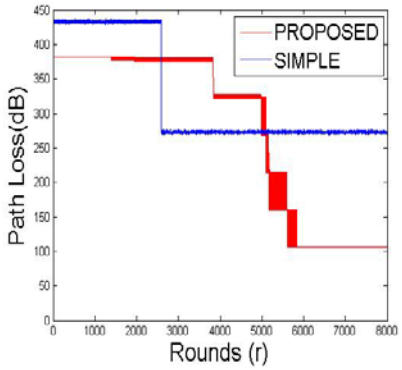

Fig. 18 Network path loss at EO = 0.6

As proposed protocol has extended stability period and extra active nodes have to extra increasing path loss [12, 13]. While comparing the EXISTING protocol with PROPOSED protocol we have concluded 11 % mean improvement has been noticed in respect of EO(initial energy) values at 0.3, 0.4, 0.5, 0.6.

VI. CONCLUSION AND FUTURE SCOPE

In this report, we have proposed a novel protocol for WBANs. The proposed technique has modified TDMA based MAC protocol to reduce the required number of sensors required to successfully monitor the environment of body are network. The proposed technique has been designed and implemented in the MATLAB 2013a with the help of wireless communication toolbox. It has been observed that the proposed technique has significantly reduced the required number of servers. Extensive experiments reveal that the proposed protocol outperforms existing one in terms of residual energy, throughput, network lifetime and path loss. The technique of Reinforcement Learning automatically depicts the situation that how to perform in artificial intelligence. In this report, we have not considered the use of any security attacks on WBANs. Therefore, in near future we will modify proposed technique to handle security attacks.

REFERENCES

[1] S. Mukherjee, K. Dolui and S. K. Datta, "Patient health management system using e-health monitoring architecture", *in Advance Computing Conference (IACC), IEEE,* pp. 400-405, 2014.

[2] X. Sun, J. Su, B. Wang and Q. Liu, "Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks", *International Journal of Security and Its Applications*, Vol. 7, No. 4, 2013.

[3] L. Zhu, Zhen Yang, Meng Li and Dan Liu, "An Efficient Data Aggregation Protocol Concentrated on Data Integrity in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, vol. 2013.

[4] N. Wadhwa, S. Z. Hussain and Rizvi SAM, "A Combined Method for Confidentiality, Integrity, Availability and Authentication (CMCIAA)", *Proceedings of the World Congress on Engineering, WCE*, Vol. 2, 2013, London, U. K.

[5] Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin and Hung-Min Sun 2012, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 4.

[6] Ruoyu Wu, Gail-JoonAhn and Hongxin Hu 2012, "Secure Sharing of Electronic Health Records in Clouds," *8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing*, Collaboratecom 2012 Pittsburgh, PA, United States.

[7] Ed Gelbestein 2011, "Data Integrity-Information Security's Poor Relation", *ISACA Journal*, Vol. 6.

[8] Vladimir Oleshchuk and Rune Fensli, "Remote Patient Monitoring Within a Future 5G Infrastructure," *Wireless Personal Communication, Springer Science*, 2010.

[9] Wenbo He, X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, "iPDA: An Integrity-Protecting Private Data Aggregation Scheme for Wireless Sensor Networks", *IEEE MILCOM*, pp. 1-7, 2008.

[10] H. T. Chu, "A Ubiquitous Warning System for Asthma-Inducement", *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, pp. 186-191, 2006.

[11] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selvao, Y. Wu, L. Fang, Z. He, S. Lin and J. Stankovic, "ALARM-NET:Wireless Sensor Networks for Assisted Living and Residential Monitoring", Technical Report CS-2006-13, Department of Computer Science, University of Virginia, 2006.

[12] Y. J. Zhao, "A MEMS Viscometric Glucose Moni-toring Device", *Proc. of the 13th IEEE International Conference on Solid-State Sensors, Actuators and Microsystems*, Pittsburgh, pp. 1816-1819, 2005.

[13] J. W. P. Ng, B. P. L. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou and G. Z. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)", In Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp"04), Nottingham, U. K., 2004.

[14] T. Park and K. G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", *in ACM Transaction*, 2004.

[15] Arjan Durresi, VamsiParuchuri, RajgopalKannan and Iyengar, "A Lightweight Protocol for Data Integrity in Sensor Networks", *IEEE, ISSNIP*, SS 2004.