ISSN NO. 2456-3129

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

Statistical Steganography Technique for Minimizing MSE in Wireless Sensor Networks

Reetika Sodhi, Anshul Sharma
Department of Electronics and Communication Engineering
Chandigarh University, Punjab, India-140413
sodhireetika@gmail.com, er.sharma.anshul@gmail.com

Abstract— As there are many threats to the security in various application areas where wireless sensor networks are deployed. These threats causes a compromise to the security thus causing the network to lose its important data such as key, secret message etc. So there is a need for making a security technique which could prevent the attacks by third party or intruder over the network. For securing the data various techniques are being used such as cryptography, steganography, watermarking and many more. Steganography is best suited for securing data as in this method the third party is not aware of the security being applied as compared with the cryptography in which the intruder knows the fact that the data is being secured using an algorithm. In this paper a steganography technique for hiding data is used and is applied over sensor nodes to test whether it is suitable to be applied over sensor network. The parameters such as MSE, PSNR, AMD, energy consumption, network lifetime are calculated. MSE, network lifetime and energy consumption are compared with the already existing Turner's technique. The network lifetime for three techniques are compared- the proposed technique, already existing technique and direct transmission network i.e. network without security and it is concluded that proposed technique works better in terms of security as well as network lifetime in comparison with the already existing technique.

Keywords- cryptography ;WSN; steganography

1. INTRODUCTION

With the arrival of Wireless sensor networks in various applications, it has become crucial to protect the sensor data communicated over wireless channel. A latest and different evolving technique which consist of an enormous amount of tiny nodes or devices used for observing changes, making procedure to sort it out and then transmitting information to interact with the actual world is termed as wireless sensor networks i.e. nodes which are wirelessly connected to each other in an environment[10].The information in WSN are transmitted through RF(radio frequency) connection so the errors may get generated due to many factors such as intervention, alterations etc. [2].These nodes communicate and transfer information between them. Sensors used by these nodes are of many kinds which are used for observing and examining the changes in temperature, passage of traffic, detection of specific entity, speed with which a body is moving its direction, pressure conditions etc. are seismic, thermal, infrared, acoustic and radar. There are numerous applications which are encountered by these wireless nodes which are as used for military purpose, health, ecological and some industrial applications. In military area WSN can be used as a tremendous means to secure and to get information regarding various parameters such as to monitor poisonous gases in particular area that may affect the health of military personals, to monitor mining activities, intruder recognition, boundary observation etc. There are numerous attacks encountered over WSN by an intruder or an attacker such as Denial of service attacks, jamming attacks, Sybil attacks, sinkhole attack and many others [4]. So providing security to data which is transferring between these nodes is concern in wireless nodes and all steganography and cryptography algorithms cannot be used directly for wireless sensor nodes because WSN are resource limited due to restrained power supply, battery life, area of network [11]. The restrictions and limitations of WSN such as limited power, limited processing requirement, low battery life and challenging distribution of nodes makes it tougher as compared to the traditional network systems, but the ability to design safety solutions into these networks from beginning as they are in their initial research phase. Moreover, we may make use of the size, physical qualities of location. Eventually, the distinctive features of wireless sensor environment permit the novel securities which are not accessible in traditional

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

systems [5]. With the growing infrastructure in WSN and its use in variety of applications there is a need of secure wireless channel that can be achieved with any traditional data encryption technique. In the present scenario of network steganography it is important to hide the information in a form such that the communication cannot be detected using advanced statistical approach of steganalysis. But WSN being a energy constraint, self-configurable network, the traditional security technique developed for wireless network that cannot be applied directly over WSN. Hence there is a need of energy efficient low complexity security technique for WSN.

The sensor networks deployed in regions like Military establishments always have to carry sensitive information about the region/area under surveillance. To secure the network, one can apply cryptographic concept, but cryptography has two problems. First is that the cryptography is detectable. In military scenario the priority is not only about securing the communication but also on its undetectability. A stream of garbage looking cipher text can immediately send the idea of concealed communication. Secondly cryptography requires additional processing cost. This can lead to increased energy consumption because of computational loads on the system.

Whereas steganography is a type of symmetric key security mechanism as the same key is known to both sender and recipient. So steganography techniques have proved to be efficient techniques for security. Moreover in terms of energy utilization asymmetric are not lightweight and they affect battery life. Although, with cryptography, one can secure the communication between multiple sensors and a sink but the algorithms for encryption and decryption are quite complicated and lengthy hence it needs a large amount of processing power which eventually affects battery life. Also cryptography is not feasible for an ever changing scenario of wireless sensor due to high variance in node replacement or addition of worm out or damaged nodes without human interaction. Hence steganography techniques can provide to be imminent for implementation over WSN. Thus, there is a need of steganography for this communication. This paper presents a steganography technique which caters special needs of wireless sensor networks. The rest paper is arranged in a particular pattern as described:

Section II presents the related work on steganography.
Section III describes the routing methods for WSN.
Section IV indicates the proposed work.
Section V defines the result section comparing our technique ith other existing native steganography techniques.
In Section VI conclusion is attained.

2. RELATED WORK

This segment provides the work which has been done in the field of steganography. Singh et. al [31] presented a method called as WRHT which detects any unintended node in a particular network and at the same time transfers the secret data to the recipient node by using the central node.This method also makes use of delay per round because the illegitimate path is more larger than the legitimate path and this idea is utilized to make an idea of the path which is corrupted. Karlof et. al [32] proposes the TinySec named technique for securing data over wireless linkage which comes out to be very energy effective.It is very proficient technique to be used in scenario where there is resource restraint environment.Sedighi et.al [9] proposed a method which is used to hide information such as to reduce the deformations. The proposed algorithm makes use of the cover image which is centred on locally estimated multivariate Gaussian method. This method works to reduce the detection of secret data by the steganalysis tests. Variance is calculated so that similarity between the secret data and cover is generated so that distortions are reduced. Ahani et.al [10] proposes a steganographic method which uses audio steganography concept. The cover is in the form of speech to hide the data and to minimize the detection of stego text from original message. The DWT is used to divide the elevated frequencies from low pitched ones. Hiding of data over non-zero values in the sparse matrix is used to reduce the deformation of data. The parameters such as PESQ, undetectability is measured which compares the quality of speech signal which is original and the one which is transmitted over the system along with other parameters such as SNR to test the quality of stego signal transmitted. Szczypiorski et al. [18] discusses the network steganographic technique based on transmitting data over Wi-fi. The other techniques which are based on 802.11 are discussed and they are analysed and evaluated and categorise them as ―good algorithms and the algorithms which are bad or ugly in terms of their performance. The paper defines the idea of ―moving observer which considers the observer to be in motion i.e. the intruder or any observation point making motion towards or away from stego-message. Collins et al. [20] looked into the prevalent strategies for traditional system steganography, depicting the point by point operations and resultant difficulties required in implanting

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

information in the system transport area. They likewise considered the different digital risk vectors of system steganography and point out the significant contrasts between traditional system steganography and the broadly known end-point mixed media installing strategies, which concentrate only on static information alteration for information covering up. They additionally presented an altogether new system information concealing strategy, which they allude to as ongoing system information steganography. At last they gave the preparation to this key change of clandestine system information implanting by shaping a fundamental structure for continuous system information operations that will open the way for considerably facilitate propels in PC system security.

3. ROUTING METHODS FOR WSN

There are different protocols designed for WSN which are as follows:

Direct communication: In this type of protocol the data is send directly from nodes to centre i.e. base station. The distance between nodes and base is important factor in this type of communication as the distance is inverse relation with the battery life. If the distance is more, more energy will be utilised to send data from nodes to base station and hence more energy will be consumed and system will run out of energy in short duration of time which is major concern in this type of communication.

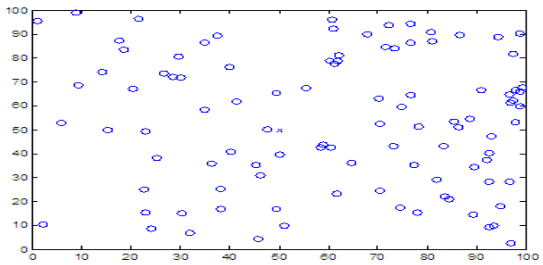

Figure 1. Wireless sensor nodes deployed

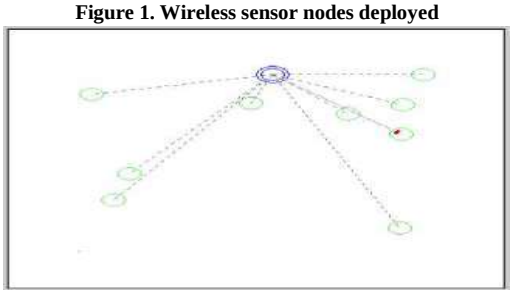

Figure 2. Transmission from nodes to centralised base station

Cluster based protocols: in this type of transmission there are multiple base stations for different groups of nodes and the nodes transfer data to its own base station which further transmits it to the main station for being accessed by the one who is intended receiver. The distance between the nodes and their constellation station is reduced and hence as distance has inverse relation with the battery life in WSN so a lot of energy is saved.

LEACH: It is considered as self-establishing grouping method. In this the energy is disseminated on random basis between the nodes. Different clusters are formed and each node sends its data to its clusters base station which is known as the head of cluster .The clusters keep on changing randomly so no single node should lose all its energy.

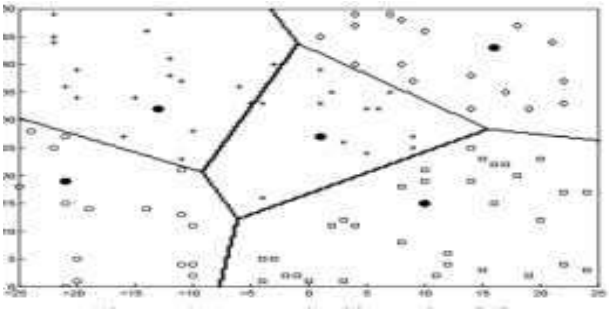

Figure 3. Clustering in LEACH

PEGASIS: It is considered to be an improved version of the LEACH. In this the data is transmitted by forming a string of nodes from the nodes to base station so that each node transmits data to its adjacent node. For transmission from node to base station one of node out of all is selected.

Stable election protocol: As the name specifies this type of protocol elects a particular node to act as head of clusters to receive data from the rest of nodes depending on their energies however the nodes are selected randomly. The lifetime of nodes is better in this type of protocol.

HCR protocol: This is hierarchical structure self-establish the nodes into clusters. It is energy efficient method of nodes. In this each node sends data to its head which then transmits data to the main head i.e. base station.

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

4. PROPOSED WORK

In the proposed work, a steganography algorithm is developed for text as cover and secret data in which the cover is generated by using secret data from sensors and calculating cover through statistical parameters. This cover is similar to the secret data so that there is no suspicion of secret data embedded in cover media. The data stream is then converted into frames and then the energy of each frame is calculated and compared with the threshold value. If energy >threshold value then the non-zero LSB is used for embedding data. The parameters such as AMD, PSNR, MSE and energy and network lifetime are calculated for the proposed algorithm. The parameter of network lifetime is then compared with the direct data transmission technique in which the data is transmitted without secure communication.

Further, Turner‘s work developed a distributed Steganographic computational framework of wireless sensor networks for communicating secret message between nodes and sink. Since the Turner‘s work is using sensor networks to distributive processing of steganography the energy consumption and network lifetime in processing information is evaluated and compared with the proposed algorithm.

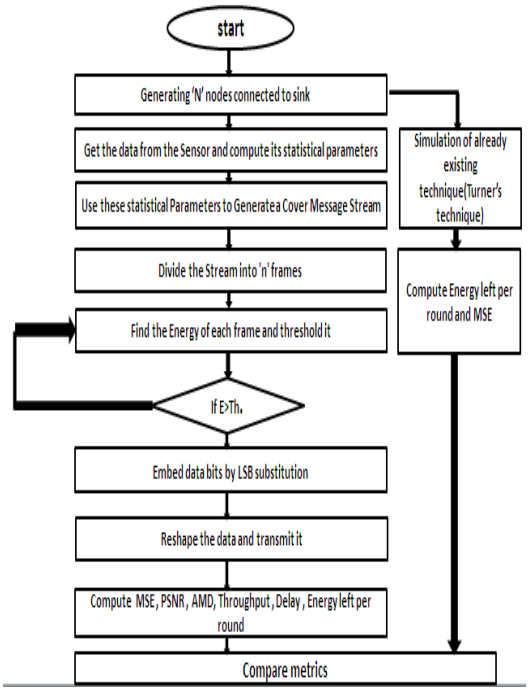

Figure 4. Flow chart for proposed algorithm

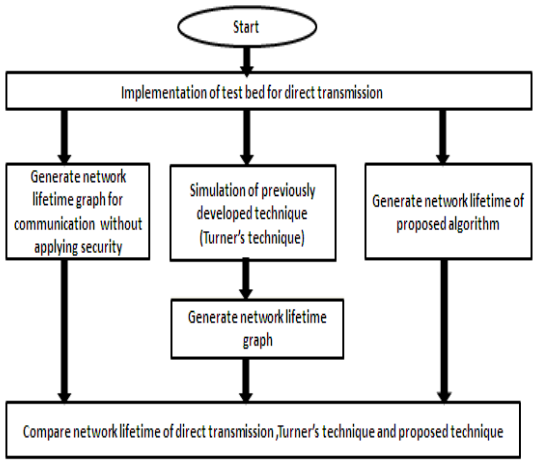

Figure 5. Methodology to generate network lifetime

5. RESULTS AND DISCUSSIONS

The system is simulated in MATLAB by developing a traffic generator for Wireless Sensor Network. It generates the traffic which goes to sink. The packet is transmitted through the sources (sensor nodes) to sink (base station) in 100 rounds of simulation. In each round a packet of 16 bytes is taken as cover data to store 1 byte of original information. Parameters like Mean squared error (MSE), Peak Signal-to-noise ratio (PSNR), and Absolute Mean Difference (AMD), are evaluated to predict the Detectability of the Signal. Based on the table I, it is seen that the developed algorithm for data security has less MSE than the already existing algorithm which means that the proposed algorithm is more secure than the existing algorithm. The absolute mean difference of the developed algorithm comes out to be 36.3981, which means that the system is highly correlated with original cover. Thus, it is highly undetectable. The Mean Squared Error is very low which represents that the system has high capacity. This high capacity can be utilized to transmit more data in single packet, although this concept is not tested in this case. Figure 6 shows the Delay per round in the Wireless Sensor Network. The scenario used a cover packet of 16 bytes to hide 1 byte data. This value of bytes is very small but on general, a Wi-Fi network uses an MTU size of 1500 bytes and thus these 16 bytes can be taken from any arbitrary block. This will not affect the system throughput or delay in any sense as showcased from the graph presented above. Figure 7 depicts the throughput (bps) per round for the Wireless Sensor network under consideration. The parameters of throughput clearly show that the throughput is not affected by packet size.

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

These graphs show the overall performance of the system while hiding the data using steganographic techniques.

Figure 8 and 9 shows the Graph of Mean Squared Error, MSE is the error computed between the original cover signal and the computed stego signal. It is clearly visible that the algorithm utilizes sparse matrix based steganography to minimize the detectability, the mean squared error is very less. Figure 10 shows the Graph of Absolute Mean Difference for proposed algorithm. The Absolute mean difference shows the statistical difference between the true data and cover data. It is clear that AMD is very low in proposed algorithm. The AMD shows the degree of camouflage in the Steganographic systems. Figure 11 shows the Graphs of Peak Signal to Noise Ratio. Again, since the Peak signal to noise ratio is a degree of error, it is highest in maximum case (Infinity) as MSE touched 0 several times during simulation and it has inverse dependence on MSE. It is clearly shown that the energy efficiency for sharing secret information in proposed algorithm is much better compared to Turner‘s Technique. The reason for this is that in Turner‘s Technique, the sensor networks is used as processing units while in other techniques used here the processing load at sensor end is minimized to effectively preserve the energy.

TABLE I. The parametric result

Comparison of parameter for proposed algorithm and Turner’s technique	
Technique	***MSE***
Proposed algorithm	0.026875
Turner’s technique	0.20875

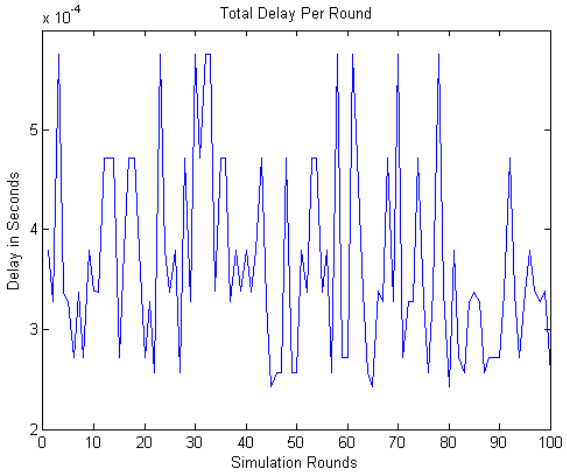

Figure 6. Delay per round in the Wireless Sensor Network

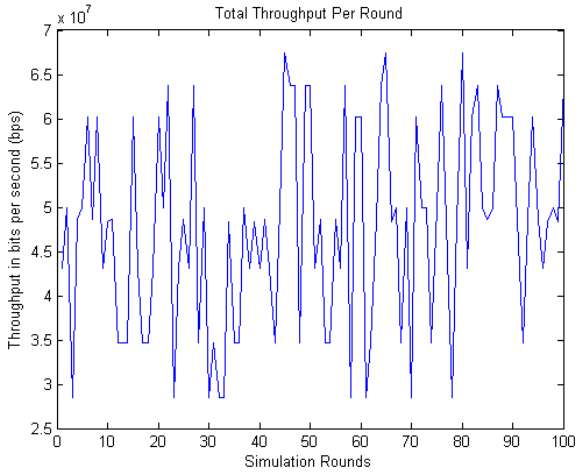

Figure 7. Total throughput per round in wireless sensor node

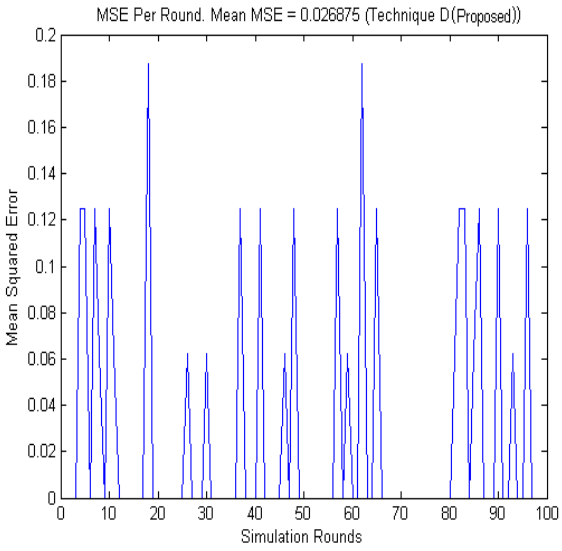

Figure 8. MSE for developed algorithm

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

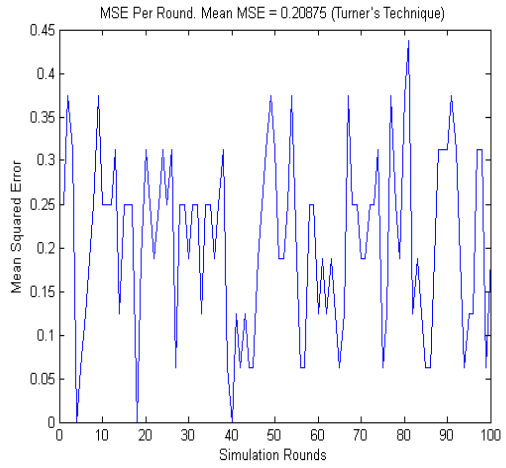

Figure 9. MSE for Turner's technique

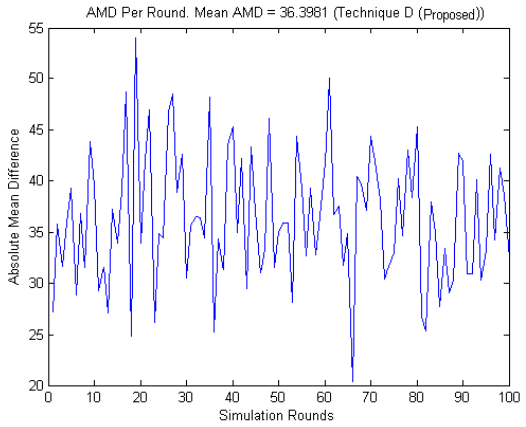

Figure 10. Absolute Mean difference between cover and original data for proposed algorithm

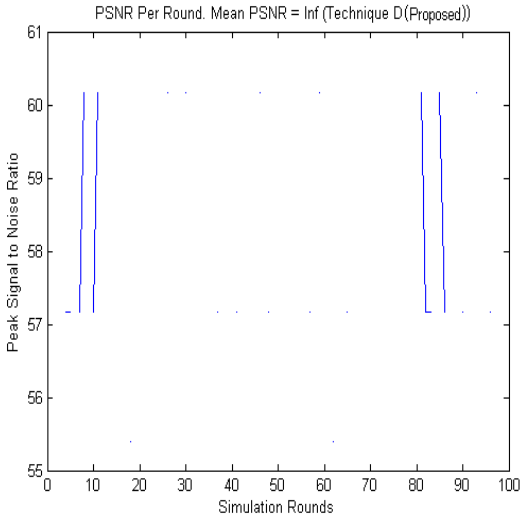

Figure 11. PSNR for developed algorithm

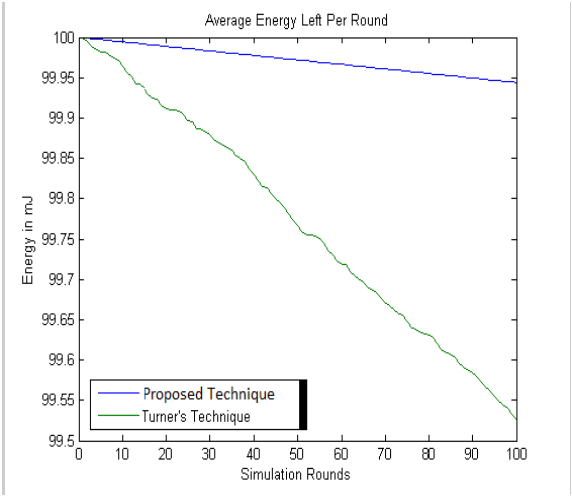

Figure 12. Energy Comparison of for proposed algorithm and Turner's Technique

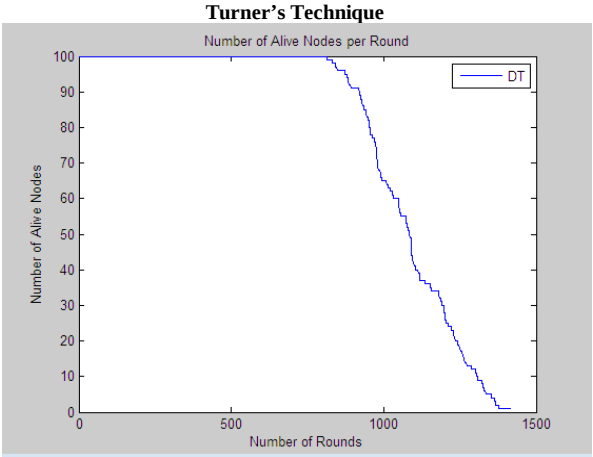

Figure 13. Network lifetime of direct transmission protocol

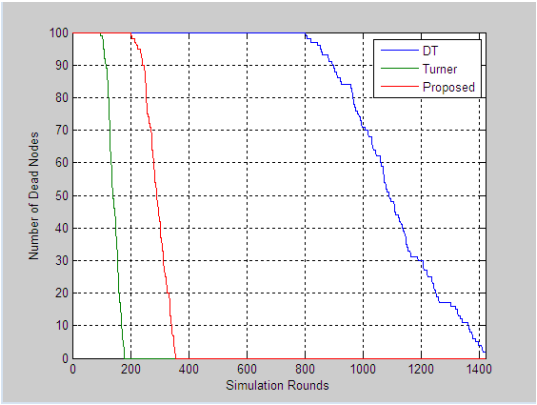

Figure 14. Comparison of Network lifetime of direct transmission, Turner's and Proposed algorithm

IJEPAS

International Journal of Engineering, Pure and Applied Sciences,
Vol. 2, No. 2, June-2017

6. CONCLUSION

In this paper, a new algorithm for network steganography is developed. The network lifetime for direct transmission algorithm is compared with turner's technique as well as direct transmission data transmission network without secure communication. In terms of network lifetime the direct transmission works out to be best as the nodes for proposed algorithm turns out of energy earlier than the direct transmission. But if we consider it from security point of view the proposed algorithm is also better in terms of security as the MSE for proposed algorithm is less as compared with the already existing algorithm. Also the proposed algorithm provides high security for transmission of data against direct transmission which is highly unsecure . In the future work, other advanced techniques can be used to exploit the low MSE and high PSNR of proposed algorithm to embed more data using high capacity embedding to evaluate the system's performance.

REFERNCES

[1] K.Jones,A.Wadaa, S.Olariu, L. Wilson, and M.Eltoweissy, "Towards a new paradigm for securing wireless sensor networks,". In Proceedings of the workshop on New security paradigms pp. 115-121, August 2003.

[2] D. Boyle, and T. Newe, "Security protocols for use with wireless sensor networks: A survey of security architectures," In Wireless and Mobile Communications, , IEEE. ICWMC'07. Third International Conference ,pp. 54-54, March 2007.

[3] C. Karlof, and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, 1(2), pp.293-315, 2003.

[4] A.Perrig, J. Stankovic, and D.Wagner, "Security in wireless sensor networks. Communications of the ACM," 47(6), pp.53-57, 2004.

[5] H.Delfs, and H.Knebl, "Symmetric-key encryption. In Introduction to Cryptography,"Springer Berlin Heidelberg, pp. 11-31, 2007.

[6] A.S Panwar, "Asymmetric Key Cryptography,".Available at SSRN 2380622, 2014.

[7] G.Gaubatz, J.P .Kaps, E. Ozturk, and B.Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks in Pervasive Computing and Communications Workshops PerCom 2005 Workshops. Third IEEE International Conference, IEEE, pp. 146-150, March 2005.

[8] A.S.K. Pathan, H.W.Lee, and C.S. Hong, "Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology,"ICACT, The 8th International Conference, IEEE, Vol. 2, pp. 6-pp, February 2006.

[9] D.Martins, and H.Guyennet, "Steganography in mac layers of 802.15. 4 protocol for securing wireless sensor networks," In Multimedia Information Networking and Security (MINES), International Conference, IEEE, pp. 824-828), November 2010.

[10] M.Younis, K.Akkaya, M.Eltoweissy, and A.Wadaa, "On handling QoS traffic in wireless sensor networks. In System Sciences, Proceedings of the 37th Annual Hawaii International Conference ," IEEE ,pp. 10-pp, January 2004..

[11] A.A Baradaran, "The applications of wireless sensor networks in military environments. Scientific Journal of Review," 4(4), pp.55-70, 2015.

[12] I.F. Akyildiz, and I.H.Kasimoglu, "Wireless sensor and actor networks: research challenges,"Ad hoc networks, 2(4), pp.351-367, 2004.

[13] J.Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography,".arXiv preprint arXiv:1207.0917, 2012.

[14] Z.Li, X.Sun, B. Wang, and X.Wang, " A steganography scheme in P2P network. In Intelligent Information Hiding and Multimedia Signal Processing," IEEE, IIHMSP'08 International Conference , pp. 20-24, August 2008.

[15] B.Jankowski, W. Mazurczyk, and K.Szczypiorski, "Information hiding using improper frame padding. In Telecommunications Network Strategy and Planning Symposium (NETWORKS),"14th International, IEEE, pp. 1-6, September 2010.

[16] W.Mazurczyk, M.Smolarczyk, and K.Szczypiorski, "Retransmission steganography and its detection," Soft Computing, 15(3), pp.505-515, 2011.

[17] G.Fisk, M.Fisk, C.Papadopoulos, and J.Neil, "Eliminating steganography in Internet traffic with active wardens In Information Hiding," Springer Berlin Heidelberg, pp. 18-35, October 2002.

[18] S.Ahani, S.Ghaemmaghami, and Z.J.Wang, "A sparse representation-based wavelet domain

speech steganography method. Audio, Speech, and Language Processing, IEEE/ACM Transactions on," 23(1), pp.80-91, 2015.

[19] V.Sedighi, R.Cogranne, and J.Fridrich, "Content-Adaptive Steganography by Minimizing Statistical Detectability. Information Forensics and Security," IEEE Transactions , 11(2), pp.221-234, 2016.

[20] X.Niu, J.Sun, and H.Li, " Network steganography based on traffic behavior in dynamically changing wireless sensor networks in Communications (ICC),"IEEE International Conference, pp. 7304-7309, June 2015.

[21] W. Fraczek, and K.Szczypiorski, "Steg Blocks: Ensuring Perfect Undetectability of Network Steganography. In Availability, Reliability and Security (ARES),"10th International Conference, pp. 436-441 ,August 2015.

[22] A.S.Nair, A.Sur, and S.Nandi, "Detection of packet length based network steganography," Multimedia Information Networking and Security (MINES),International Conference ,IEEE.pp. 574-578, November 2010.

[23] A.S.Nair, A .Kumar, A. Sur, and S.Nandi, "Length based network steganography using UDP protocol," Communication Software and Networks (ICCSN), IEEE 3rd International Conference, pp. 726-730, May 2011.

[24] W.Mazurczyk, K. Szczypiorski, and B.Jankowski, "Towards steganography detection through network traffic visualisation," Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 4th International Confress ,pp. 947-954, October 2012.

[25] S.Grabski, and k.Szczypiorski, " Network steganalysis: Detection of steganography in IEEE 802.11 wireless networks," Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),5th International Congress ,pp. 13-19, September 2013.

[26] O.I. Abdullaziz, V.T.Goh, H.C. Ling, and K.Wong, "Network packet payload parity based steganography. In Sustainable Utilization and Development in Engineering and Technology (CSUDET),"IEEE Conference ,pp. 56-59, May 2013.

[27] K.Szczypiorski, A.Janicki, and S.Wendzel, "The Good, The Bad And The Ugly": Evaluation of Wi-Fi Steganography," arXiv preprint arXiv:1508.04978, 2015.

[28] R. Holloway, and R.Beyah, "Covert DCF: A DCF-based covert timing channel in 802.11 networks,"Master of science thesis, Georgia State University, 2011.

[29] C.Turner, "A steganographic computational paradigm for wireless sensor networks," In Proceedings of the 6th international conference on Innovations in information technology , IEEE Press , pp. 270-274, December 2009.

[30] Lee, S.H., Lee, S., Song, H. and Lee, H.S., 2009, October. Wireless sensor network design for tactical military applications: remote large-scale environments. In MILCOM 2009-2009 IEEE Military Communications Conference (pp. 1-7). IEEE.

[31] R.Singh,J.Singh and R.Singh,2016,August.WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks.Mobile Information Systems Volume 2016 .