Contents list available at IJRED website

Int. Journal of Renewable Energy Development (IJRED)

Journal homepage: http://ejournal.undip.ac.id/index.php/ijred

Research Article

Detection of Attacks on Wireless Sensor Network Using Genetic Algorithms Based on Fuzzy

Shaymaa Al Hayali[a], Osman Ucan[a], Javad Rahebi[b*] and Oguz Bayat[a]

[a] *Altinbas University, Istanbul, Turkey*

[b] *Turkish Aeronautical Association University, Ankara, Turkey*

ABSTRACT. In this paper an individual - suitable function calculating design for WSNs is conferred. A multi-agent- located construction for WSNs is planned and an analytical type of the active combination is built for the function appropriation difficulty. The purpose of this study is to identify the threats identified by clustering genetic algorithms in clustering networks, which will prolong network lifetime. In addition, optimal routing is done using the fuzzy function. Simulation results show that the simulated genetic algorithm improves diagnostic speed and improves energy consumption.

Keywords: wireless sensor network, fuzzy, genetic algorithm, detection of attack, malicious node.

Article History: Received May 16th 2018; Received in revised form October 6th 2018; Accepted January 6th 2019; Available online
How to Cite This Article: Al-Hayali, S., Ucan, O., Rahebi, J. and Bayat, O. (2019) Detection of Attacks on Wireless Sensor Network Using Genetic Algorithms Based on Fuzzy. International Journal of Renewable Energy Development, 8(1), 57-64.
https://doi.org/10.14710/ijred.8.1.57-64

1. Introduction

Current advances in hardware miniaturization and communication without material contact connection have increased the organization of the recent class of Wireless Sensor Networks (WSNs). WSNs are leading to the discovery of new applications in various fields such as demonstrative action controlling, tsunami discovering, and environmental controlling. Generally, the capability of a sensor node poses a basic constraint. In a high WSN arrangement, it is usually not possible to alter the batteries of the nodes. As a result, the ability to minimize is the main objective in o organizing full WSNs actions, containing sensing, information processing, and connection. Controlling natural phenomena is one of the central operations of WSNs. In such operations, a table-adjusted view of WSNs has proved to be of great help. Therefore, a WSN is considered to be delivering the origin of information where the values are created by a group of WSN nodes that set up a series of connection side by side in all nodes in the group. The data are adjusted with a view to bringing about the structure of WSN information reception regimes with two essential goals. WSNs combined with little form determine the equipment (nodes) that are arranged with various forms of sensors to carry away confident sensing functions within a nominated action field. Individual system and infrastructure with a few characteristics of WSNs promise answers to the examination and monitoring functions. Because WSN characteristics can be used in unfavorable climactic conditions, they are used for strategic connection and networking in military operations. Because the performance of nodes is mostly neglected and the connection catch area in a program is average, protection of WSNs poses a critical problem.

Remote Wireless Sensor Networks (WSNs) are as of late created to enhance many uses, which incorporate movement control, home robotization, shrewd war zone, condition checking and so on. WSN combines different sensors that are distributed around a specific hub. In a WSN, steering is an essential assignment that will be taken care of painstakingly. The steering method is required to send information between the sensor nodes and the base stations in order to accumulate correspondence. The fundamental basis, as presented in this paper, is the directing convention that changes in light of the application. The directing issue prompts diminished system lifetime with expanded vitality utilization. Along these lines, different directing conventions have been produced to limit the vitality utilization and to expand system lifetime. The steering conventions can be classified in view of the cooperation of the nodes, grouping conventions, methods of working and system structure. The various difficulties lie in directing incorporate vitality utilization, hub arrangement, adaptability, availability, scope, security (Sarkar & Murugan, 2016).

An ordinary remote sensor can gather data on the system, in the region of interest, and for each deciphering there are numerous circulated sensors in the boundary.

* Corresponding author: javadrahebi@gmail.com

These sensors gather the data being sent to the base station. In a remote sensor array, the power supply units are one of the real issues experienced because of the physical impediments being constrained in its vitality. Bearing in mind the end goal to utilize the sensor sources viably and effectively, the sensors and sensor stages must be overseen. There is a requirement for error tolerance, ideally a working sensor structure. Moreover, there are asset limitations, insecure movements, information abundance, array elements. This improvement is because of requirements, such as vitality adjust, different activity writes, packet criticality becoming significantly more difficult. In this way, numerous examinations have been made regarding this matter. In this work, remote sensor systems are utilized as a part of a group of sensors that work with a base station keeping in mind the end goal of expanding the life of the system. A set number of sensors and calculations are proposed to be dynamic. With a specific end goal to provide data from each district, the territory is isolated from the entryways and a sensor task is performed on the framework at each work step on which it was focused. The quantity of dynamic sensors in every network is the aggregate number of dynamic second sensors that is likely to be computed by partitioning the aggregate entropy utilizing these probabilities. The objective is to have a sensor actuated in every lattice. It is likely to be utilized as a part of optimization that is sent by the base to different sensors and keeping in mind the end goal to expand the system life, the quantity of working sensors has been attempted to be limited, as has the homogenous scope zone in the meantime with the most extreme entropy characterized above. Entropy is utilized for the general consumption of sensor vitality, and normal vitality use is given. he acquired scope zone and system lifetime relies upon these criteria: The quantity of working sensors being reduced however much as could reasonably be expected and entropy being near to the best conceivable entropy value (Elbaşı & Suat, 2012).

Remote sensor arrays are characterized as standing out amongst the most imperative advances of the 21st century. Changes in remote innovation are significantly less expensive andit becomes conceivable to create smaller scale sensors. A Wireless Sensor can be arranged in physical or ecological conditions areas according to various properties (temperature, sound, weight, movement, contamination, and so on.) by utilizing sensors to screen with coordinated effort, comprising of scattered gadgets in a system. The improvements in remote sensor systems began predominantly with military applications. However, these days, remote sensor arrays are found in numerous zones, such as natural perceptions and live observation, social insurance, home computerization and activity control. All sensor information disseminated over a particular territory in these systems has the ability to gather and direct information to the base station. Information is sent to the station through a multi-hop, non-foundation design, base correspondence by means of the Internet or satellite with the sensors of the station in addition to the Task Manager. The plan of sensor systems is affected by numerous elements, such as adaptation to internal failure, versatility, the cost of creation, working conditions, sensor array topology, equipment imperatives, and sensors such as correspondences and power utilization. Sensor arrays are ordinarily radio beneficiaries, transmitters or they may comprise different remote specialized devices and a power source. Sensor measurements can range from molecule to shoe box, and the costs are for this and the sensor as the unpredictability relies upon the need. Moreover, minimal effort sensors and correspondence arranging its essence has brought about the advancement of other potential applications. Potential sensor applications, running from military applications to biomedical applications, see sensors that can be set in places where life is not conceivable. It can last for a long time without restarting or overwhelming the power supply. General remote sensor system applications are for checking and controlling.

The key point in commitment cycling is to show a sub-tree of those nodes that will remain active while the others rest. Thus, correspondence throughout the framework is so far unique while a small number of the nodes remain alert. Another basic point is to describe sensible rest and wake-up plans for these nodes with a particular ultimate objective to give the sensibility of the framework. Two important subcategories constituting the data driven approach are data obtainment and data collection procedures which tend to diminish the amount of data to be forwarded. Data acquisition is performed at the signal level and data mixture is performed at the application level. Data securing includes unmistakable banners and transmitting data as a lone aggregate. In any case, data gathering is somewhat akin to filtering and plotting the main data beginning from every sensor node. Another to a great degree surely understood class of systems for lifetime prolongation is gathering. The rule assumed in batching is gathering the sensor center points depending upon different criteria, so to speak, in every manner that actually matters allocating the topology into grids. Batching can provide colossal essentialness hold subsidizes especially in high thickness frameworks (Anandh & Baburaj, 2016).

Remote sensor systems are an accumulation of spatially circulated self-sufficient sensor nodes that frame into systems with the purpose of detecting one or more physical properties, such as weight, temperature, sound and so forth inside their range. Different uses of such a WSN arrangement include observation of conditions, counting of wildlife, contamination control, health checking and military observations. Facilitating each WSN comprises at least one base station with the role of gathering information from individual sensor nodes and presenting them to an external system for ensuing preparation and activity. Certain sensor nodes function as specific nodes that perform information collection from nodes that are far from the base station. Regular working methods of WSN nodes include detection, information gathering, information processing and transmission. All tasks require a significant measure of battery life in the sensor nodes. Arbitrary association of the remote sensor system may prompt high utilization of energy by these activities, which may drain batteries rapidly subsequently shortening the lifetime of the remote sensor array. As the greater part of the WSN applications are transmitted under remote conditions, it is for all intents and purposes inconceivable to revive the batteries of the sensor nodes once they are conveyed into benefit. This vitality impediment has prompted the development of another sensor array engineering in light

of the grouping of remote sensor nodes. Clustering depends on the procedure of collecting a certain number of neighboring sensor nodes. A specific node of the group forms the cluster head that accepts the role of gathering information from cluster individuals and sends them to other bunch goes to the base station itself. The determination of the group head itself is viewed as vital for efficient energy use as the cluster proceeds directly for have high measure of vitality for the duration of the life-time of the system. At the point when the group heads are low in energy, a re-evaluation of the cluster head needs to be started such that a node with high energy becomes the new cluster head. During the time spent on information collection, the cluster heads similarly perform information pressure by removing any excess information caused due to the detection of limited information by group individuals (Anandh & Baburaj, 2016).

Giannecchini et al.(2004) suggested using CoRAl, online task scheduling mechanism, in designating the network resources allotted for different tasks to be applied at regular intervals in WSNs. Nevertheless, CoRAl failed to respond to the need to map sensor nodes and energy consumption (Giannecchini, Caccamo, & Shih, 2004). Lin, developed an "adaptive energy-efficient multisensory scheduling" system to be used in observing the course of targets in WSNs (Lin, Xiao, Lewis, & Xie, 2009). The EBSEL, developed by Abdelhak, is a system of balancing energy and increasing the energy life time (Abdelhak, Gurram, Ghosh, & Bayoumi, 2010). Clustering routing is leading to the development of efficient routing methods in WSNs considered to be beneficial in additional scalability, info collection, little amount, less efficiency utilization, further robustness. In recent years, approximately high digit of clustering routing rules has been advanced for WSNs. However; clustering routing protocols for WSNs have not been reviewed recently. The first aim of those analyses was to categorize the features of clustering and to summarize the favorable clustering routing methods by observing locations of various features. We have prepared a complete review of various clustering routing methods used in current years. The first study combines the clustering structure with a private key shared by the main cluster and the representative cluster in a cluster. This procedure uses the genetic algorithm to cluster and accomplish the routing located on the fuzzy election, addressed to find the aggressor nodes routing. Since clustering can decrease efficiency of the wireless sensor network, the connection range can be decreased considerably and thus, the network lifetime can be lengthened. We suggest using genetic method to cluster networks. It plays an important role in reducing the energy consumption and enhancing routing. If a node ceases to function, it is taken out and a new cluster is added. GA checks up the nodes in the routes and finds and removes each node before the attack. A recent clustering is made at the end. We found out that clustering is a procedure good enough to decrease the effective utilization of the network. In accordance with this, we propose using the incursion discovering method. The clustering provides meaningful information and decreases the network. Since protection and administration functions are valuable in cluster head nodes, there is no need for additional sensor nodes. To make this effective among the clustering, a dispersed clustering form is used to detect efficiency, node rate and topological attributes of a heterogeneous WSN. LEACH chooses chunk heads dynamically and periodically by means of a round mechanism, which allows various nodes to form cluster heads at each round clustering rule needs a hybrid standard for chunk head election, The clustering method finishes in O (1) repetition and does not rely upon the net amount. In the Highest-Degree scheme, designed by M. Gerla (Gerla & Tsai, 1995), the node selected as a cluster head has "the maximum number of neighbors" in which any connection is "broken by the unique IDs". . In Energy Efficient Clustering with Self-organized ID Assignment (EECSIA) the node chosen as a cluster head "in the high-density areas" is assigned an ID depending on the information about its locality. In addition, the clustering method will be used periodically, and the efficiency of the method depends on the node scale chosen as the cluster head. It is considered in classical clustering rules that as long as the nodes are supplied with the same size of efficiency, they cannot pick total characteristic of the turnout of node heterogeneity. The simulation results show that SEP constantly extends the stability of interval in contrast to that acquired by recent clustering rules. We display by emulation that SEP supply extended the stability of interval and that a higher output was obtained than that in recent clustering heterogeneous- inattentive rules. Such a clustering is desirable because efficiency loss is fully dealt with by the sensors and because the overall efficiency consumption is lower, similar to the efficiency sample we used. We explain why heterogeneous-clustering rule fails to keep the system stable, particularly when nodes are heterogeneous. We also explain SEP, which develops the steady area of the clustering hierarchy operation and uses the distinctive parameters of heterogeneity, namely the portion of advanced nodes and the extra efficiency agent among advanced and normal nodes. Abbasi (Boyinbode, Le, & Takizawa, 2011) made a review of the clustering methods for WSNs and suggested anatomy and rating of model clustering schema. Clustering methods for WSNs are based on the ranking of mutable assemblage time rules, fixed assemblage time methods, and their goals, characteristic, complication, etc. These clustering methods were compared instituted on metrics like concourse average, cluster stabilization, cluster overlapping, position- consciousness and support for node mobility. Arboleda (Arboleda & Nasser, 2006) compared various clustering protocols and outlined their usages. The authors discussed cluster construction, cluster forms, clustering benefits, and LEACH-based protocols in WSNs. The author classifies the routing protocols into nine in addition to two algorithms previously set up (Maimour, Zeghilet, & Lepage, 2010). The functions, advantages, and limitations of clustering protocols were studied in the survey, which was based on algorithms such as LEACH, TL-LEACH, EECS, TEEN, APTEEN, and etc. In addition, their energy use and life span were compared. Boyinbode studied algorithms for WSNs such as LEACH, TL-LEACH, EECS, HEED, EEUC, etc. using the metrics such as residual energy, uniformity of CH distribution, cluster size, delay, hop distance and cluster formation methodology (Abbasi & Younis, 2007). The author summarizes the routing techniques for WSNs in addition to structure of clustering considering the parameters of CH selection in order to find out whether

"there is a centralized control during clustering, and hops between nodes and CH in intra-cluster communication". The survey also focused on the clustering difficulties and routing techniques. The results of the survey Younis carried out point out that clustering has better routing and longer lifetime for WSN (Younis, Krunz, & Ramasubramanian, 2006). Every sensor develops the sensory data and sends them to the main (sink) in a secure way. Because sensor networks can function in unfavorable weather conditions and transmit precise facts, it is important to apply the portion to find an external attack that will destroy the network. However, it is difficult to protect sensor network because of the unfavorable distribution, developing topologies, limited calculation and battery resources, and reaching the goal. Sensor networks have their rare characteristics. First, immoderate sensor nodes are made up of cheap and strained hardware material that fails to meet the need for monitoring and desertification capacity. The genetic algorithm (GA) developed in the paper found the place of the machine to separate and put together the sensors in the best collection and direction with cluster-head. The genetic algorithm, the method that simulates the normal development, is especially of great help in applications that include form and growth where there a great number of variables and where two of the procedural invention do not exist or are very difficult. The GA, as a global optimizer, eliminates the complex expansion difficulty and thus it becomes easier to choose the model's form. All possible answers to LMN can be chosen evenly for. The highest area inclusion will be obtained effectively for LMNs. Genetic algorithms make it easier to decrease the complexity thanks to the different generation that appears together, and thus it makes it easier to get in actual-time. Furthermore, different probable answers help to choose different marks at the same time. Heinzelman's analysis of cluster heads was based on per round but the amount of energy in the network was unknown (Heinzelman, Chandrakasan, & Balakrishnan, 2002). The performance and energy consumption of wireless sensor networks were analyzed by considering fewer but more powerful nodes of overlay. All the data are conveyed to the sink, but the disadvantage of this method is that the cluster heads of the two types of nodes are not selected dynamically. Therefore, the distant nodes die first (Duarte-Melo & Liu, 2002). Mhatre and Rosenberg studied homogeneous and heterogeneous clustered wireless sensor networks to calculate the desirable range of sensors. However, it is difficult to apply such a method if heterogeneity results from the function of the network. Only the more powerful nodes are selected as cluster heads (Mhatre & Rosenberg, 2004). Guo states that the desirable way for WSN can be found through the genetic (Guo & Tang, 2010). Khanna states that Reduced Complexity Intrusion Detection in Sensor Networks Using Genetic Algorithm contributes to the life span of WSN with GA (Khanna, Liu, & Chen, 2009). Pires proposes an IDS procedure to find out whether the message conveyance is reliable when the signal power does not agree with its geographical place (Pires, de Paula Figueiredo, Wong, & Loureiro, 2004). Du states that safe routing protocol that benefit from the high-end sensors can hinder usual routing attacks (Al-Karaki & Kamal, 2004). Silva suggests an IDS scheme to find the reactions of the network by supervising the node (da Silva et al., 2005). According to Agah's game-theoretic approach, a comparison of Markov model (HMM) is made. Agah stated that the use of intuitive metric approach contributes to the defense of the sensor network (Agah, Das, Basu, & Asadi, 2004). Liu points out that spatial correlation of the functions of sensors should be determined through "insider attacker detection in wireless sensor networks" obtain a more accurate alarm rate (Liu, Cheng, & Chen, 2007). Doumit's HMM approach, a structure of natural events, uses the knoeledge from the region and separates it (Doumit & Agrawal, 2003). S.Gupta suggested a Wormhole Attack Detection Protocol that used Hound packet called WHOP to find any wormhole attack without a monitoring system or hardware. Any attack is discovered by the source node by making use of the hound packet. The difference between the neighboring hops is calculated. After this, the wormhole is found by the node in the distance (Gupta, Kar, & Dharmaraja, 2011). Some of the defense mechanisms suggested by Newsome (2004) include radio resource verification, position verification, node registration and random key pre-distribution (Newsome, Shi, Song, & Perrig, 2004). In Zhu, Setia, and Jajodia (2003), an encryption and authentication protocol (LEAP) protects WSNs from attacks. There are four classes of keys: individual, group, pairwise and cluster keys (Zhu, Setia, & Jajodia, 2006). In the design of Zhang, Wang, Reeves, and Ning (2005), Sybil attacks in WSNs are identified (Banerjee, Mukhopadhyay, & Roy, 2007). In the technique suggested by Piro, Shields, and Levine (2006), different identities are recorded regularly by a monitor, and they are analyzed statistically against Sybil attacks. This is because nodes often move inside the network, while Sybil nodes stay together (Piro, Shields, & Levine, 2006). Parno applied a random value to all nodes (Parno, Perrig, & Gligor, 2005) whereas Conti et al. applied a location claim to its neighbors

Demirbas and Song suggested a Received Signal Strength Indicator (RSSI) to prevent Sybil attacks (Demirbas & Song, 2006). In addition to the classification of potential attacks, David R. Raymond categorizes denial-of-sleep attacks on WSN MAC protocols by testing their effect on sensor networks. The effectiveness of the implementations of these attacks are also tested on these protocols (Raymond, Marchany, Brownfield, & Midkiff, 2009). Manju.V.C suggested using "Network organization and Selective level authentication" to protect the denial of sleep attacks (Goudar & Kulkarni, 2015). Kyung Choi uses Zigbee, (AES) security algorithm, for safety, which contributes to the security protocol supported by IEEE 802.15.4 (Choi, Yun, Chae, & Kim, 2012). Martin Peres proposed creating a secret key by means of an already-shared key, called key derivation. Thus, the network is provided with a chance to identify all that is shared by all the nodes of this network (Peres, Chalouf, & Krief, 2011). Jayanthiladevi made improvements on the suggestion by Martin Peres and added that safe communication can be made possible by user authentication in addition to using "public key cryptography" when the number of users exceed scalability (Rafik & Mohammed, 2013).

2. Materials and Methods

Optimal energy consumption in wireless sensor networks can be found through evolutionary algorithms. In genetic

algorithms, each solution may be represented as a binary string (chromosome) and the corresponding fit function can be measured. Sequential solutions are parts of an evolutionary process in which one of the selective solutions chooses one person for the next generation. The probability of choosing a solution is shown below:

$$P_i = \frac{F_i}{\sum_{j=0}^{N} F_j} \quad (1)$$

It shows the possibility of choosing a specific solution to the parents' population. The suitability of the candidate solution and N is desired way for a population.

In this paper, a genetic algorithm is used to distribute sensors randomly assigned to cluster networks, which are divided into optimal clusters with heads of clusters. A genetic algorithm was used for clustering and routing was based on fuzzy selection to detect the routing of the attacker's nodes. Incompatible (destructive) nodes provide more observations about the behavior of the network, due to the analysis of sensor events in their neighborhoods.

The data consist of message patterns, message collision, active traffic flow, sensor positioning, and synchronized events. Increasing the life expectancy was important in these networks. The distance of communication between sensors and the sink in a wireless sensor network increases the consumption of energy and thus reduces the network lifetime. Since clustering can reduce the power consumption of a wireless sensor network, we can significantly reduce communication distance and thus increase the network lifetime. Firstly, we used the genetic algorithm to cluster the network, which played an important role in reducing the energy consumption and optimizing the routing. In this paper, a genetic algorithm was used to distribute sensors randomly assigned to a cluster network, which was divided into independent cluster and optimal cluster headings. Clustering algorithm was used for clustering and routing based on fuzzy selection to detect the routing of the attacking nodes. Sink was also considered to be a reliable element to create a secure connection between different nodes. The closest socket to the socket was the most reliable connector. Communication between different sensor nodes was realized by sending and receiving messages. The sink was responsible for the authentication of the nodes. The genetic algorithm consists of monitoring nodes that control the network and each item that conflicts with the network's criteria (communication costs and battery energy), which increases the reliability of the network. The cluster head or any of the cluster nodes can act as a monitoring node. This node receives information about the other nodes and compares them to previous network configuration. The attacker identifies the attacker and sends the information to the sink.

3. Simulation Result and Discussion

The proposed method was simulated in MATLAB. We considered an area with an initial energy of 1000 J that was randomly distributed in the network. The number of clusters was assumed to be 10. We also had a three-dimensional matrix whose first and second dimensions were coordinates and the third dimension contained energy. The sink was placed at (0,0) on the page. We define the values of the genetic algorithm as follows:

> Primary population: 10, length of each chromosome = number of chromosomes * 2 = 10, two arteries = 0.7, mutation = 0.4, mutation rate = 0.2. Each node acts as a step counter for the sink.

First, the proposed method performs clustering and routing by using the nodes in the domain, and then the best optimal path is selected using the fuzzy method. If a node dies, it is deleted and a new cluster is executed. The genetic algorithm checks the nodes in the optimal path. Then it identifies and removes any node that matches the attack criterion. Finally, a new clustering is made. In this method, the two criteria for optimization are battery consumption and the best path. Since the genetic algorithm chooses several optimal paths, a fuzzy method is assumed to select the best path between them. In the fuzzy method, the path that has the lowest density, and the shortest distance from the sink is selected as the answer. At higher densities, nodes also consume more energy, and thus the paths that pass through these nodes consume more energy. In addition, short-to-syringe-to-sink nodes have less energy dissipation and save the network power. In multipurpose genetic algorithm, the two criteria are considered for optimization: battery consumption and the best path. Since the genetic algorithm chooses several optimal paths, a fuzzy method is assumed to select the best path between them. In the fuzzy method, the path that has the lowest density and the shortest distance from the sink is selected as the answer. In our proposed method, the entire sensor network was not investigated to detect an attacker node, but only the path chosen was investigated by the fuzzy algorithm. As a result, instead of looking at all of them, we only considered the selected nodes.

The different modes considered were as follows:

- The other node showing itself as the head of the cluster.
- A message that is repeated continuously.

We proposed a genetic algorithm approach to improve the pattern of attack detection. We showed that clustering is a suitable method for reducing network energy consumption and, based on this, an intrusion detection algorithm is presented. The results are summarized as follows:

1. Due to the tangible overhead of sending packets in the network, the nature of clustering idea in data integration and reduction of network traffic is very desirable.
2. Given that security and management tools are costly in cluster head nodes; there is no need for other sensor nodes to keep this service active during clustering. This service will help reduce the average energy consumption of each node in the network.
3. In our proposed method, the entire sensor network was not investigated to detect an attacker node, and only the path chosen was taken into consideration by the fuzzy algorithm. As a result, instead of looking at all of them, we only considered the

selected nodes. Different states are considered as follows:

- The other node showing itself as the head of the cluster.
- A message that is repeated continuously.

Figure 1 shows the structure of the nodes and the configuration of the node setup.

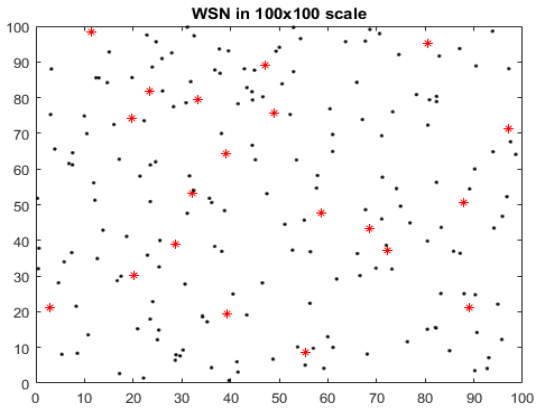

Fig. 1 Node setup

Figure 2 shows the number of network nodes against the network lifetime for fuzzy genetic algorithm with other methods.

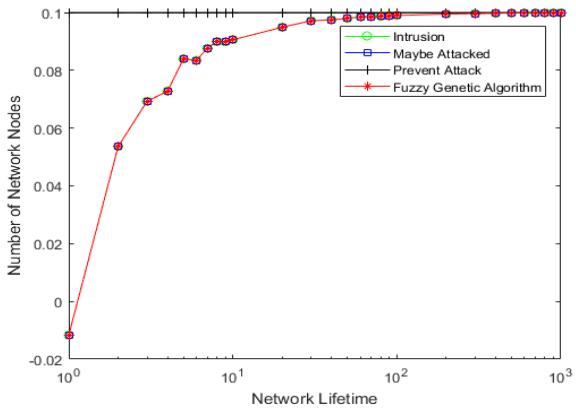

Fig. 2 Number of network nodes against the network lifetime with fuzzy genetic algorithm

Figure 3 shows the number of network nodes against the network lifetime for fuzzy genetic algorithm with other methods.

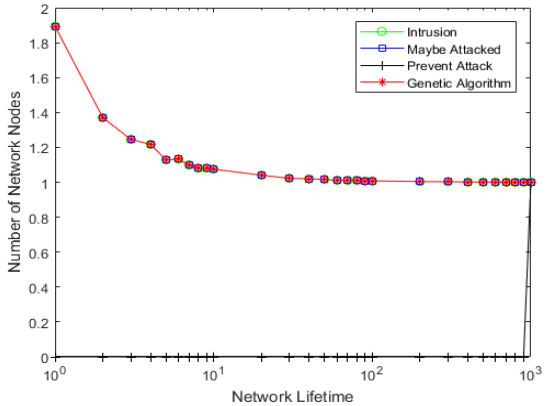

Fig. 3 Number of network nodes against the network lifetime with genetic algorithm

The test data with MSE and RMSE with small data are shown in figure 4.

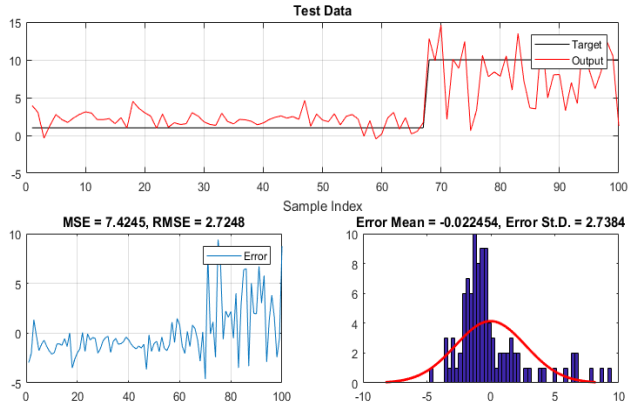

Fig. 4 Test data with MSE and RMSE with small data

The test data with MSE and RMSE with more data are shown in figure 5.

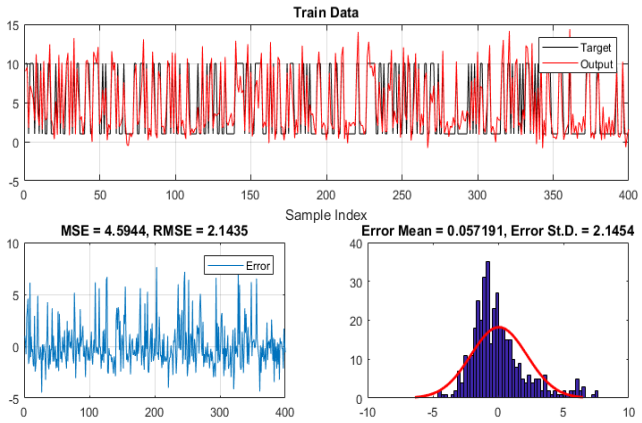

Fig. 5 Test data with MSE and RMSE with more data.

4. Conclusion

It is important to control the assembling of information for the material experience by means of Wireless Sensor Networks (WSNs). The difference in direction makes it necessary to protect Wireless Sensor Networks in contrast to an opponent trying to get perceptive sensor assemble. As the sensor nodes perform with restricted efficiency assets, it is important to effectively protect the structure, which is the main responsibility of WSNs. Organizations that follow income use high- range wireless sensor networks. Sensor administration plays a fundamental role in consideration of equilibrium that follows accomplishment and expense answerable to restricted network possessions in conditions of efficiency, connection frequency range, and perceives extent. In a wireless sensor network, the custom of possessions is frequently connected to the implementing of functions which use up a confident volume of calculating and connection frequency range. Aligned preparing between sensors is an encouraging resolution to support the demanded calculation volume in WSNs. Function distribution and organizing is a usual difficulty in the field of large achievement calculating. Even though function distribution and organization in connected processor networks have been well considered in the

preceding, their complement for WSNs stays highly undetermined. Available classic large accomplishment calculating answers cannot be straightly executed in WSNs because of the condition of WSNs such as restricted resource opportunity and the shared connection average.

References

Abbasi, A. A., & Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. *Computer communications, 30*(14-15), 2826-2841.

Abdelhak, S., Gurram, C. S., Ghosh, S., & Bayoumi, M. (2010). *Energy-balancing task allocation on wireless sensor networks for extending the lifetime.* Paper presented at the Circuits and Systems (MWSCAS), 2010 53rd IEEE International Midwest Symposium on.

Agah, A., Das, S. K., Basu, K., & Asadi, M. (2004). *Intrusion detection in sensor networks: A non-cooperative game approach.* Paper presented at the Network Computing and Applications, 2004.(NCA 2004). Proceedings. Third IEEE International Symposium on.

Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications, 11*(6), 6-28.

Anandh, S. J., & Baburaj, E. (2016). An Improved Energy Balanced Dissimilar Clustered Routing Architecture for Wireless Sensor Networks. *Circuit and Systems, Scientific Research.*

Arboleda, L. M., & Nasser, N. (2006). *Comparison of clustering algorithms and protocols for wireless sensor networks.* Paper presented at the Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on.

Banerjee, S., Mukhopadhyay, D., & Roy, S. (2007). Defending against sybil attacks in sensor networks: Google Patents.

Boyinbode, O., Le, H., & Takizawa, M. (2011). A survey on clustering algorithms for wireless sensor networks. *International Journal of Space-Based and Situated Computing, 1*(2-3), 130-136.

Choi, K., Yun, M., Chae, K., & Kim, M. (2012). *An enhanced key management using ZigBee Pro for wireless sensor networks.* Paper presented at the Information Networking (ICOIN), 2012 International Conference on.

da Silva, A. P. R., Martins, M. H., Rocha, B. P., Loureiro, A. A., Ruiz, L. B., & Wong, H. C. (2005). *Decentralized intrusion detection in wireless sensor networks.* Paper presented at the Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.

Demirbas, M., & Song, Y. (2006). *An RSSI-based scheme for sybil attack detection in wireless sensor networks.* Paper presented at the Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks.

Doumit, S. S., & Agrawal, D. P. (2003). *Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks.* Paper presented at the Military Communications Conference, 2003. MILCOM'03. 2003 IEEE.

Duarte-Melo, E. J., & Liu, M. (2002). *Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks.* Paper presented at the Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE.

Elbaşı, E., & Suat, Ö. (2012). *Secure data aggregation in wireless multimedia sensor networks via watermarking.* Paper presented at the Application of Information and Communication Technologies (AICT), 2012 6th International Conference on.

Gerla, M., & Tsai, J. T.-C. (1995). Multicluster, mobile, multimedia radio network. *Wireless networks, 1*(3), 255-265.

Giannecchini, S., Caccamo, M., & Shih, C.-S. (2004). *Collaborative resource allocation in wireless sensor networks.* Paper presented at the Real-Time Systems, 2004. ECRTS 2004. Proceedings. 16th Euromicro Conference on.

Goudar, C. P., & Kulkarni, S. S. (2015). Mechanisms for detecting and preventing denial of sleep attacks and strengthening signals in wireless sensor networks. *Int. J. Emerg. Res. Manag. Technol, 4*(6).

Guo, L., & Tang, Q. (2010). *An improved routing protocol in WSN with hybrid genetic algorithm.* Paper presented at the Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on.

Gupta, S., Kar, S., & Dharmaraja, S. (2011). *WHOP: Wormhole attack detection protocol using hound packet.* Paper presented at the Innovations in information technology (IIT), 2011 international conference on.

Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on wireless communications, 1*(4), 660-670.

Khanna, R., Liu, H., & Chen, H.-H. (2009). *Reduced complexity intrusion detection in sensor networks using genetic algorithm.* Paper presented at the Communications, 2009. ICC'09. IEEE International Conference on.

Lin, J., Xiao, W., Lewis, F. L., & Xie, L. (2009). Energy-efficient distributed adaptive multisensor scheduling for target tracking in wireless sensor networks. *IEEE Transactions on Instrumentation and Measurement, 58*(6), 1886-1896.

Liu, F., Cheng, X., & Chen, D. (2007). *Insider attacker detection in wireless sensor networks.* Paper presented at the INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE.

Maimour, M., Zeghilet, H., & Lepage, F. (2010). Cluster-based Routing Protocols for Energy-Efficiency in Wireless Sensor Networks *Sustainable Wireless Sensor Networks*: Intech.

Mhatre, V., & Rosenberg, C. (2004). *Homogeneous vs heterogeneous clustered sensor networks: a comparative study.* Paper presented at the Communications, 2004 IEEE International Conference on.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). *The sybil attack in sensor networks: analysis & defenses.* Paper presented at the Proceedings of the 3rd international symposium on Information processing in sensor networks.

Parno, B., Perrig, A., & Gligor, V. (2005). *Distributed detection of node replication attacks in sensor networks.* Paper presented at the Security and Privacy, 2005 IEEE Symposium on.

Peres, M., Chalouf, M. A., & Krief, F. (2011). *On optimizing energy consumption: An adaptative authentication level in wireless sensor networks.* Paper presented at the Global Information Infrastructure Symposium (GIIS), 2011.

Pires, W., de Paula Figueiredo, T. H., Wong, H. C., & Loureiro, A. A. F. (2004). *Malicious node detection in wireless sensor networks.* Paper presented at the Parallel and distributed processing symposium, 2004. Proceedings. 18th international.

Piro, C., Shields, C., & Levine, B. N. (2006). *Detecting the sybil attack in mobile ad hoc networks.* Paper presented at the Securecomm and Workshops, 2006.

Rafik, M. B. O., & Mohammed, F. (2013). *The impact of ECC's scalar multiplication on wireless sensor networks.* Paper presented at the Programming and Systems (ISPS), 2013 11th International Symposium on.

Raymond, D. R., Marchany, R. C., Brownfield, M. I., & Midkiff, S. F. (2009). Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE transactions on vehicular technology, 58*(1), 367-380.

Sarkar, A., & Murugan, T. S. (2016). Routing protocols for wireless sensor networks: What the literature says? *Alexandria Engineering Journal, 55*(4), 3173-3183.

Younis, O., Krunz, M., & Ramasubramanian, S. (2006). Node clustering in wireless sensor networks: Recent developments and deployment challenges. *IEEE network, 20*(3), 20-25.

Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN), 2*(4), 500-528.