iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.30844

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

Wireless Sensor Network Jammer Attack: A Detailed Review

K. Dhivyasri[1], Dr. A. Suphalakshmi[2], M. Revathi[3]
[1, 2, 3]*Department of Computer Science Engineering, Paavai Engineering College, Namakkal, Tamilnadu, India.*

Abstract: ***In todays era there is open access wireless medium and shared nature available everywhere, where the Wireless Networks can be attacked by the jammer easily. By this attack the real normal communication by utilizing the similar wireless channel of legal nodes are stopped. It's a tedious process to prevent the attack or find out the jammer location. When located an indication of implementing anti-jamming mechanism is applied. In account of locating the jammer attacks accurately, a discussion of existing attack localization techniques relating to gravitation locate algorithm (GLA) is applied. This heuristic optimization evolutionary algorithm on newton's law of global gravitation and interaction follows several steps. Also for selecting the alternative ways Link-quality Aware Path Selection algorithm is used on finest link quality. Also various detection algorithms such as PSO (detecting malicious node in WSN, LEACH protocol for IoT applications, distance related threshold for CH selection , particle swarn optimization and several more algorithms are discussed in brief.***
Keyword- WSN, GLA, LAPSE, PSO, Swarn optimization, LEACH.

I. INTRODUCTION

In general each and every network needs security measures that too the wireless networks undergoes many security issues as they are open access medium. The WSN have evolved due to wide varied accessability among various domains namely target locating, managing fuel, military applications, medical field, robotics and even in agriculture [1,2,3,4].The major issue in wireless network is the jamming attack that eliminates unwanted radio signals to stop or interrupt real normal communication among WSN. Further the process is done by occupying the WN channel or demolishing the protocols coupling among two or many low-end easy end shelf wireless devices [5,6,7,8]. By interference differentiation within the Wireless nodes the attack can be able to break the MAC protocol by ack indication to the channels. The attacker can initiate jamming attack from various protocol layers and even by different sources. When the attack is initiated the performance gets shattered on minimal resource consumption that is entirely projected by adversaries. The attack also leads to tremendous packet drops and and re-transmission failure, network failure again and again. On the other way the Real-time wireless communication is an evolving application criteria of wireless sensor networks that true efficient research path. The real time and upcoming wireless sensors can be able to monitor everything, reply immediately to the input of the user or even manage the outer environment. The real time path are the Wireless sensor networks that enable the network origin delay conformed that is apt for the end to end packet delivery.

This method involved may require a sensor node to maximize the energy of the transmitter as a resistant estimation against the jammer. Also, these nodes with the capacity to format their transmission energy that is highly complex and vendor-particular, thereby querying the applicability of this suggestion.

Spread spectrum methods: the Frequency- Hopping Spread Spectrum ((FHSS) and Direct Sequence Spread Spectrum (DSSS) method transmission are used to diagnose the jamming process while comparing the single frequency transmission.

Here the wireless network jamming attacks and its solution on the previous papers are discussed below[15]. Here Spuhler et al. [16], states that the process focuses on calculating the packet delivery ratio from the calculated v value of the ratio. The theory involves the jammers detection process studying for signal synchronizing and knowledge for few bits of signal. The main drawback of DSSS involves reduced chip rate and minimal transmission energyof sensor nodes.

Azim et al. [18] targeted on addressing the main issue of dominant attacked/jammed zones in an exceedingly WSN. The work determines the information of the perimeter of the attacked zone and uses mapping routines at intervals the zones. Eventually, the work determines the radius vector and calculates the purpose wherever the message notification method must terminate. As mentioned earlier, this approach would result in floodingwith too several broadcast messages among the packed zone. this could result in extreme inaccurate results because the nodes at intervals the attacked space become too clattery and it additionally exhausts the battery lifetime of the nodes. Several ultra wide band technology: This technology permits a node to transmit short pulses at intervals an oversized frequency spectrum, thereby disabling signal interception. Oppermann et al. targeted on the fine

arts aspects of extremist wide bandbased device networks. However, such a technological approach has limitations associated with hyperbolic power consumption and energy consumption. a posh system setup: a number of the systems have an especially complex setup and hardware dependencies that build such systems tough to be incorporated in sensible situations

As an example, Sedehi et al. [16] targeted on electronic jamming detection and cancellation utilizing airborne/space borne measuring instrument equipped systems.

The characterization and also the performance of the work depend extremely on the degrees of freedom of the auxiliary beams used for detection of the sender. The limitation of the work is multifold.

Firstly, the associated ranging primarily based setup with several multiple channels can have an maximized complexness in sensible systems requiring high power provides. the amount of auxiliary beans to be used for the most part depends on the gain issue of the most antenna of the measuring instrument. Further, the choice of the degrees of freedom is considerably advanced subjected to the intensity of the disturbance created by the sender.

In a wireless sensor networks the authors focuses majorly on two main aspects that include minimization of energy consumption and network lifespan prologing. Here the research papers describes LEACH protocol [22,24] as a basic algorithm in which several changes have been done relating different applications. A detailed survey of LEACH and its successors are shown in [28] considering four important parameters such as clustering method, data aggregation, mobility type and scalability.

The protocol combination with the flat-based routing protocol as in Sec-LEACH [11].where a security-based protocol combines the advantages of LEACH and SPIN protocols improvizing the security measures of the network. This by turn increases the entire net researchers have modified LEACH with the representation of quadrant-related directional routing (Q-DIR) protocol to improvise network lifespan and constant of the network but ended up increasing the management overhead. Kandpal and Singh [13] have stated IL-LEACH, where the correlated data is transmitted through a group of nodes into the virtual correlated cluster and allowing only one node to send data [24,25,26,27].

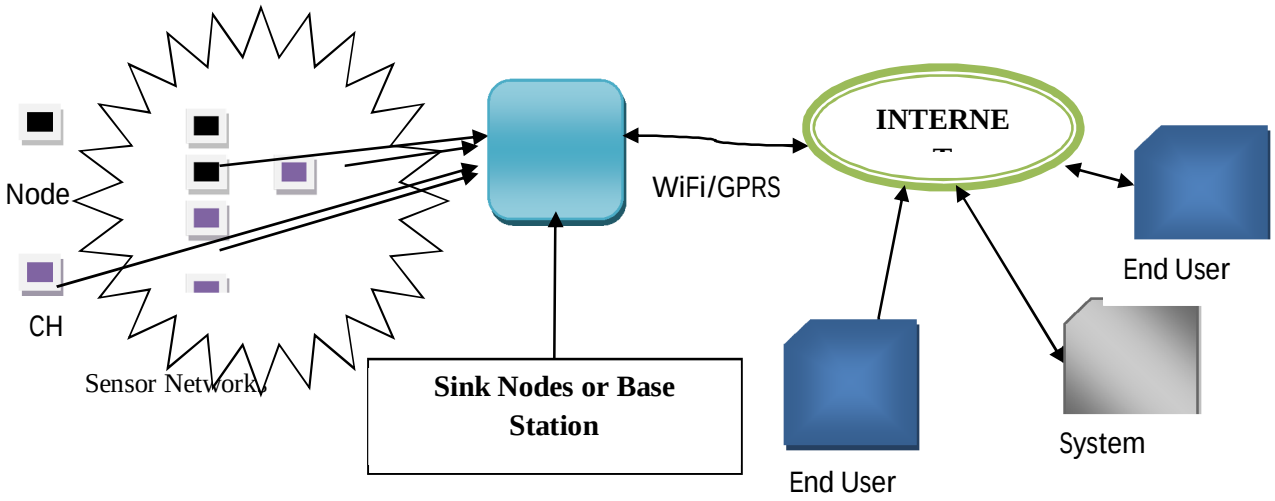


Fig 1. WSN system Model

II. METHODOLOGY

A. LAPSE Algorithm

At first, the initial particles are chosen arbitrarily from the jammer attack space. Then, the fitness perform is meant supported range-free methodology. A series of simulations are conducted to judge the discussed rules and also the simulation results show that the GSA-based localization algorithm outperforms several progressive algorithms[31].

The proposal formats Link-quality Aware Path choice (LAPSE) algorithmic rule that chooses different ways supported the best link quality. LAPSE is predicated on best call Rule (ODR) and its style considers the fallible nature of the nodes whereas choosing/rejecting a selected link. Finally, the performance of the projected rule, LAPSE, is evaluated in terms of the network parameters – packet delivery rate, network throughput procedure, transmission energy, node life, and network life. Results indicate that the performance of LAPSE is considerably higher than the prevailing jamming techniques rejection algorithms.

There are 2 key observations that drive our modelling of reactive and non-reactive jammers.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

1) In an exceedingly time-critical application, a message becomes invalid as long because the message delay D is larger than its delay threshold σ. Thus, the systems outline a metric, message invalidation value, to quantify the impact of jammer attacks against the time-critical application.

2) Once a retransmission mechanism is adopted, to with success disrupt the delivery of a time-critical message, the transmitter must jam every transmission try of this message till the delay D is larger than σ.

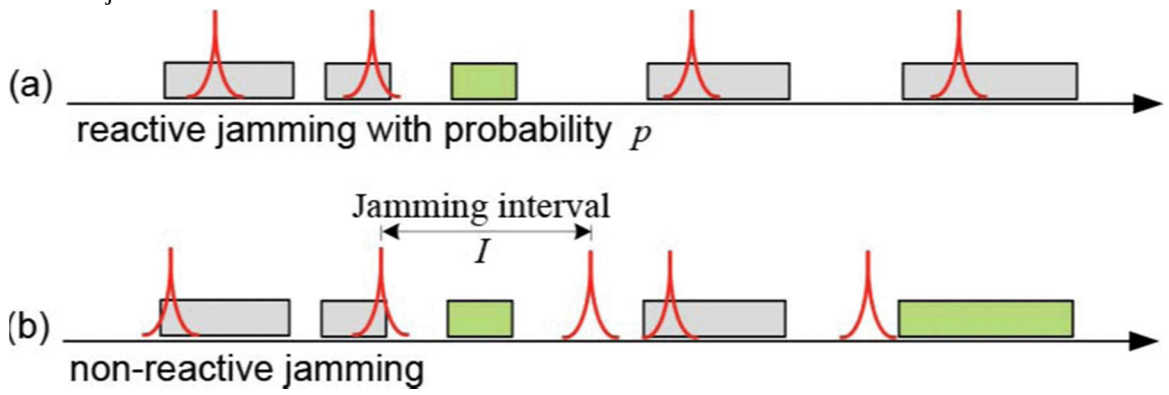
As a result, such behaviour of the transmitter is strictly an equivalent as the behaviour of a gambler WHO intends to win every play in a game to gather enough fortune to realize his gambling goal of σ dollars.

The system involves complex wireless networks to jamming attacks which may damage or cause major impact on the network performance [8]–[10]. The jamming issue in conventional wireless network CWN has been widely discussed considering the jammer performance, detection, anti-jamming techniques and applications ets..,The major two types of jammer attacks are reactive and non-reactive jammer.

a) *Reactive Jammer:* Reactive jammers are used to prevent the target communication systems. The reactive jammer remains constant at time when the channel is idle. They also trigger radio signal transmission at once an activity is sensed on the WN channels.

b) *Non-reactive Jammers:* Nonreactive jammers are unaware jammers in which they have no idea about the legitimate nodes and transmit the radio interference among the wireless channel on their own jamming strategies [32,33,34,37].

Reactive jammers interupt legitimate transmissions in a more active and versatile manner than non-reactive jammers. When a reactive jammer feels any moving packet transmission, it can stop the packet with a managing probability . Thus, we model the strategy of a reactive jammer.



III. PSO BASED MALICIOUS NODE DETECTION

However, in a much ranked cluster primarily based WSN, cluster heads (CHs) consume additional energy because of further overload for receiving and aggregating the data from their member detector nodes and transmission the collective information to the bottom station. Therefore, the proper choice of CHs plays important role to conserve theenergy of detector nodes for prolonging the time period of WSNs. during this paper, the approach involves propose proposal of energy effectiveness cluster head choice algorithmic rule that relies on particle swarm optimization (PSO) known as PSO-ECHS. The algorithmic rule is developed with a effective procedure of particle encryption and fitness operate [38,40,42].

For the energy accuracy of the planned PSO approach, the system further contemplate numerous parameters such as intra-cluster distance, sink distance and residual energy of detector nodes. system conjointly provide cluster formation within which non-cluster head detector nodes be a part of their CHs supported derived weight operate. The algorithmic rule is then produced for testing on various numerous situations of WSNs, variable variety of sensor nodes and also the CHs. The results are compared with some existing algorithms to demonstrate the prevalence of the planned algorithmic rule.

The four stage working process of PSO

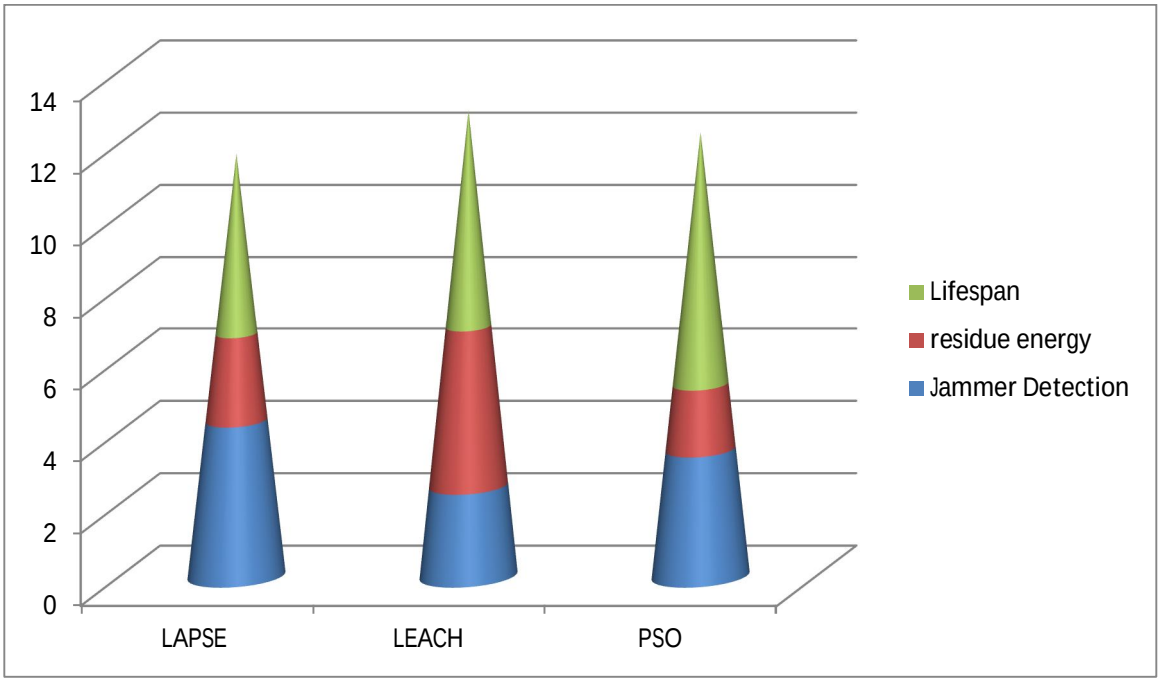
A. The first step involves the Malicious Node finding and elimination from the wireless sensor network.

B. The second one is the employment step, the Employment of PSO to compute Potential for all nodes in the wireless sensor .network.

C. Then the next step is the clustering step. Clustering in the wireless sensor networks is followed.

D. Then the final step is choosing cluster heads with high potential.

IV. RESULT ANALYSIS



Here in this analysis the jammer attack in the wireless network is considered and compared with various algorithms namely LAPSE, LEACH, PSO and other. Here the lifespan, residue energy of the WSN and jammer detection and anti-jammer is calculated.

V. CONCLUSION

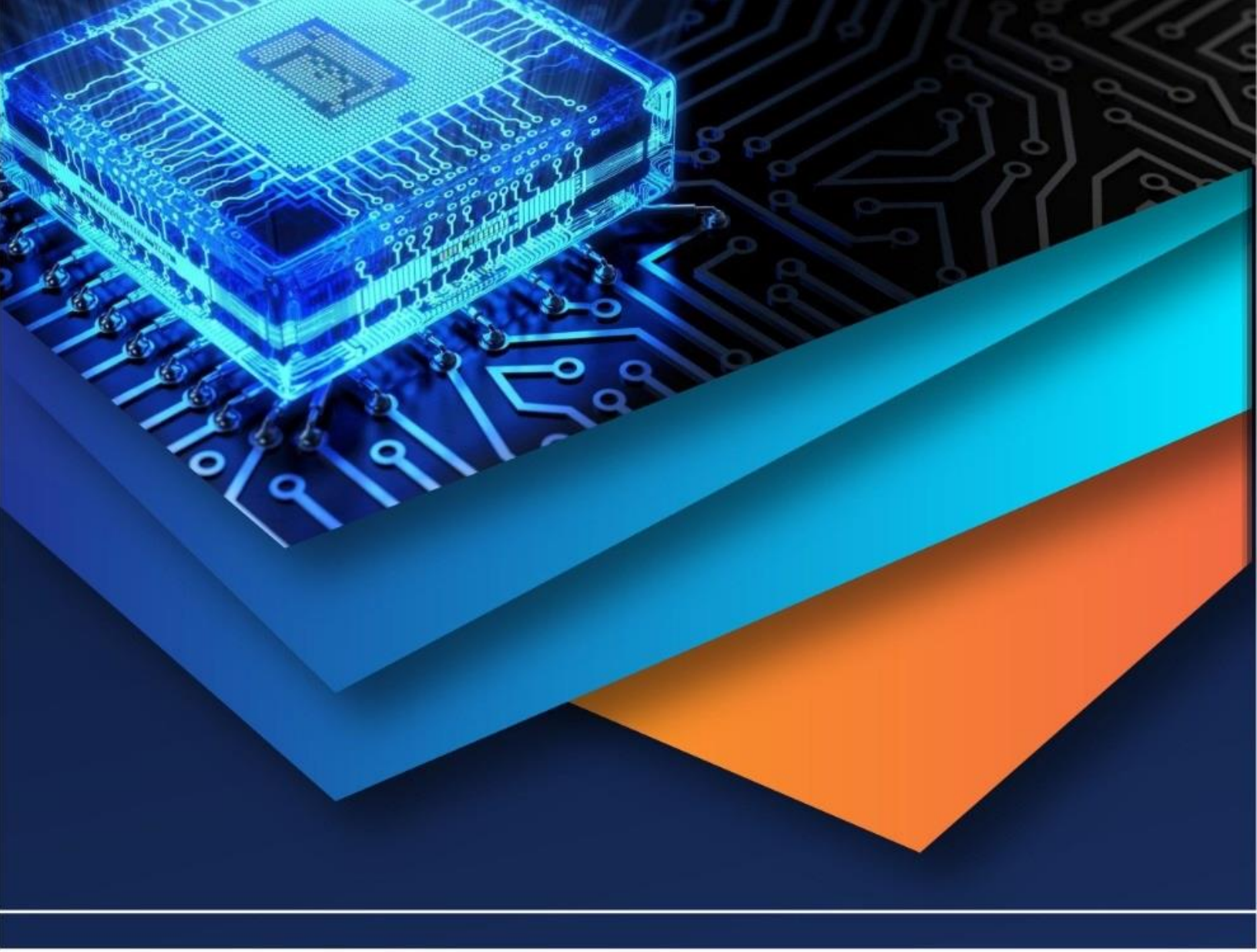
In this study, a review of jammer attack in wireless sensor network is elaborated. WSN has the potential to be employed in the measurement and controlling applications. With the aid of WSN, the incrementing spaces could be controlled and observed long-term data could be transferred at that scale, which is hard to achieve[44,45,46,47,48]. As wireless sensor network is used in various field its true fact that its open access medium that undergoes several attacks.one of the major attack is the jammer attack. In this survey a detailed view of wireless sensor network attack and reactive jammer, non-reactive jammers were discussed. Also the various algorithms for jammer attack detection are discussed and compared[50].

REFERENCES

[1] T. Y. Wang, L. Y. Chang, and P. Y. Chen, "A collaborative sensor-fault detection scheme for robust distributed estimation in sensor networks," IEEE Transactions on Communications, vol. 57, no. 10, pp. 3045–3058, October 2009.
[2] J. Barros and M. Tuchler, "Scalable decoding on factor trees: a practical solution for wireless sensor networks," IEEE Transactionson Communications, vol. 54, no. 2, pp. 284–294, Feb 2006.
[3] S. Chatterjee and S. Misra, "Target tracking using sensor-cloud:Sensor-target mapping in presence of overlapping coverage," IEEE Communications Letters, vol. PP, no. 99, pp. 1–1, 2014
[4] S. Aeron, V. Saligrama, and D. A. Castanon, "Efficient sensor management policies for distributed target tracking in multihopsensor networks," IEEE Transactions on Signal Processing, vol. 56, no. 6, pp. 2562–2574, June 2008.
[5] J. Oetting, "An analysis of meteor burst communications for military applications," IEEE Transactions on Communications, vol. 28, no. 9, pp. 1591–1601, Sep 1980.
[6] R. J. Kenefic, "Performance of an fmcw radar sensor," IEEE Transactions on Communications, vol. 40, pp. 1675–1678, 1992.
[7] K. ho Ahn, A. G. Stefanopoulou, and M. Jankovic, "AFR-basedfuel ethanol content estimation in flex-fuel engines tolerant to MAF sensor drifts," IEEE Transactions on Control Systems Technology, vol. 21, no. 3, pp. 590 – 603, 2013.
[8] S. Misra and S. Chatterjee, "Social choice considerations in cloud-assisted WBAN architecture for post-disaster healthcare Data aggregation and channelization," Information Sciences, vol. 284, no. 0, pp. 95 – 117, 2014.
[9] D. Kruse, J. Wen, and R. Radke, "A sensor-based dual-arm telerobotic system," IEEE Transactions on Automation Science and Engineering, vol. 12, no. 1, pp. 4–18, Jan 2015.
[10] C. Kone, A. Hafid, and M. Boushaba, "Performance management of IEEE 802.15.4 wireless sensor network for precision agriculture," IEEE Sensors Journal, vol. 15, no. 10, pp. 5734– 5747, Oct 2015.

[11] T. Wark, P. Corke, P. Sikka, L. Klingbeil, Y. Guo, C. Crossman,P. Valencia, D. Swain, and G. Bishop-Hurley, "Transforming agriculture through pervasive wireless sensor networks," IEEE Pervasive Computing, vol. 6, no. 2, pp. 50–57, April 2007.
[12] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in dsss-based wirelesscommunications," IEEE Transactions on Wireless Communications, vol. 13, no. 3, pp. 1593 – 1603, 2014.
[13] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," IEEE Transactions on Mobile Computing, vol. 13, no. 8, pp. 1746 – 1759, 2014.
[14] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," IEEE Network, vol. 20, 2006.
[15] M. Sedehi, F. Colone, D. Cristallini, and P. Lombardo, "Reduced order jammer cancellation scheme based on doubleadaptivity," IEEE Transactions on Aerospace and Electronic Systems, vol. 46, no. 4, pp. 1762–1781, Oct 2010.
[16] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," IEEE Transactions on Mobile Computing, vol. 11, no. 5, pp. 793 – 806, 2012.
[17] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Communications Surveys and Tutorials, vol. 11, no. 4, pp. 42–56, Fourth 2009.
[18] A. Azim, S. Mahiba, T. Sabbir, and S. Ahmad, "Efficient jammed area mapping in wireless sensor networks," IEEEEmbedded Systems Letters, vol. 6, no. 4, pp. 93–96, Dec 2014.
[19] R. C. Ben-Yashar and S. I. Nitzan, "The optimal decision rule for fixed-size committees in dichotomous choice situations: The general result," International Economic Review, vol. 38, no. 1, pp. pp. 175–186, 1997.
[20] S. Misra, R. Singh, and S. Mohan, "Geomorphic zonalisation ofwireless sensor networks based on prevalent jamming effects,"communication protocol for wireless microsensor networks'. Proc. of the 33rd Annual Hawaii Int. Conf. on System Sciences, Maui, HI, USA, 2000, vol. **2**, p. 10
[21] Mahapatra, R.P., Yadav, R.K.: 'Descendant of LEACH based routing protocols in wireless sensor networks', *Procedia Comput. Sci.*, 2015, **57**, pp. 1005–1014
[22] Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: 'An application specific protocol architecture for wireless microsensor networks', *IEEETrans. Wirel. Commun.*, 2002, **1**, (4), pp. 660–670
[23] Muruganathan, S.D., Ma, D.C.F., Bhasin, R.I., *et al.*: 'A centralized energyefficient routing protocol for wireless sensor networks', *IEEE Commun. Mag.*,2005, **43**, (3), pp. S8–13
[24] Yadav, L., Sunitha, C.: 'Low energy adaptive clustering hierarchy in wireless sensor network (LEACH)', *Int. J. Comput. Sci. Inf. Technol.*, 2014, **5**, (3), pp. 4661–4664[20] Sindhwani, N., Vaid, R.: 'V LEACH: an energy efficient communication protocol for WSN', *Mechanica Confab*, 2013, **2**, (2), pp. 79–84
[25] Oliveira, L.B., Wong, H.C., Bern, M., *et al.*: 'SecLEACH – a random keydistribution solution for securing clustered sensor networks'. Fifth IEEE Int. Symp. on Network Computing and Applications, 2006, NCA 2006, Cambridge, MA, USA, 2006, pp. 145–154
[26] Gnanambigai, J., Rengarajan, N., Anbukkarasi, K.: 'Q-LEACH: an energy efficient cluster based routing protocol for wireless sensor networks'. 2013 7th Int. Conf. on Intelligent Systems and Control (ISCO), Coimbatore, India, 2013, pp. 359–362
[27] Kandpal, R., Singh, R.: 'Improving lifetime of wireless sensor networks by mitigating correlated data using LEACH protocol'. 2016 1st India Int. Conf. on Information Processing (IICIP), Delhi, India, 2016, pp. 1–6
[28] Handy, M., Haase, M., Timmermann, D.: 'Low energy adaptive clustering hierarchy with deterministic cluster-head selection'. 4th Int. Workshop on Mobile and Wireless Communications Network, Stockholm, Sweden, 2002, pp. 368–372
[29]]Liu, L., et al. (2015). Physarum optimization: A biology-inspired algorithm for the steiner tree problem in networks. IEEE Transactionson Computers, 64(3), 818–831.
[30] Song, Y., et al. (2014). A biology-based algorithm to minimal exposure problem of wireless sensor networks. IEEE Transactions on Network and Service Management, 11(3), 417–430.
[31] Rao, P. C. S., et al. (2015). Energy efficient clustering algorithmsfor wireless sensor networks: novel chemical reaction optimization approach. Wireless Networks. doi:10.1007/s11276-015-1156-0.
[32] Rao, P. C. S., et al. (2016). Novel chemical reaction optimization based unequal clustering and routing algorithms for wireless sensor networks. Wireless Networks. doi:10.1007/s11276-015- 1148-0.
[33] Rao., P. C. S., et al. (2016). PSO-based multiple-sink placement algorithm for protracting the lifetime of wireless sensor networks. In Proceedings of the Second International Conference on Computer and Communication Technologies (pp. 605–616). Springer India.
[34] Kennedy, J., et al. (1995). Particle swarm optimization. IEEE International Conference on Neural Networks, 4, 1942–1948.
[35] Xu, J., et al. (2010). Distance measurement model based on RSSI in WSN. Wireless Sensor Networks, 2(8), 606–611.
[36] S. D. Babar, N. R. Prasad, and R. Prasad, "Jamming attack:Behavioral modelling and analysis," in *Proceedings of the 2013 3rd International Conference onWireless Communications, Vehicular Technology, Information Theory and Aerospace &Electronic Systems (VITAE)*, pp. 1–5, IEEE, 2013.
[37] K. Pelechrinis, M. Iliofotou, and S.V.Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEECommunications Surveys & Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.
[38] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.
[39] Y. Liu, F. Jiang,H. Liu, J.Wu, C.Hu, andM. Zhang, "Interference robust channel hopping strategies for wireless sensor networks," *China Communications*, vol. 13, no. 3, Article ID 7445505, pp. 96–104, 2016.
[40] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proceedings of the 2004 ACM Workshop on Wireless Security, WiSe*, pp. 80–89, October 2004.
[41] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-baseddata sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, Article ID S0167404817301621, pp. 1–12, 2018.
[42] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks,"*Information Sciences*, vol. 412-413, pp. 223–241, 2017.
[43] W. Xu,W. Trappe, Y. Zhang, and T.Wood, "The feasibility of launching and detecting jamming attacks in wireless networks,"in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05)*, pp. 46–57, ACM, Urbana-Champaign, Ill, USA, May 2005.

[44] X.Wei, Q.Wang, T.Wang, and J. Fan, "Jammer Localization in Multi-HopWireless Network: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 765–799, 2017.
[45] Z.-M.Wang and Y. Zheng, "The study of the weighted centroidlocalization algorithm based on RSSI," in *Proceedings of the 2014 International Conference on Wireless Communication an Sensor Network, WCSN 2014*, pp. 276–279, Wuhan, China December 2014.
[46] T. Y. Wang, L. Y. Chang, and P. Y. Chen, "A collaborative sensor-fault detection scheme for robust distributed estimationin sensor networks," IEEE Transactions on Communications, vol. 57, no. 10, pp. 3045–3058, October 2009.
[47] J. Barros and M. Tuchler, "Scalable decoding on factor trees: a practical solution for wireless sensor networks," IEEE Transactions on Communications, vol. 54, no. 2, pp. 284–294, Feb 2006.
[48] S. Chatterjee and S. Misra, "Target tracking using sensor-cloud: Sensor-target mapping in presence of overlapping coverage," IEEE Communications Letters, vol. PP, no. 99, pp. 1–1, 2014.
[49] S. Aeron, V. Saligrama, and D. A. Castanon, "Efficient sensor management policies for distributed target tracking in multihopsensor networks," IEEE Transactions on Signal Processing, vol. 56, no. 6, pp. 2562–2574, June 2008.
[50] J. Oetting, "An analysis of meteor burst communications for military applications," IEEE Transactions on Communications, vol. 28, no. 9, pp. 1591–1601, Sep 1980.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY