ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/1292
DOI URL: http://dx.doi.org/10.21474/IJAR01/1292

*RESEARCH ARTICLE*

# GA BASED CONTAINMENT ALGORITHM AGAINST STEALTHY ATTACKS IN WIRELESS SENSOR NETWORKS.

**Ram Pradheep Manohar[1] and E Baburaj[2].**
1. Research Scholar, Research Scholar, St. Peter’s University, Chennai.
2. Professor, Sun College of Engineering and Technology, Nagercoil.

## Manuscript Info

*Manuscript History*

Received: 18 June 2016
Final Accepted: 17 July 2016
Published: August 2016

***Key words:-***
GA, attacks, Wireless Sensor Networks, Network Security, Stealthy attacks

## Abstract

Intrusiondetection is an imperative part of a security framework. Subsequent to new attacks are rising each day, Intrusion discovery frameworks (IDS) assume a key part in recognizing conceivable attacks to the framework and giving legitimate reactions. IDSs ought to adjust to these new attacks and assault procedures, and persistently make strides. Instructions to create compelling, productive and versatile Intrusiondetection frameworks are an inquiry that analysts have been dealing with for quite a long time. Analysts have been investigating the suitability of diverse strategies to this examination area. The Evolutionarycomputation propelled from characteristic development is one of the methodologies progressively contemplated. A few qualities, for example, creating lucid yields for security specialists, delivering lightweight arrangements, giving an arrangement of arrangements with various exchange offs between strife destinations, make these strategies a promising contender for the issue. Evolutionarycomputation is a subfield of counterfeit consciousness propelled from characteristic advancement. It has been effectively connected to numerous exploration zones, for example, programming testing, PC systems, medication, what's more, workmanship. Intrusiondetection is the most concentrated on range in the security area, and different Intrusion discovery strategies as of now exist in the writing. There are numerous promising utilizations of Evolutionary algorithmdetectionon Intrusion location. It is particularly suitable for asset obliged and very rapid situations, because of their need of arrangements fulfilling different destinations. In this paper, the proposed methods in the writing are taken a gander at in point of interest. For instance, how applicant arrangements are spoken to, how advanced arrangements are assessed, which datasets are utilized, what favorable circumstances and inconveniences the proposed arrangements have, are all introduced.

**Corresponding Author: -Ram Pradheep Manohar**
Address: -Research Scholar, Research Scholar, St. Peter’s University, Chennai.

## Introduction:-

Wireless sensor systems (WSNs) comprise of an expansive number of small sensor gadgets or nodes with detecting, computational, and correspondence abilities. Sensor nodes screen some physical wonders in their surroundings, record the estimations of proper variables, and send them utilizing wireless transmission toward one (or, now and again, a few) system sinks. Along the way, information might go through various halfway nodes where a few separating and conglomeration might be performed. System sinks go about as entryways which gather the information, conceivably total it, and pass it on to the detecting applications that asked for it as shown in fig1. Sensor nodes are little and have restricted vitality, memory, data transfer capacity, and preparing power. They can be conveyed in all places, with next to zero human mediation from that point. A sensor system is (or ought to be) ready to work independently, from the minute sensor nodes as conveyed in the space of enthusiasm to the time when batteries are depleted and sensor nodes quit working. They are conveyed to the depletion this nonspecific situation might be connected by and large, what's more, it ought to shock no one that wireless sensor systems are getting to be progressively main stream in numerous natural, business, building, social insurance, military, observation, and different applications [1].Security is the critical issue in the WSN and the key management is the crucial point of the security issues. Because of the characteristics, following security problem for the key management in a WSN also should be taken into consideration: (1) Because of the wireless communication, it is easy to eavesdrop, intercept or interrupt the messages in a network.(2) The security scheme must be scalable because that the size of network would change even after deployment [2].Intrusion location is a critical viewpoint inside of the more extensive range of PC security; specifically organize security, so an endeavor to apply the thought in WSNs bodes well. Be that as it may, there are right now just a couple contemplates around there. Da Silva et al. and Onat and Miri [3] propose comparative IDS frameworks, where certain screen nodes in the system are in charge of observing their neighbors, searching for gatecrashers.

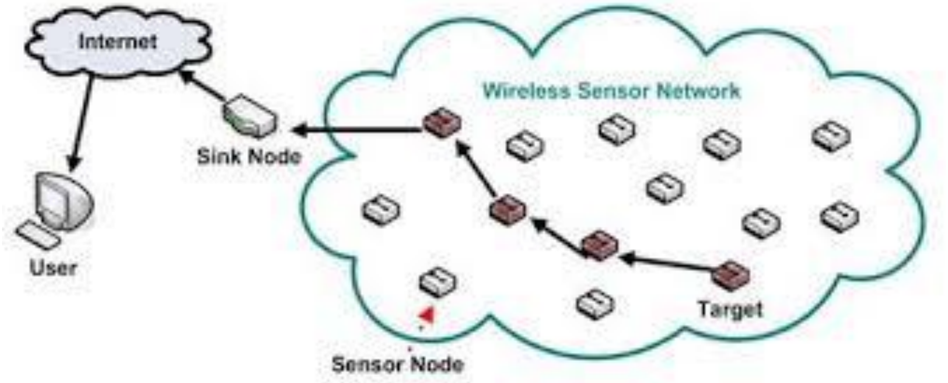

**Fig 1:-** Wireless Sensor Networks in Data Communication.

They listen to messages in their radio range and store in a cradle particular message handle that may be valuable to IDS framework running inside of a sensor node, yet no points of interest is given how this framework functions. In these architectures, there is no coordinated effort among the screen nodes. It is finished up from both papers that the support size is an imperative element that incredibly influences the rate of false cautions. Loo et al. [4] and Bhuse and Gupta [5] portray two more IDSs for routingattacks in sensor systems. Both papers accept that routing conventions for impromptu systems can likewise be connected to WSNs: Loo et al. [4] accept the AODV (Ad hoc On-Demand Distance Vector) convention while Bhuse and Gupta [5] utilize the DSDV and DSR conventions. At that point, particular attributes of these conventions are utilized like "number of course demands got" to distinguish gatecrashers. Be that as it may, as far as anyone is concerned, these routing conventions are not alluring for sensor systems and they have not been connected to any usage that we know about. More broad work has been done in Intrusiondetection for specially appointed systems [6, 7]. In such systems, dispersed what's more, agreeable IDS architectures are likewise ideal. Point by point circulated outlines; real location methods and their execution have been contemplated in more profundity. While likewise being specially appointed systems, WSNs are considerably more asset compelled. We are unconscious of any work that has researched the issue of Intrusiondetection in a general path for WSNs. In this paper we along these lines endeavor to move towards that course, characterizing the necessities, concentrating on the conceivable outline decisions and proposing a particular measured construction modeling proper for IDSs in WSNs.

The accompanying qualities of transformative computation pull in analysts to explore these procedures on Intrusion location: producing decipherable yields by security specialists, simplicity of representation, creating lightweight arrangements, and making an arrangement of arrangements giving diverse exchange offs between struggle destinations, for example, location ate versus power utilization. Moreover, EC does not require presumptions about the arrangement space [8].

## Intrusion detection system:-

Intrusion, i.e. unapproved access or login (to the framework, or the system or different assets) [9]; Intrusion is an arrangement of activities from inner or outer of the system, which disregard security perspectives (counting honesty, secrecy, accessibility and genuineness) of a system's asset [10]. Intrusion identification is a procedure which distinguishing opposing exercises with security approaches to unapproved access or execution diminishment of a framework or system [11]; the motivation behind Intrusion discovery procedure is inspecting, controlling, investigating and speaking to reports from the framework and system exercises. Intrusion Detection System (IDS), i.e.: Equipment or programming or combinational framework, with forceful cautious way to deal with ensures data, frameworks and systems [11]; Usable on host, system and application levels; For investigating movement, controlling correspondences and ports, distinguishing attacks and event vandalism, by inward clients or outer aggressors; Using so as to conclude deterministic techniques or nondeterministic Informing and cautioning to the security chief [12] (once in a while detach suspicious interchanges and square malevolent activity); Determining character of attacker and following him/her/it; There are three fundamental functionalities for IDS, including: observing (assessment), breaking down (detection) furthermore, responding (reporting) [13] to the happening attacks on PC frameworks and systems. On the off chance that IDS be arranged, effectively; it can speak to three sorts of occasions: essential distinguishing proof occasions (like stealthy filter and document content control), attacks (programmed/manual or neighborhood/wireless) and suspicious, Since routing consumes a lot of energy, and security was not a focus in the design of some routing protocol, an efficient and secure routing scheme in sensor networks is of importance. Routing protocols for wireless sensor networks are categorized as data-centric (flat) protocols, hierarchical (cluster-based) protocols and location-based protocols. A typical clustering protocol is called low-energy adaptive clustering hierarchy. It uses the technique of randomly rotating the role of a cluster head among all the nodes in the network [14].

## Stealthy attacks:-

Stealthyattacks were initially presented in [15]. Stealthy packet dropping is a suite of four attacks-misrouting, power control, identity delegation, and colluding collision-that can be easily launched against multihop wireless sensor networks. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors that it performs the legitimate forwarding action. Moreover, a legitimate node comes under suspicion Stealth attacks are routingattacks which "minimize the expense to and deceivability of the attacker yet which are about as destructive as beast power attacks". There are two sorts of stealth attacks, both of which depend on entering false sections or evacuating substantial passages in the routing tables of legit nodes. The top of the line of attacks means to diminish the throughput and separate casualty nodes of the system, or all the more by and large, debase and segment the system. The second kind of assault is equipped towards seizing movement to and from particular casualty nodes all together to take into consideration pernicious activities, for example, for instance, dynamic listening in and bundle sifting. It is imperative to note that while the likelihood of inactive listening in is characteristic to the show way of specially appointed systems, the attacker in the second sort of assault is outside of the transmission scope of the casualty, controlling the assault from a wireless area of the system.

In [15], the attacks are portrayed by method for six distinctive building pieces which thusly depend on the two fundamental weapons of "lying" and "impersonation": An aggressor, who is lying, will possibly proliferate wrong (routing) data. By method for mimic, the starting data of right routing parcels is changed.

## Containment algorithm against stealthy attacks:-

We propose to utilize lightweight security primitives and notoriety instruments to check the risk of the stealth attacks in sensor systems. These methodologies parity anticipation components as in they shield maximally against both DoS attacks and routingattacks. The proposed algorithm has the following steps.

The system is designed to unresponsiveness against the undesired messages. Keep views on each entry point of the network and asses the data transfer. Allow network communication only to sensor node. If many more entry points are there designates the security systems contain elements that scan rootkits for malware. Load the security systems before the components loaded. Spruce up the security systems help in the detection of malicious scripts. Collect the data over time and check the communication to unknown and unwanted addresses through traffic analysis. The following patterns are used to analyses the traffic of the attacker.

**Dummy Packet:-** This is a spurious activity era instrument, where the door infuses sham messages in a totally irregular way, subsequently; making commotion that covers the genuine movement.

**Dummy Route:-** This is likewise a fake movement era component, where the passage recreates the transmissions of a fake sensor; consequently, making the aggressor accept that the given sort of sensor is mounted on the patient, while in actuality, it is definitely not. All the more particularly, if the attacker realizes that this system is utilized for sham activity era, then he can't make sure that any recognized sensor sort is really on the patient or its vicinity is simply reenacted by the attacker.

## Optimized containment algorithm:-

Swarm intelligence (SI), inspired by the biological behavior of birds, is an innovative intelligent optimization technique [16, 17]. SI techniques are based on the collective behavior of swarms of bees, fish schools, and colonies of insects while searching for food, communicating with each other and socializing in their colonies. The SI models are based on self-organization, decentralization, communication, and cooperation between the individuals within the team [18]. Optimization has been proven to be very good solving many global problems. The evolution process of speeding up to a certain extent, but also can be implemented in parallel in nature and different individuals through continuous information exchange and transmission. The algorithm presents optimization of routing protocol in wireless sensor networks based on improved optimization algorithm which improves effectiveness of the algorithm, and improve the search for optimal routing [19].

A GA is a population based Swarm Intelligence model that uses choice and recombination operators to create new specimen focuses in the arrangement space [20]. A GA encodes a potential answer for a particular issue on a chromosome-such as information structure and applies recombination operators to these structures in a way that jam basic data. Proliferation opportunities are connected in a manner that those chromosomes speaking to a superior answer for the objective issue are given more opportunities to repeat than chromosomes with poorer arrangements. GAs is a promising heuristic way to deal with situating close ideal arrangements in expansive inquiry spaces [21].

To develop an algorithm against stealthy attacks have doubt on each packet passing through may be made to pass through multiple virtual interfaces. The total number of virtual interfaces taken is $V_n$. The set of Packets send are $S_p$ = (P1, P2,…..,Pn). 'n' is the maximum number of packets. Use Random allocation algorithm or round Robin algorithm to select the interfaces. The interval time may be changed from original traffic by introducing some variation in time $V_t$. The size of the packets $P_s$ varies from $P_{min}$ to $P_{max}$. The variation in packet sizes indicates the different applications use the sensor network. Now the scheduling algorithm may be optimized by analyzing thestrength of the security.

The time variation is calculated as $V_t = T_{original} – T_{actual}$. The computation cost of the each packet is calculated and the average is taken. The interface which possesses the optimized cost in terms of time is given priority for packet forwarding. After the optimized interface is identified, the priority scheduling may be used by giving priority to the interface based on the cost.

**Algorithm:-**

1. Start
2. Set the initial population (Random selection from the interfaces with cost).
3. Evaluate the fitness

$$Pi = \frac{Inti}{\sum_{i=0}^{N} Intj}$$

4. Cross over (interface): A new child is created with two parents. Now the computation cost of the new interface is calculated.

5. Mutation (interface): A chromosome from each parent interface change.
6. Rearrange (new population); (interfaces with cost).
7. End.

The Pi is the probability of choosing the specific interface for the parent solution. The $Int_i$is the fitness function of the candidate solution and N is the total number of packets through that interface. $Int_j$is the average fitness function of the standard interface. In this method, GA is used to distribute the randomly used interfaces with the network. The network is divided into optimal number of segments. The proposed method uses the GA for segmenting and performs the routing based on optimal selection of interfaces, which is used to detect the attacker nodes. The malicious nodes include multiple different findings of the network actions due to observing the sensor events in its neighbors.

## Results and discussion:-

In this algorithm, two important considerations area taken into account, one the network life time and the other is secured best route. Since the fitness function of every interface is evaluated GA is used to find the best secure route among the multiple optimal routes which is highly resistive against the stealthy attacks. When the data packets take higher time to pass the interfaces consume more energy. The nodes with an optimal distance to the sink have consumed less energy and increases the life time of the network. In our proposed algorithm only the optimized interfaces are selected for the forwarding of data after their behavior is studied. The proposed GA scheme increases the detection percentage of the attacks. Due to the optimization in forwarding and behavior study the energy consumed is less which in turn increase the network life time. The following graphs show the effectiveness and efficiency of our proposed scheme as compared with the existing algorithms. This paper also concentrates on secured routing algorithm in wireless sensor system. Routing with secured delivery utilizes by the safe interface and studying the nodes behavior. This spares vitality to begin the transmission the distance from source node. Insect state streamlining and Genetic algorithm based methodology, are motivated from swarm knowledge what more, advancement hypothesis is individually. Both methodologies are powerful and versatile. They take into thought, the current level of vitality and general vitality utilization to choose the ideal course. In this paper, we have used the fitness function of Genetic Algorithm based methodology for routing in WSN with data gathering without aggregation. We have analyzed exploratory results for diverse size of systems utilizing GA based approach and evaluating the algorithm proposed with other evolutionary techniques is our future work. The results of simulation are shown in the fig 2 and fig 3.

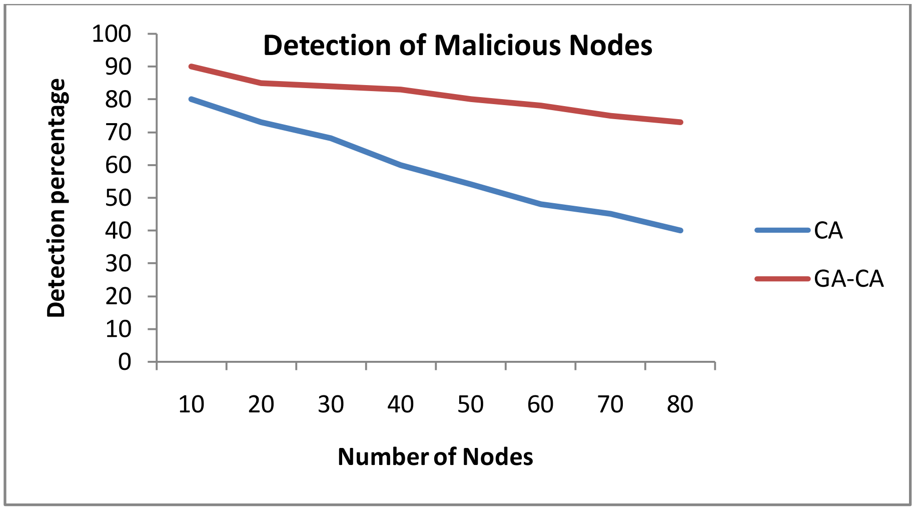

**Fig 2:-** Detection percentage of malicious nodes in GA-CA.

It is the ratio of the detection of malicious nodes to the number of nodes involved in transmission. As can be seen from the Figure 2 on traffic communication scenarios, the GA-CA performs better than the CA. Both the protocols detect a great percentage of the malicious nodes when there is little number of nodes. At lower number, the performance of both the protocols seems to converge. The detection ratio for both protocols are depicted at higher number of nodes, which indicates that the performance of both the CA and optimized CA drop rapidly as the number increases above 20. The performance gap between the two protocols in terms of detection percentage is found to be nearly 30%. Although the interfaces may change quickly, the minimum cost interface does not change so frequently, leads to establish a stabilized detection in GA-CA.

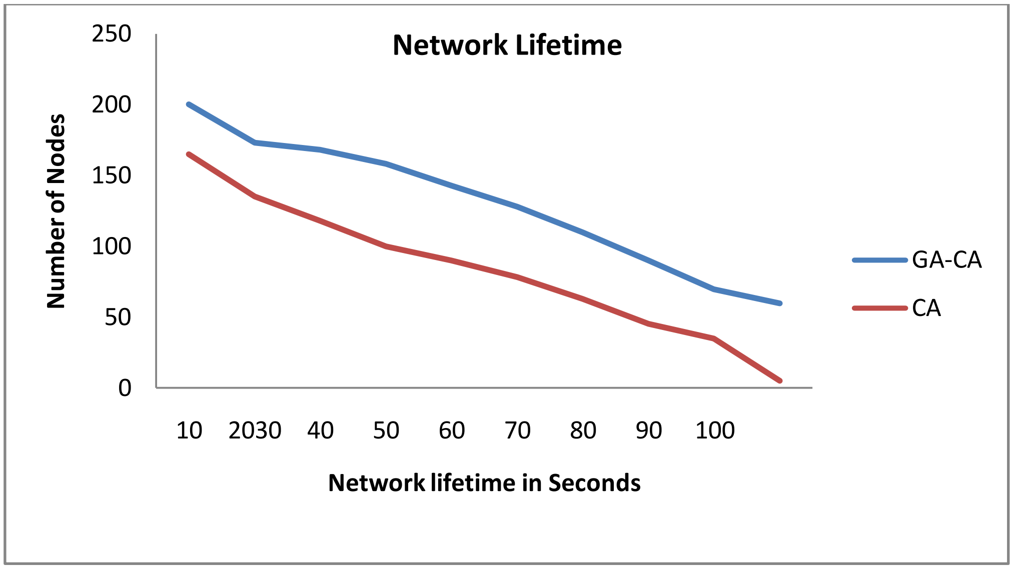

**Fig 3:-** Comparison between the algorithms in terms of Network lifetime and Number of Nodes

It is known that, both the existing and proposed protocols introduce virtually the same methodologies other than the optimization for all experiments. But when the number of nodes increases, due to the optimization of interface selection, there is a slight decrease in the overhead which in turn increases the life time of the sensor nodes. In the original CA, around 50% of the nodes lose their energy while selecting the right interface for routing; the GA-CA reduces the number of selection procedure to half the original, and manages not to become much affected by data forwarding. This, in turn, decreases the control message overhead considerably. Also, the quick convergence characteristic of the GA-CA and optimality in interface selection, are the reasons which contribute in minimizing the control overhead and increasing network lifetime.

## Conclusion:-

This Genetic Algorithm based Containment algorithm is a source-based computation which considers vitality utilization and also end-to-end delay in course determination. The proposed algorithm applies crossover and mutation operations specifically on interfaces, which streamlines the coding operation and excludes the coding/deciphering process. Heuristic change method can enhance the aggregate vitality utilization of a network life time. A progression of investigations was performed to check the execution, Network life time and percentage of detection of the malicious nodes of the proposed method. The outcomes show that this algorithm is powerful and proficient. Our results have been very encouraging. We were able to generate a rule based system using the principles GA to classify all types of stealthy attacks. The results have encouraged us to extend the research and apply it to search over all the fields in the connections. We hope this would improve the performance of the GA based algorithm considering that at present.  we are able to classify all types of the attacksand to detect them easily.

## References:-

1. Abadeh, M.S, Habibi, J., Lucas, C. (2007). Intrusion detection using a fuzzy genetics-based learning algorithm. Journal of Network and Computer Applications, Vol. 30, pp. 414-428.
2. Enjian Bai*, Xueqin Jiang, “A Dynamic Key Management Scheme Based on Secret Sharing for Hierarchical Wireless Sensor Networks “, Indonesian journal of Electrical Engineering, Vol.11, No.3, March 2013, pp. 1514 ~ 1523.
3. I. Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and communications, vol. 3, Montreal, Canada, August 2005, pp. 253–259.
4. C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, “Intrusion detection for routing attacks in sensor networks,” International Journal of Distributed Sensor Networks, 2005.
5. V. Bhuse and A. Gupta, “Anomaly intrusion detection in wireless sensor networks,” Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006. [10] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, February 2004.
6. K. Scarfone and P. Mell; Guide to Intrusion Detection and Prevention Systems (IDPS); NIST 800-94; Feb 2007.
7. Y.C. Yee, S.W. Tan, H.S. Lim, S.F. Chien, Application of Particle Swarm Optimizer on load distribution for hybrid network selection scheme in heterogeneous wireless networks, ISRN Commun. Netw. 2012 (2012), http://dx.doi.org/10.5402/2012/340720, Article ID 340720, 7 pages.
8. Fogel, D.B. (2000). What is evolutionary computation? IEEE Spectrum, Vol. 37, pp. 28–32.
9. V. Chandala, A. Banerjee and V. Kumar; Anomaly Detection: A Survey; ACM Computing Surveys; University of Minnesota; Sep 2009.
10. Ch. Krügel and Th. Toth; A Survey on Intrusion Detection Systems; TU Vienna , Austria; 2000.
11. Mohammad Saiful Islam Mamun, A.F.M. SultanulKabir, “Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network” , International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3 (July 2010).
12. G. Maselli, L. Deri and S. Suin; Design and Implementation of an Anomaly Detection System: an Empirical Approach; University of Pisa, Italy; 2002.
13. M. Jakobsson, s. Wetzel, and b. Yener. Stealth Attacks on Ad Hoc Wireless Networks. Proceedings of IEEE VTC 2003-Fall, 2003.
14. Zhang Yu-Quan and Wei Lei A, “New Routing Protocol for Efficient and Secure Wireless Sensor Networks”, Indonesian Journal of electrical Engineering, Vol.11, No.11, November 2013, pp. 6794~6801.
15. Khalil and S. Bagchi , “Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure” IEEE transactions on Mobile computing, Vol 10, No 8, PP 1096-112. 2011.
16. ShafiqAlam, Gillian Dobbie,Yun Sing Koh, Patricia Riddle “Research on particle swarm optimization based clustering: A systematic review of literature and techniques “, Swarm and Evolutionary Computation Elsevier, 2014, 17, PP 1-13.
17. A.P. Engelbrecht, Fundamentals of Computational Swarm Intelligence, vol. 1,Wiley, Chichester, 2005.
18. A. Abraham, H. Guo, H. Liu, Swarm intelligence: foundations, perspectives and applications, in: Swarm Intelligent Systems, Springer, 2006, pp. 3–25.
19. Tianshun Huang, “Optimization of Routing Protocol in Wireless Sensor Networks by Improved Ant Colony and Particle Swarm Algorithm”, International journal of Electrical Engineering, Vol 12 No 10, 2014pages 7486-7494.
20. Moatamad and A.Younes “Solving File Allocation problem in the Distributed Networks using Genetic Algorithms”, International Journal of Information and Network Security, Vol 2 No 1 PP 109-117. 2013.
21. L. Wang, H. J. Siegel, V. P. Roychowdhury, and A. A. Maciejewski. “Task Matching and Scheduling in Heterogeneous Computing Environments Using a Genetic-Algorithm-Based Approach,” Journal of Parallel and Distributed Computing, Special Issue on Parallel Evolutionary Computing, Vol. 47, No 1, pp. 8-22, Nov. 25, 1997.