The Fig 4-7 shows the simulation results. The simulation results show the total no. of transmissions, throughput loss, and malicious user detection delay. Total transmissions deals with number of tests performed by Fastprobe over a certain period of time. Plot of total transmission contains two graph, first one indicates total transmission of Fastprobe algorithm and the second one is that adding elliptic curve cryptography to the CRNs.

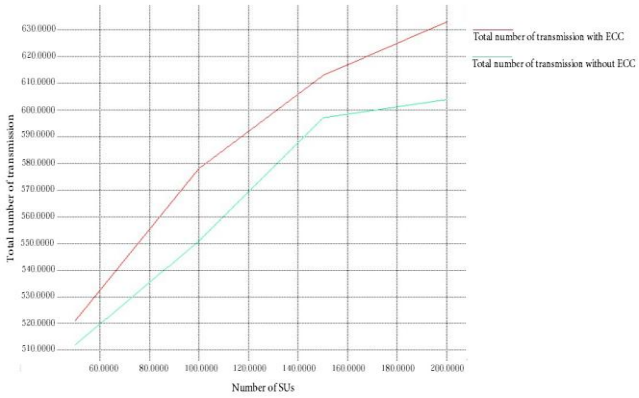

Figure 5: Total number of transmission with and without ECC

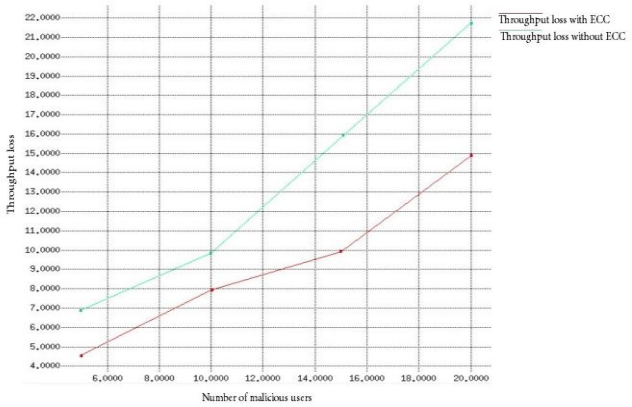

Figure 6: Throughput loss with and without ECC

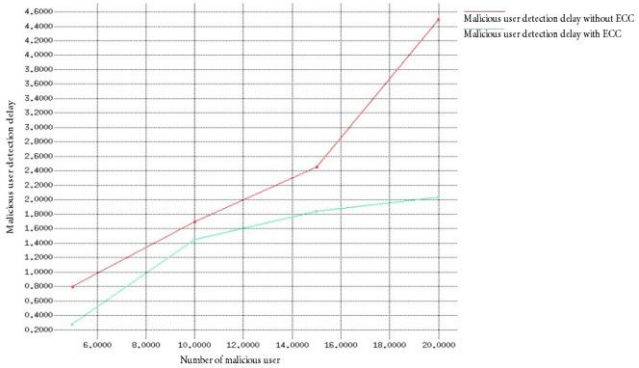

Figure 7: Malicious user detection delay with and without ECC

Throughput loss per user, which define as the average fraction of time spend by SUs as well as SBS in sensing, transmitting and receiving data related to sensing. The simulation shows that throughput loss is reduced when using the elliptic curve cryptography. In the case of malicious user detection delay, simulation result shows that detection delay is reduced when ECC is added to the CR network. Fig. 7 shows the plot of malicious user detection delay with or without ECC. Simulation is carried out in NS2.

6. Conclusion

Cognitive network is sensitive to security threats. The attackers may be external users or secondary users acting as a malicious user. So, in order to overcome these issues malicious user detection system is used. Cooperative sensing improves sensing accuracy but at the same time makes the system more susceptible to malicious users that may be present in the system. In cooperative spectrum sensing (CSS), cooperation among SUs raises concerns about reliability and security of cooperative spectrum sensing, as some of the SUs may report incorrect sensing data .All the control messages from SBS to SUs and from SUs to SBS are encrypted that can only be decrypted by the intended recipient. SBS gives a unique key to the other nodes participated in the CR network. The simulation results shows that Fastprobe with ECC reduces the throughput loss and malicious user detection delay.

References

[1] S. Mishra, A. Sahai, R. Brodersen, "Cooperative sensing among cognitive radios", in: Proc. of IEEE ICC 2006, vol. 4, 2006, pp. 1658-1663.
[2] O. Fatemieh, R. Chandra, and C. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in Proc. 4th IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2010, pp.112.
[3] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in Proc. IEEE International Conference on Communications (ICC), 2008, pp. 3406-3410.
[4] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in Proc. IEEE International Conference on Communications (ICC), 2009, pp. 15.
[5] A. Min, K. Shin, and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation," IEEE Transactions on Mobile Computing, vol. 10, no. 10, pp. 1434-1447, 2011
[6] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," IEEE Transactions on Wireless Communications, vol. 9, no. 8, pp. 2488-2497, 2010.
[7] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in Proc. 26th IEEE International Conference on Computer Communications (INFOCOM), 2007, pp. 1937-1945.
[8] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in Proc. 31st IEEE International Conference on Computer Communications (IN-FOCOM), 2012, pp. 900-908.
[9] C. S. Hyder, B. Grebur, and L. Xiao,"Defense against spectrum sensing data falsification attacks in cognitive radio networks," in Security and Privacy in Communication Networks. Springer, 2012, pp. 154-

171.
[10] T. Bansal, B. Chen, and P. Sinha, "Malicious User Detection in Cognitive Radio Networks Through Active Transmissions," Tech.
[11] Kiyomichi Araki, Takakazu Satoh and Shinji Miura. "Overview of Elliptic Curve Cryptography", Lecture Notes in Computer Science Vol.1431, 1998.