International Journal of Research in Engineering, Science and Management
Volume-1, Issue-10, October-2018
www.ijresm.com | ISSN (Online): 2581-5792

Localisation in WSN & Security: A Survey

Ruchi[1], Deepti Ahlawat[2]
[1]*M. Tech. Scholar, Department of ECE, N.C. College of Engineering, Panipat, India*
[2]*Assistant Professor, Department of ECE, N.C. College of Engineering, Panipat, India*

***Abstract*—Wireless sensor network is fastly growing network used in surveillance, military, and other emergency applications. It provides a very fast and low cost data transmission, but due to battery constraint in sensor nodes used to collect or transmit the information, their use are limited. To locate the position of unknown sensors for continuous communication, a lot of work and algorithms are developed but some are very computational complex and some are based on bio inspired algorithm, though non heuristic algorithm and heuristic algorithms are iterative methods yet bio inspired algorithms are found more attractive because of large researcher community and less computational complexity compared to others like TSA, RSSI etc.**

***Index Terms*—dynamic technique, localization, communication**

I. Introduction

A. Overview of Wireless Sensor Networks

The current innovative change in the fields of wireless communication has made conceivable the improvement of ease, low power, and multi-practical sensors that are little in size and communication over short distances. A wireless sensor technique is involved distinctive sensor nodes, little in measure, battery fueled gadgets that can convey and figure signals with different nodes. These days, intelligent sensor networks are used in huge numbers to give chance to checking and controlling homes, urban communities and the environment. In expansion, they have an extensive variety of utilizations in giving new innovation to surveillance, defense field. Sensors joined into machinery, structures and the conditions are joined with the powerful transmission of detected information that can offer tremendous advantages to guild. A sensor technique is a foundation comprise of detecting, registering, and communication components that gives an administrator the ability to instrument, watch, also, respond to occasions and wonders in a predefined environment. A wireless sensor technique (WSN) contains various passage (or \base station") that can pass information with various sensors nodes by means of a wireless association. Information accumulated by the node is compacted and sent to the base station straightforwardly or in the event that required, it utilizes different nodes to exchange information to the base station. The information which is exchanged, at that point used by base station link.

The elements of a WSN include: Dynamic technique topology, heterogeneity of nodes, extensive size of node organization, nodes capacity to oppose cruel ecological conditions, nodes should keep running under extremely strict vitality requirements and ought to perform detecting and information handling functionalities. The communication plot is many-to-one (information got together at a base station) instead of shared.

B. Localization in Wireless Sensor Networks

Research about localization of sensor nodes in wireless sensor networks has turned out to be dynamic since most recent couple of years and much research has just been finished for different application around this field. This part will give an unmistakable thought regarding significance of localization, distinctive methods that are now existing to discover to position of sensor nodes.

1) Importance of localization

Sensor location is extremely significant in a sensor technique since numerous application for example, observing woodlands or potentially handle, where a lot of sensor nodes are put. A proficient localization calculation can decide the exact position directions of gadgets or nodes utilizing the information accessible from sensor nodes. What's more, location based directing convention can spare and use huge sum of vitality by evacuating the requirement for course finding and enhance the location for application. In wireless sensor networks, the issue of deciding the location of localized sensor nodes is alluded to as localization. There are diverse situations where impediment expect an essential part is at surveillance all through strikes, military provisions to spot targets, movement checking and a part of individuals more provision .On imagining about the scenes after each cataclysm where houses are hurt and people are hurt or killed or stalled out some place in the demolish, the need of making sense of the impacted people and spots must be done to any detriment. To achieve the goal of putting the people or things, there are various networks reaching out from physically recognizing the people by the crisis treatment men to using present day developments. From late disasters, we can comprehend that if we had high inventive devices, at that point abused individuals may have been protected immediately. In this kind of circumstance, if all people and profitable articles are furnished with wearable contraptions like Zigbee 802.15 and practically identical devices from the therapeutic beacon men or mostly controlled contraptions, at that point they may structure a wireless extemporaneous system as exhibited in Fig.1. Afterward, every sensor focus point can apply a position estimation figuring with the goal that all gadgets can know there and others region. Around at that point, the emergency drug men will reasonably keep running over the zone of the general population or thing to secure. Additionally, the individuals

require help correspondingly think about the zones around them and help supervising them to escape from the peril. The Localization issue offers two indispensable issues. Firstly, portraying a bearing technique. Second, which is the all the more indeed testing, is the issue of determining the partition between sensors (the going problem).Solution to these issues could be refined using any of the systems beneath portrayed.

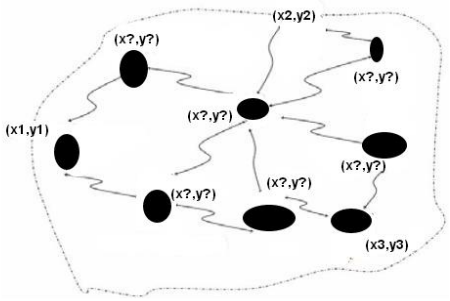

Fig. 1. Localization requirement

This location portrays the significance of localization in numerous applications, where a substantial number of sensor nodes are set. Localization is utilized to discover the position of these nodes. Head and shoulders shots of authors that appear at the end of our papers.

II. Literature Survey

S. Goyal et.al [1] described the Meta heuristic optimization algorithm known as bat algorithm in order to evaluate the precision of node localization problem in wireless sensor networks. Meanwhile the existing bat algorithm has also been modified by using the bacterial foraging strategies of bacterial foraging optimization algorithm. Compared with the existing bat algorithm, the proposed modified bat algorithm is shown through simulations to perform constantly better not only in increasing localization success ratios and fast convergence speed but also enhance its robustness. J. Cao et.al [2] discussed the localization method based on improved particle swarm optimization algorithm and Quasi-Newton algorithm, which obtains the approximate solutions through PSO, and then makes local search and gets the final results by BFGS. The simulation shows that the algorithm can effectively improve the localization accuracy.

X. Zhang et.al [3] proposed an accurate and simply scheme of mobile-assisted localization for the wireless channel loss model unknown environment in WSN. One localization algorithm is implemented using the particle swarm optimization (PSO). For improved the localization effect, the path planning strategy based on a kind of grid scan is suggested. To comparative evaluation of the proposed localization algorithm, the results of the localization algorithm based on multilateration in the same conditions are also provided.

P. H. Namin et.al [4] presented a two-step distance-based algorithm to sensor network localization carried out in a centralized architecture. The first phase of the algorithm utilizes an improved version of the DV distance method used to provide coarse position estimates for all the nodes. During the second phase, Particle Swarm Optimization (PSO) is performed to fine tune and obtain accurate estimation of the locations. In the second phase, several techniques are also used to address the main problems of localization such as flip ambiguity, collective translation and error propagation. To evaluate the performance of the algorithm, numerical simulations were performed and the results were compared with similar distance-based methods, namely one-phase simulated annealing (SA), trilateration and simulated annealing (TSA) and semi-definite programming localization (SDP). S.R. Sujatha et.al [5] proposed DE algorithm is used to along with DWPSO to obtain the better localization accuracy. Simulation results indicate that this method provides smaller localization error, higher localization accuracy and better stability performance in DWPSO compared to LM.

R. Rajkumar et.al [6] incorporated GWO algorithm is to spot the correct position of unknown nodes, so as to handle the node localization problem. The proposed work is implemented using MATLAB 8.2 whereas nodes are deployed in a random location within the desired network area. The parameters like computation time, percentage of localized node, and minimum localization error measures are utilized to analyses the potency of GWO rule with other variants of met heuristics algorithms such as particle swarm optimization (PSO) and modified bat algorithm (MBA). The observed results convey that the GWO provides promising results compared to the PSO and MBA in terms of the quick convergence rate and success rate.

D.Li et.al [7] proposed a distributed two phase PSO algorithm to solve the flp ambiguity problem, and improve the efficiency and precision. In this work, the initial search space is defined by bounding box method and a refinement phase is put forward to correct the error due to flip ambiguity. Moreover, the unknown nodes which only have two references or three near-collinear references are tried to be localized in our research. Simulation results indicate that the proposed distributed localization algorithm is superior to the previous algorithms.

S. Singh et.al [8] proposed the application of different migration variants of Biogeography-Based Optimization (BBO) algorithms and Particle Swarm Optimization (PSO) for distributed optimal localization of randomly deployed sensors. Biogeography is collective learning of geographical allotment of biological organisms. BBO has a new inclusive vigor based on the science of biogeography and employs migration operator to share information between different habitats, i.e., problem solution. PSO models had only fast convergence but less mature. An investigation on distributed iterative localization is presented in this paper. Here the nodes that get localized in iteration act as anchor node. A comparison of the performance of PSO and different migration variants of BBO in terms of number of nodes localized, localization accuracy and computation time is presented.

M. Milhoubi et.al [9] proposed an effective Bat algorithm for the node localization problem, the effectiveness of which is

based on the adaptation of velocity of the Bats by hybridization, with Doppler effect for improving the performance, aptly termed Dopeffbat. Hence, Dopeffbat

Computes (through evolution) the nodes' positions iteratively through the Euclidian distance as fitness. Deploying this algorithm on a large WSN with hundreds of sensors demonstrates decent performance in terms of node localization. Moreover, the Dopeffbat parameters are simulated and interpreted in different scenarios of simulation; in addition, a comparative study was performed to further demonstrate the performance of the proposed algorithm, and the simulation results prove that Dopeffbat has a high convergence rate and greater precision compared with the original Bat algorithm and particle swarm optimization (PSO) algorithms. S. Nasrani et.a al [10] achieved the efficient localization is by the implementation of membrane computing. The optimized location a target node has been determined by the use of membrane computing. The simulation results reveal that the localization error has been minimized by the use of efficient routing schemes along with membrane computing.

Belkadi, M. et al [11] used secured direct diffusion method for energy consumption reduction and made the direct diffusion protocol safe from attackers. Directed Diffusion is a data centric protocols commonly used in wireless sensor networks. It consists of several elements: interests, gradients, data messages and reinforcements (positive and negative). An interest is a request, in which it specifies the desired data, sent by the base station (sink node) to the sensor nodes gradient is a response link to the neighbor from which the interest was received. Therefore, using the interest and gradients, routes are established between sensor nodes and sink node. Several routes can be set so that one of them is selected according to the rate. Data messages are events generated by one or more sensor nodes in response to requests sent by the base station. To secure it key base security management is used and it used three keys rather than four different keys used by LEAP security protocol which was used by author. The energy consumption is improved in case of secure direct diffusion protocol but no information about security is provided at the end. Julie, E. G. et al [12] improved packet delivery ratio, average end-to-end delay and normalized routing overhead by using opportunistic routing. Markov decision Process is used by the author to determine the time slot for transmission so that data loss is minimum. The proposed work is shown in figure 2.

The Fig. 2 shows the architectural diagram of the proposed protocol. Multicasting with Opportunistic Routing determines the best path. Packets are authenticated using null keys before transmission. Markov Decision based Adaptive Scheduling decides on the time slot to transmit the authenticated packets. Although MDP is very good algorithm for dynamic decisions but it is very complex and from sensor point of views, is also very energy consuming even some researchers have used it in their work to minimize the energy consumption of sensor nodes.

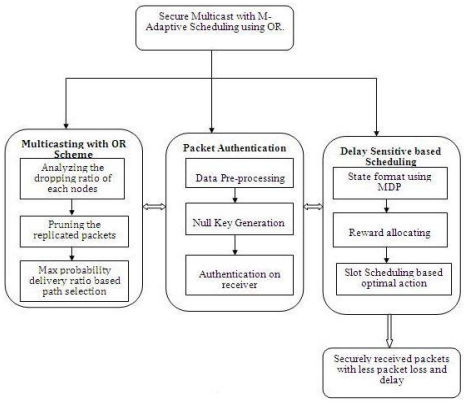

Fig. 2. Architectural Diagram

A Paper by Daniluk, K. et al [13] is itself a survey paper of various security and energy efficient secure protocols. He selected the protocols on the basis of architecture of network. The tabular comparison by the author is given in appendix. Garg, A. at al [14] discussed first, the security requirements of wireless sensor networks are presented and the relationships between network security and network lifetime limited by often insufficient resources of network nodes are explained. Second, a short literature survey of energy aware security solutions for use in WSNs is presented. This paper used the trust management mechanism. Trust is built hop by hop communication of sensor nodes with others and based on the higher trust value node is considered as a healthy node not the malicious node.

Jean de Dieu, I. [15] overcame the limitation caused by the symmetric key cryptography algorithms for securing data in WSNs. It proposed a mechanism for checking data integrity in a balanced energy network backbone. On this basis, we use the combined version of distance energy aware routing and a checking data integrity method for WSNs. ESPA provides a better performance in maximizing the network lifetime. Author used distance-based energy aware routing algorithm which can effectively alleviate the hotspot problem based on the theoretical deduction and analysis of relevant models. Under this well-designed route, the packet will be delivered to the destination in a secure manner with help of a keyed hash function. The proposed model was divided into two parts. At the first phase, they proposed a distance based energy aware routing (DEAR) algorithm on selected optimal path through Ant colony optimization (ACO). The objective of this phase is to balance the available amount of energy in the wholeWSNs as well as to maximize the network lifetime. At the second phase in the proposed network routing we ensured confidentiality, authenticity, and integrity security services on the sensed data. Figure 3 shows the complete architecture of the proposed model.

Prabhu, T.N. et al. [16] proposed an energy efficient secure routing protocol to deliver the message to the sink correctly without any alterations. It is a routing protocol with security mechanism to defense the attacks. Detection of compromised

node is done by forwarding messages between various sensor nodes. We also propose energy efficient secure routing protocol to deliver the message to the sink correctly without any alterations. It is a routing protocol with security mechanism to defence the attacks. The implementation of our routing protocol is feasible. The performance of our routing protocol is also shown to be energy efficient. Paper follow several testing standard and assume some reasonable routing topology to calculate the performance. Trust based security mechanism is used in this paper also.

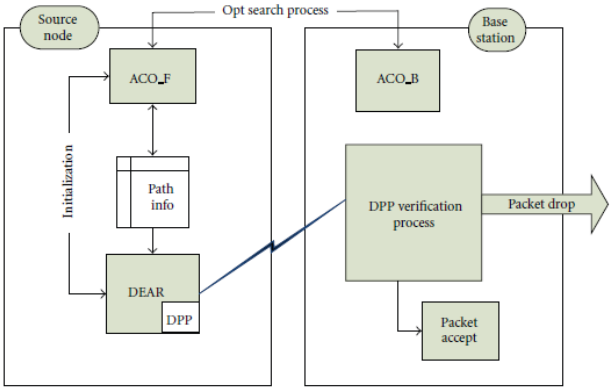

Fig. 3. General backbone model

Obaidat, S.M [17] carefully analyzed the previous research done in field of security and energy efficiency. Most of the existing sensor networks usually have dedicated sensor devices with a single purpose in mind, but in an urban environment, the devices used by the people often have multiple tasks. Thus, it is important not only to keep the footprint of the running algorithm low, but also to enable the user to have trust in the system. The proposed DEESR protocol is an attempt geared towards the same objective. As shown in this paper, the proposed protocol is not only energy efficient but is highly resilient in low mobility, medium mobility and high mobility scenarios. Apart from this, the packet delivery ratio delivered by the protocol is comparable and sometimes better than some of the well-established protocols like DSR and MMBCR.

El-Semary, A.M et.al [18] proposed an energy-efficient secure routing protocol for WSNs in which each sensor node forwards packets based on its own information. Thus it cannot be deceived by any other sensor node. The protocol employs the Roulette Wheel selection algorithm to select a next node during the forwarding process while using µTesla protocol together with symmetric encryption and hash function algorithms to provide the needed security. Simulation results indicate that the performance of the proposed protocol outperforms the performance of the Path Energy Weight and the minimum hop protocols under such attacks. In roulette wheel selection algorithm, an individual is given probability of being selected that is directly proportional to its measured metric. The individual is then chosen randomly based on its probability.

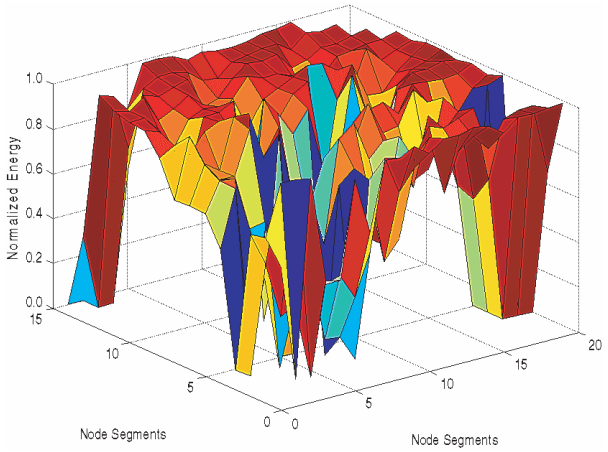

Fig. 4. EERP

Figure 4 shows the energy distribution of the network deploying the EESRP and it clearly shows that each malicious node only consumed the energy of the nodes in its neighborhood due to receiving malicious packets. Dhawale, A. et al [19] discussed various authentication techniques available in wireless sensor network and analyzes them. Some techniques are very helpful but come with some disadvantages. The effort is also done to point out these difficulties. Authentication is one of the best security solutions which protects whole sensor network. The proposed security using authentication without opening the secret information is highly secured and will not be broken. If the zero knowledge protocol is used for repeated challenges then it will be very secured and sure scheme for the security of entire network. The computational cost of this technique also appears to be very less as there are no high calculations required. So this will reduce the energy, storage requirements of the sensor node. Thus much effort should be given to develop such highly secured authentication schemes. Yang, Q at al [20] published a very good survey paper in which various algorithms categorized under categories like architecture based, position based etc. are considered.

III. Conclusion

This study surveys various research papers for WSN nodes localization. Several methods including bio-inspired and analytical are used previously but promising results are achieved through bio inspired methods. So in this paper we reviewed some papers which are based on heuristic methods for WSN nodes localization. We noticed none of the paper has targeted the security issue in nodes localization though very few left this for future work, so we also considered some WSN security papers so that a collective review can be presented. A comprehensive review table is presented in appendix.

APPENDIX

TABLE I
REVIEW

Techniques	Author & Reference	Year	Advantages	Limitations
Modified bat Algorithm	Sonia Goyal and Manjeet Singh Patterh [1]	2016	Improved accuracy with less mean localization error	easy to fall into local optimum
PSO and Quasi Newton algorithm	Jingang Cao [2]	2015	Effectively improves the localisation than LPSO	Computational complexity is increased
PSO	X. Zhang, T. Wang and J. Fang [3]	2014	path planning algorithm based on a kind of grid scan is considered and better results than multilateration algorithm	PSO is now old algorithm and prematurely converges
DV-distance and PSO	P. H. Namin and M. A. Tinati [4]	2011	Localisation error has reduced to 12% compared to TSA	NA
Hybrid PSO and DE optimisation	S.R.Sujatha, Dr.M.Siddappa [5]	2017	Better results compared to DWPSO	Hybridization of PSO-DE increases computational complexity
Grey Wolf Optimisation	R. Rajakumar, J. Amudhavel, P. Dhavachelvan, and T. Vengattaraman [6]	2017	Compared to PSO and MBA, it gives better localization of nodes	easy to fall into local optimum
Improved PSO	Dan Li[1], Xian bin Wen [7]	2015	Solves multi-dimensional optimisation problem	Nodes position in 2-D is used whereas in real it is in 3D
Biogeography-Based Optimization (BBO) algorithms and (PSO)	S. Singh, Shivangna and E. Mittal [8]	2013	1. Better accuracy and fast convergence 2. advantage of reduced number of transmissions to the base station	Not compared with centralized and distributed localization methods
BAT algorithm and doppler effects	Miloud, Mihoubi & Rahmoun, Abdellatif & Lorenz, Pascal & Lasla, Noureddine [9]0	2017	Adding doppler effect in BAT algorithm, convergence rate and localisation error is reduced	Multi criteria objective function could be considered and not applicable for scalable network
Membrane computing	Shagun Nasrani, Aashima Singla [10]	2015	Reduced the localisation error to 0.258	NA
Ant colony optimisation for routing	Malika BELKADI [11]	2014	Immediate response action to counter the attacks Balancing action benefit in the quantification of trade off	Less accommodation to node reputation and attack
Genetic algorithm for suitable nodes position	E. Golden Julie, S. Tamil Selvi, Y. Harold Robinson [12]	2014	Minimization of overall network cost. High beneficial compared to region based location management	Trustworthiness of elaborated model was poor Less mobility management under malicious behavior
Ant colony optimisation	Krzysztof Daniluka, Ewa Niewiadomska-Szynkiewicza [13]	2012	Better PDR for CBR traffic model with AODV Improvement in speed	Performance measurement of hybrid protocol non-investigated for unequal number of nodes
Bacterial Foraging Optimisation	Anuradha Garg, Ajay Tiwari, Hemant Kumar Garg [14]	2013	High suitability of hybrid protocols for large network	Non-investigation of suitability for unequal number of nodes
Survey Report	Imanishimwe Jean de Dieu, Nyirabahizi Assouma [15]	2012	Minimization of relative routing overhead. Maximum average hop count.	Trade-off is required between the communication capabilities and saving of resources.
Fuzzy logic considering security issue	T. N. Prabhu, C. Ranjeeth Kumar, B.Mohankumar [16]	2014	Minimization of overall network cost. High beneficial compared to region based location management	Trustworthiness of elaborated model was poor Less mobility
PSO based clustering of nodes	Aly M. El-Semary [18]	2012	Reduction of overhead Increase in delivery ratio	Computational overhead More number of route nodes
Multiple base station approach	Anand D. Dhawale, M. B. Chandak [19]	2012	Better security Less computation	Less investigation about the resistance of CSRP against various attacks
Fuzzy Logic based	T. Bayrem, R. Slim, and B. Noureddine [20]	2010	Accurate prediction of flow loss and data forwarding attacks	Quantitative parametric computation to be required

REFERENCES

[1] Sonia Goyal and Manjeet Singh Patterh. 2016. Modified Bat Algorithm for Localization of Wireless Sensor Network. Wirel. Pers. Commun. 86, 2 (January 2016)
[2] Jingang Cao,"A Localization Algorithm Based on Particle Swarm Optimization and Quasi-Newton Algorithm for Wireless Sensor Networks", Journal of Communication and Computer 12 (2015)
[3] X. Zhang, T. Wang and J. Fang, "A Node Localization Approach Using Particle Swarm Optimization in Wireless Sensor Networks," 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, Beijing, 2014
[4] P. H. Namin and M. A. Tinati, "Node localization using Particle Swarm Optimization," 2011 Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Adelaide, SA, 2011
[5] S.R.Sujatha 1, Dr.M.Siddappa," Node Localization Method for Wireless Sensor Networks Based on Hybrid Optimization of Particle Swarm Optimization and Differential Evolution", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 2, Ver. III (Mar.-Apr. 2017)
[6] R. Rajakumar, J. Amudhavel, P. Dhavachelvan, and T. Vengattaraman, "GWO-LPWSN: Grey Wolf Optimization Algorithm for Node Localization Problem in Wireless Sensor Networks," Journal of Computer Networks and Communications, vol. 2017, Article ID 7348141, 10 pages, 2017
[7] Dan Li1, Xian bin Wen," An Improved PSO Algorithm for Distributed Localization in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, January 1, 2015
[8] S. Singh, Shivangna and E. Mittal, "Range Based Wireless Sensor Node Localization Using PSO and BBO and Its Variants," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013
[9] Miloud, Mihoubi & Rahmoun, Abdellatif & Lorenz, Pascal & Lasla, Noureddine, " An effective Bat algorithm for node localization in distributed wireless sensor network" Security and Privacy, 2017
[10] Shagun Nasrani, Aashima Singla," Localization Enhancement of Wireless Sensor Networks By Using Membrane Computing", IJITKM Volume 8, Number 2 Jan-Jun 2015
[11] Malika BELKADI,"Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks" I.J. Information Technology and Computer Science, 2014
[12] E. Golden Julie, S. Tamil Selvi, Y. Harold Robinson,"Opportunistic Routing with Secure Coded Wireless Multicast Using MAS Approach", International Journal of Computer, Control, Quantum and Information Engineering Vol:8, No:7, 2014
[13] Krzysztof Daniluka, Ewa Niewiadomska-Szynkiewicza,"A Survey of Energy Efficient Security Architectures and Protocols for Wireless Sensor Networks" Journal of Telecommunications & Industrial Technology, 2012.
[14] Anuradha Garg, Ajay Tiwari, Hemant Kumar Garg,"A Secure Energy Efficiency Routing Approach In Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-3, February 2013
[15] Imanishimwe Jean de Dieu, Nyirabahizi Assouma,"Energy-Efficient Secure Path Algorithm for Wireless Sensor Networks" International Journal of Distributed Sensor Networks Volume 2012
[16] T. N. Prabhu, C. Ranjeeth Kumar, B.Mohankumar,"Energy-efficient and Secured Data Gathering in Wireless Multimedia Sensor Networks" IJIRCCE, Vol. 2, Issue 2, February 2014
[17] Mohammad S. Obaidat, Sanjay K. Dhurandher, Deepank Gupta,"DEESR: Dynamic Energy Efficient and Secure Routing Protocol for Wireless Sensor Networks in Urban Environments" Journal of Information Processing Systems, Vol.6, No.3, September 2010
[18] Aly M. El-Semary,"Energy-Efficient Secure Routing Protocol Based on Roulette-Wheel and μTesla for Wireless Sensor Networks" International Journal of Sensor Networks and Data Communications Vol. 1 (2012)
[19] Anand D. Dhawale, M. B. Chandak,"Authentication Techniques for Wireless Sensor Network", MPGI National Multi Conference 2012, Proceedings published by International Journal of Computer Applications
[20] T. Bayrem, R. Slim, and B. Noureddine, A novel secure and multipath routing algorithm in wireless sensor networks, in Proceedings of the 2010 International Conference on Data Communication Networking, Athens, Greece, 2010, 25–34.