rogue access point in the Bluetooth network.

References

[1] Demuth H., Beale M., (2012): *Neural Network Toolbox*, Fourth Edition. The Math Works.

[2] Kui M., Xiuying C. (2003): Research of Bluetooth Security Manager. International Conference on Neural Networks and Signal Processing, **2**, pp. 1681–1684.

[3] Menal, Gill S. (2016). Secured Bluetooth Authentication using Artificial Neural Network. IJRCCT, **5(5)**, pp. 244-248.

[4] Ma D., Tsudik G., (2010): Security and Privacy in Emerging Wireless Networks. IEEE Wireless Communication, **17(5)**, pp. 12-21.

[5] Sivanandam N. S., Deepa N. S., (2008): *Principal of Soft Computing*. Wiley-India, pp. 71–83.

[6] Yeh C. T., et al. (2012): Securing Bluetooth Communications. International Journal of Network Security, **14(4)**, pp. 229–235.