based fake packet generation and TTL as 8 while series2 presents the results for total number of transmitted packets with TTL as 4.As it is evident by the results the scheme improves the network energy consumption by decreasing the total number of fake packets generated and transmitted in the network still maintain the traffic uniformity in the network.

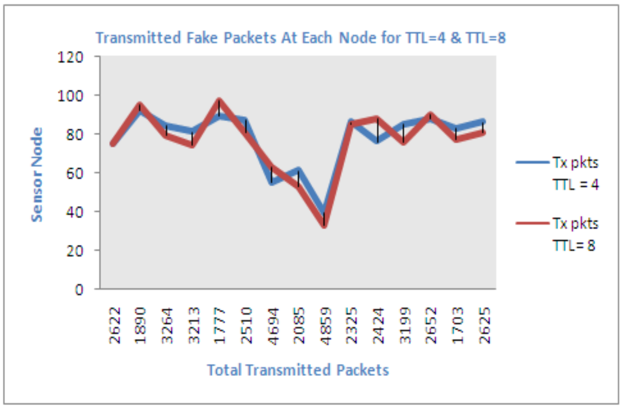

Fig.7. Comparative transmitted packets at each node for different TTL values and without any TTL.

8 Conclusions

The routing structure of a wireless sensor network is tree-based that is rooted at the base station [33]. Thusthe message transmission patterns are highly pronounced in and around the base station. This leads to revelation of location of the base station through traffic volume and directions of messages transmissions. This may prove to be a boon to the adversarymaking it capable of rate monitoring and traffic analysis attacks to locate and destroy the base station that is the central computational point of the entire WSN. The present paper proposed a residual energy based privacy provisioning for WSN .With the aim to countermeasures correlating network traffic to preserve location privacy of a base station that can be revealed in traffic analysis techniques [34]. We introduced residual energy based random fake paths taken by fake packets to confuse an adversary from tracking a message though certain amount of delay is added up to the transmitted packet to a base station. The simulations presented results supporting the proposed residual energy based fake packet generation scheme. The scheme achieved deco-relation comparable to the best possible deco- relation represented by the broadcast, at a fraction of broadcast's messaging cost.

Also these fake packets have a limited lifetime with the TTL value so as to optimize the energy consumption overhead in the network. The idea of fake packet propagation aids significantly in spreading out the communication traffic evenly over the network and obfuscating any paths to the base station with a little delay that too may be utilized for temporal privacy preservation.

9 Future Perspectives

The future prospective for the current research induces the key idea to generate hotspots in the network to trap the adversary [35]. To enhance the deco relation in traffic further local high data sending rate areas are generate, called hot spots, in the network. An adversary may be trapped in those areas and not be able to determine the correct path to the base station. The challenge here is how to create hot spots that are evenly spread out in the network, such that only a minimum (preferably zero) amount of extra communication/coordination among the sensor nodes is needed.

This may be done by letting the nodes that forwarded fake packets earlier have a higher chance to forward fake packets in the future. This way, after a node has forwarded a fake packet to one of its neighboring nodes, it will continue to forward other fake packets to the same neighboring node with higher and higher probability. If an area of nodes receive fake packets, they are more likely to process more and more fake packets in the future. This will turn that area into a hot spot. It is also very easy to destroy current hot spots and reconstruct new hot spots at different places. For example, sensor nodes just reset the value of tickets to 1 when they receive a broadcast message from the base station, and then start to build hot spots from scratch.

A patient attacker can wait at a hot spot until the communication pattern changes. While this will allow the attacker to determine that he was at a fake hot spot, it does not provide any other information about the possible location of the base station. Furthermore, waiting for a long time at a fake hot spot will add more delay to finding the location of the base station.

References:

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci.A survey on Sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham , "Privacy preservation in wireless sensor networks: A state-of-the-art

survey" in Ad Hoc Networks 7 (2009), p. 1501–1514, 2009.

[3] J. Deng, R. Han, and S. Mishra. Security, privacy, and fault tolerance in wireless sensor networks. Artech House, August 2005.

[4] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September 2003.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.

[6] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In ACM WiSe, pages 80–89, 2004.

[7] G. Gaubatz, J.P. Kaps, and B. Sunar. Public key cryptography in sensor networks - revisited. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.

[8] J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 43–52, New York, NY, USA, 2004. ACM Press.

[9] R. Zhang, Y Zhang, and K. Ren,"DP 000b2;ac: Distributed privacy preserving access control in sensor networks", in INFOCOM 2009, IEEE, pp. 1251-1259, April 2009

[10] Perrig et. al. SPINS: Security Protocols for Sensor Networks. Wireless Networks, 8(5):521–534, 2002.

[11] Aysal, T.C.; Barner, K.E.; Sensor Data Cryptography in Wireless Sensor Networks. In IEEE Transactions on Information Forensics and Security, Volume: 3 Issue:2
On page(s): 273 – 289,2008

[12] R. Zhang, Y. Zhang, K. Ren, "DP2AC: Distributed privacy-preserving access control in sensor networks", in proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM 2009), pp.1298–1306, 2009.

[13] Pandurang Kamat, Wenyuan Xu, Wade Trappe, Yanyong Zhang , "Temporal Privacy in Wireless Sensor Networks" in International Conference on Distributed Computing Systems, 2007, ICDCS'07, p. 23-35,27 june 2007.

[14] A. Cerpa and D. Estrin, "ASCENT: Adaptive Self-Configuring Sensor Networks Topologies," in Proceedings of IEEE INFOCOM'02, June2002.

[15] Jing Deng, Richard Han, Shivakant Mishra, "Decorrelating Wireless Sensor Network Traffic To Inhibit Traffic Analysis Attacks" in Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing Systems, vol 2, issue 2, pp. 159-186, April 2006.

[16] W.S. Zhang, C. Wang, T.M. Feng, "GP^2S: generic privacy-preservation solutions for approximate aggregation of sensor data", in proceedings of the Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), Hong Kong, P.R.C., pp.179–184,March 17–21, 2008.

[17] C.Ozturk, Y. Zhang, and W. Trappe. "Source-location privacy in energy-constrained sensor network routing". In SASN'04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004.

[18] Yi Ouyang, Zhengyi Le, Yurong Xu, N. Triandopoulos, Sheng Zhang,J. Ford, and F. Makedon. Providing anonymity in wireless sensor networks. In Pervasive Services, IEEE International Conference on, pages145-148, July 2007.

[19] Yong Xi, L. Schwiebert, and Weisong Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In IEEE International Parallel and Distributed Processing Symposium, Los Alamitos, CA, USA, 2006. IEEE Computer Society.

[20] Jing Deng, Richard Han, and Shivakant Mishra. Intrusion toleranceand anti-traffic analysis strategies for wireless sensor networks. In DSN'04: Proceedings of the 2004 International Conference on Dependable Systems and Networks, pages 637-646, Washington, DC, USA, 2004 IEEE Computer Society.

[21] Celal Ozturk, Yanyong Zhang, and Wade Trappe. Source-location privacy in energy-constrained sensor network routing. In SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor

networks, pages 88-93, New York, NY, USA, 2004. ACM.

[22] Jing Deng, Richard Han, and Shivakant Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. In SECURECOMM '05: Proceedings of the First International Conferenceon Security and Privacy for Emerging Areas in Communications Networks, pages 113-126, Washington, DC, USA, 2005. IEEE Computer Society.

[23] Yong Xi, L. Schwiebert, and Weisong Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In IEEE International Parallel and Distributed Processing Symposium, Los Alamitos,CA, USA, 2006. IEEE Computer Society

[24] P.F. Syverson, D.M. Goldschlag, and M.G. Reed. Anonymous connections and onion routing. In Proceedings of IEEE Symposium on Security and Privacy, 1997, pages 44-54, May 1997.

[25] Y. Xi, L. Schwiebert, W.S. Shi, “Preserving source location privacy in monitoring-based wireless sensor networks”, in: Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), April 2006.

[26] Xiaoyan Hong, Pu Wang, Jiejun Kong, Qunwei Zheng, and jun Liu. Elective probabilistic approach protecting sensor traffic. In Military Communications Conference, 2005. MILCOM 2005. IEEE, volume 1,pages 169-175, Oct. 2005.

[27] Jing Deng, Richard Han and Shivakant Mishra : Defending Against Traffic Analysis Attacks in Wireless SensoNetworks.www.usenix.org/event/sec04/tech/wips/posters/05-deng-wireless.pdf

[28] J. Luo, and J.- P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks", Proceedings IEEE INFOCOM'05, vol. 3, Miami, FL, Mar. 2005, pp. 1735-1746.

[29] Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks", in the Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, San Francisco CA, April 2001, pp. 2009-1015.

[30] http://castalia.npc.nicta.com.au/

[31] Y. Jian, S.G. Chen, Z. Zhang, L. Zhang, ”Protecting receiver-location privacy in wireless sensor networks”, in proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), pp. 1955–1963, May 2007.

[32] Z. Cheng and W. Heinzelman, “Flooding Strategy for Target Discovery in Wireless Networks,” in proceedings of the Sixth ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2003), 2003.

[33] Haodong Wang, Bo Sheng, and Qun Li. Privacy-aware routing in sensor networks. Computer Networks,

[34] P. kamat, Y. Zhang, W trappe, and C. Ozturk,. Enhancing source-location privacy in sensor network routing. in Proceedings. 25th IEEE International Conference on Distributed Computing Systems, 2005.ICDCS 2005, pp. 599-608, june 2005.

[35] R.A. Shaikh, H. Jameel, B.J. d'Auriol, Sungyoung Lee, Young-Jae Song,and Heejo Lee. Network Level Privacy for Wireless Sensor Networks. InFourth International Conference on Information Assurance and Security, 2008, pages 261-266, Sept. 2008.

BIOGRAPHIES

Ms. Manjusha Pandey
is pursuing her Ph.D. from Indian Institute of Information Technology, Allahabad, India in Information and Technology, has done her M. Tech in Computer Science.

Her research interest areas include Wireless Sensor Networks, Privacy in Wireless Communication, Privacy and security in Digital & Mobile Communication, Signal Processing and Vehicular Technology.

I

Dr. Shekhar Verma
Received his Ph.D. degree from University, Varanasi, India in Computer Science and Engg. He is Associate Professor in Information Technology at

Indian Institute of Information Technology, Allahabad, India. His research interest areas are Computer Networks, Wireless Sensor Networks, Vehicular Technology, Cryptography, Information and Network Security.