Scientific Journal of Review (2016) 5(10) 464-473
ISSN 2322-2433
doi: 10.14196/sjr.v5i10.2213

Contents lists available at Sjournals
Scientific Journal of **Review**
Journal homepage: www.Sjournals.com

Review article

New methods based on genetics in wireless sensor networks with contemplating data security

Nader Abbasi[a,*], Shina Hekmat[b], Atefeh Heidaryan[b], Abolfazl Torghi Haghighat[c]
[a]*Guilan University, Guilan, Iran.*
[b]*Payame Noor University, Tehran branch, Tehran, Iran.*
[c]*Islamic Azad University, Qazvin branch, Qazvin, Iran.*

*Corresponding author; Guilan University, Guilan, Iran.

ARTICLE INFO

Article history,
Received 14 September 2016
Accepted 13 October 2016
Available online 20 October 2016
iThenticate screening 17 September 2016
English editing 11 October 2016
Quality control 17 October 2016

Keywords,
Wireless sensor networks
Genetic algorithms
Data security
Aggregation

ABSTRACT

Nowadays, one of the major issues in wireless sensor networks (WSNs) is data security. Often, data security issue is associated with data aggregation. Using this kind of network in sensitive areas, especially in military environments, without contemplating data security creates main problems. A great number of researches have been conducted in recent years. For example, issues such as coding and use of key and optimum routing based on data security have been taken into consideration. Each method makes use of different parameters that have created strengths and weaknesses. The present research is intended to consider the new ideas presented in this field. Then, to contribute to strengths and weaknesses existing in these methods, we present new ideas. The routine is to study new methods in a valid research. Issues such as data integration, individual or multiple data transfer, the impact of genetic algorithms on data security, encoding and cryptography, secure data aggregation based on fuzzy logic, etc have been discussed thoroughly.

1. Introduction

Wireless sensor networks consist of a number of nodes. The nodes' main task is to collect environmental information and to transfer them to a base station (BS). In some applications, data transmission to the BS is performed through the single-hop method and in some applications, it is done through the multi - hop method. The difference between the two methods is a network structure. Often, the high-density networks are used for multi-hop method. However, in each of these two methods, the network is divided into different areas called clusters. Each cluster has one or more than one cluster heads (CH). The transmission data mode is in such a way that information collection for each cluster is first done by cluster heads. Then, the CH sends them to the BS or to the higher CH. The most important issue that can jeopardize the data security is vital cluster heads. Figure1 shows a vital cluster head.

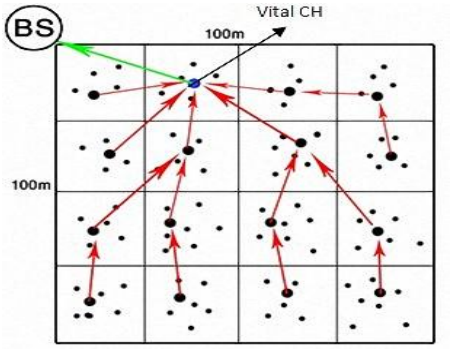

Fig. 1. Vital node in the WSNs.

As shown in Figure 1, the demolition of vital cluster head destroys all data on the network. This problem often occurs in wireless sensor networks that have just one cluster head in each cluster. The Genetic algorithm (GA) can easily solve this problem. The GA is used by operators for optimization. The benefit of the GA, Compared to other optimization methods, is that non-optimum points in the previous steps enter into the next steps. This work is done for each round. This method is suitable for multi-level networks because multi-level networks are based on vital nodes. The GA can easily select several cluster heads in each cluster.

2. Genetic algorithm

There are some basic differences between common methods and Genetic algorithm. The GA has four operators, including encoding, selection, combination and mutation. Also, the GA has a fitness function. The fitness function is created by suitable conversion of the target function. The target function is a function that must be optimized. The most important of all stages in the GA is encoding stage. The GA often uses binary coding. In this method, chromosomes consist of bit strings, with each bit including 0 or 1. The combination is a process by which old generation chromosomes are combined together. This action creates a new generation of chromosomes. Selection operator is used before combination round. Overall, Selection operator selects two populations in combination to create new children.The mutation operator changes a gene. This operator makes the GA grow rapidly.

3. New approaches in the WSNs

There are many approaches to data security consideration. But these methods have strengths and weaknesses. Our main aim is to review new methods in WSN that have been presented years ago.

3.1. Security in data aggregation

There are so many special services in WSN that these services are in the application layer. Two of these services are security and data aggregation (Cheng and Yin, 2008). In the WSN, nodes receive environment data and send them to the BS. Nodes close to each other will probably receive the similar data. If each of them tends to

send data to the BS, a lot of energy will be wasted. So, nodes closer to the BS (or CHs) try to collect the farther nodes information. Finally, the CHs send aggregated data to the BS.

If a saboteur node exists in trajectory of information, the BS is likely to receive incorrect information. Also, saboteur node can change information of other nodes. This makes an incorrect total aggregation. To cope with these attacks, we can draw upon the following three ideas:

1- Prevention of false aggregation of previous nodes in saboteur nodes.
2- The nodes will be made to confirm their participation. In this way, a lot of attempts have been made to provide an acceptable security for data aggregation.
3- The aggregation occurs in some of the nodes.

One of the presented methods in this field is RHC method. This method is provided by Shih et al. This method is based on data aggregation and security. Hierarchical clustering is used in this method. Main centralization of the RHC is on the WWSNs (wide wireless sensor networks). This method is provided for ring WSNs with 1000 meter radius. Aggregation function in this method is equal to: $f_a(x) = \beta x$

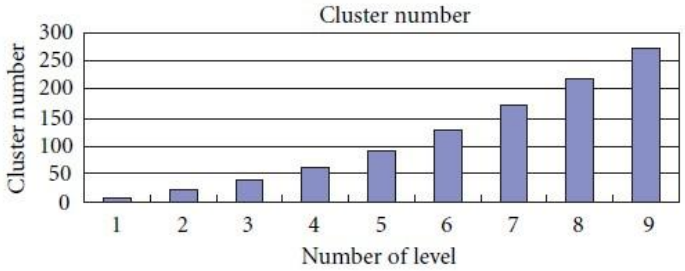

Fig. 2. Number of the CHs (Number of cluster heads for various levels).

As shown in Figure 2, the number of CHs increases with an increment of level. This makes data aggregation at the end levels (Where is high data volumes) better. This means that the lifetime of network and data security is, based on this idea, guaranteed since, by this method, the network has more than one CH at the end levels. Figure 1 shows the end level of network with one CH. As shown in Figure 1, CH of end level is a vital CH. Loss of this CH will lead to loss of all network information. The benefit of RHC method is that, in the final levels, there is not a vital CH.

3.2. Security at the network layer

The main task of the network layer is routing. For secure routing, methods not specific to sensor networks have been proposed. Overall, to create a secure trajectory, we must make changes to network layer structure. One of these approaches is creating a secure routing algorithm. One of these methods is H. M. Choi method and et al. Simulation results show that this method has improved network lifetime to 20%. In this method, nodes are to send a byte of data Consume 16.25µj of energy. This is done while nodes receive a byte of data Consume 12.25µj of energy. In this method, sent and received power amounts are inappropriate because high energy for Preparing of primary energy in a network with large number of nodes is needed. To guarantee the security, this method uses an ACK message (similar to the TCP / IP protocol). The fundamental difference between this approach and previous methods is the ACK message. The ACK message's main task in this method is to control network traffic. Figure 3 shows the proposed algorithm.

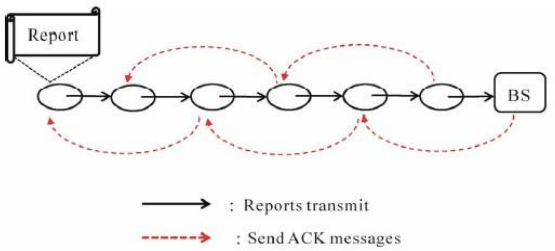

Fig. 3. Control of network traffic in presented algorithm.

Another advantage of this method is that this method also checks the node's false reports. Thus, the issue of false information aggregation is solvable.

3.3. Use of encoding

The advantage of encoding is resistance against uncoordinated attacks. One of these methods is SEAD. This method uses symmetric encoding and mixed sequence numbers and is resistant against uncoordinated attacks, but it is weak against coordinated attacks. The other method is ARAN that hinders repeated attack using the asymmetric encoding. This method is vulnerable to coordinated attacks. The data in the WSNs are important in terms of authentication, data integrity, and more security to be used in data encoding (data encryption). Due to the limitations of these networks, symmetric key encoding is used more than unsymmetrical key encoding. To use asymmetric encoding methods, the works that can be pointed to ellipsoid bends method, are done. For the use of symmetric-key encryption, it is necessary to nodes to have shared key. Historically, the first work that was done in the areas of network security is key management protocols. This method is one of the most basic necessary tools for security. In sensor networks, due to the applications and Special features, generally General security would not be appropriate and we must think to the node to node security.

3.4. The use of probabilistic and deterministic algorithms

Algorithms are divided into two categories: deterministic and probabilistic algorithms. In the probabilistic algorithms, some nodes get random key. This will ensure a secure connection. EG02, RJR08, UL09 and CPS03 methods are based on a probabilistic key distribution algorithm. Keys in the sensor networks distribute as a grouping, networking and paired. An assumption that can help to key distribution, it is that nodes be aware of their location. It is somewhat difficult, but there is a one mode that we assume nodes are in areas as a group. Also, we must assume that nodes are aware of their location (approximate location instead of the precise location).
Key management in sensor network consists of four steps:

1- Key distribution: In the factory, private keys should be placed on the sensors or at the first sensors product keys themselves.
2- Key discovery: With the network starting to work, each sensor node needs to organize its neighbors in order to share a key.
3- Key creation: Neighbors that have not a common key with own private key and transmission on the channel can reach a common key.
4- Updating the key: Nodes need to be updated since they have a limited lifetime in the network.

3.5. Optimal routing in military areas

The accurate information on the position, changes and developments of friendly and enemy forces are main parameters in the control of forces. Wireless sensor networks can collect and process sensitive data in a dangerous environment. The use of wireless sensor networks in search operations and controlling the battlefield destruction of enemy forces, estimation of damage, espionage operations, warning systems are not easy. So the protocols for such networks must adhere to the above limits. Also, due to the sensitive nature of the data in the battlefield, security of protocol is a main parameter in selection of optimum protocol.

Table 1
Comparison between protocols.

Protocol name	Structure	Energy consumption	Security	Efficiency	Lifetime
SPIN	Flat	High	Very low	Low	Low
LEACH	Clustering	Low	Medium	Low	Low
HDA	Hierarchy	Medium	Medium	Low	Low
MECH	Hybrid	Low	Medium	Low	Low
FDCBR	Hybrid	Low	Medium	Good	Excellent
SACBR	Hybrid	Low	High	Good	Excellent

3.6. Routing of based on secure data aggregation

The other routing method is EEHA method. This method uses the secure data aggregation for routing. This method is based on energy and high efficiency. The main idea in this method is the secure transmission of data between nodes. Generally, secure transmission results in optimum routing. Simulation result shows that the efficiency of this method, as compared with those of previous similar methods, has been improved. Figures 4 and 5 show the time interval difference in EEHA method.

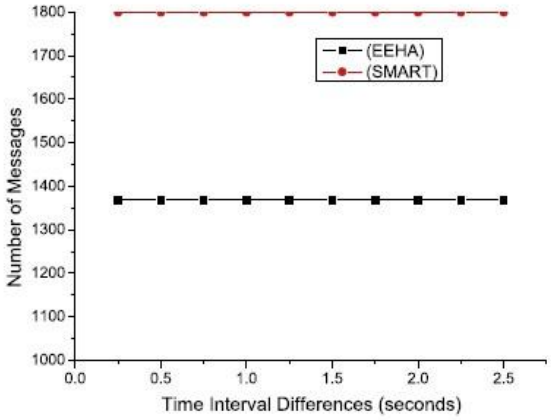

Fig. 4. Time interval difference (number of messages).

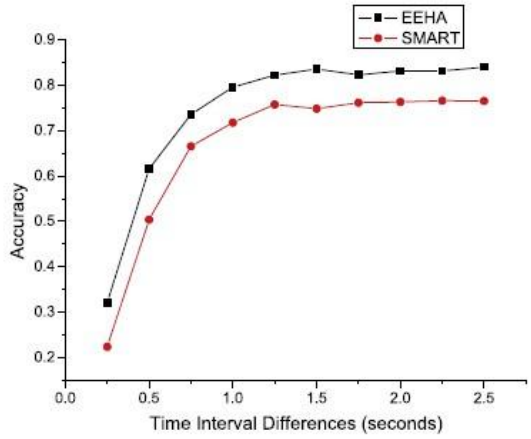

Fig. 5. Time interval difference (accuracy).

As figures shown, EEHA apply a true time structure. This method has two flaws:

1- Diagram of data security is low.
2- In this method, it is not specified that has been improved the death of the first node and the network lifetime.

3.7. Secure data aggregation based on fuzzy logic

The important features of fuzzy-based methods are that these methods include steps or phases. It means that the accuracy of the algorithm is based on phases. This means that the algorithm ends when all phases are implemented. One of the problems with this approach is that these algorithms have high time complexity. It means that algorithms must be implemented in phases and if the phases are not fully implemented, the algorithm is incomplete. PESRP and FBSDA methods are based on fuzzy logic. An important feature of this method is that the energy model is heinzelman energy model. Table 2 shows the simulation parameters in this method.

Table 2
Simulation parameters.

Number of nodes	30
Size of network	500 m*500 m
Round	50
Length of message	512byte
Initial energy	5.1J
Number of clusters	4

Figures 6, 7, 8 and 9 show the transfer rate.

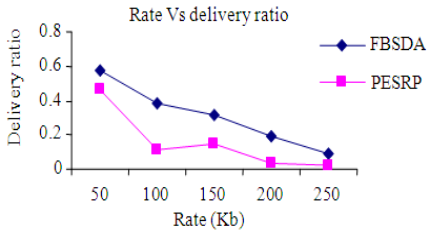

Fig. 6. Transfer rate with delivery ratio.

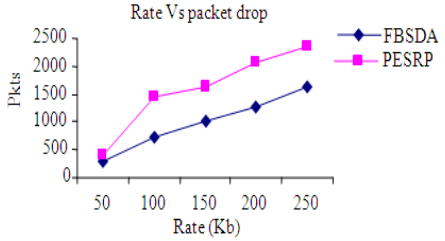

Fig. 7. Transfer rate with packet drop.

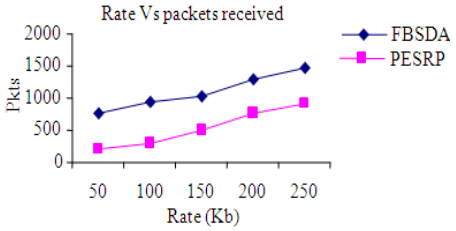

Fig. 8. Transfer rate packet received.

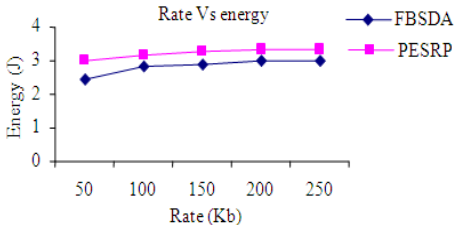

Fig. 9. Transfer rate with energy.

Although the transfer rate is improved in this method, there are similar methods that have better transfer rates (for example: EEHA method). Another problem of this method is the initial energy of each node that is very high.

4. New ideas proposed based on genetics

In this section, we will try to present new ideas based on GA.

4.1. The use of key distribution algorithms based on the GA in the WSN

This type of algorithm can be based on needs (uncertain or probabilistic) or network segmentation. Also, these methods can, in a hierarchical network, distribute the keys.

4.2. New key management algorithm or improving of existing algorithms in terms of safety / efficacy in order to update the key

These algorithms can be deterministic, probabilistic, area or site-independent, flat and hierarchical.

4.3. Methods based on the security of transmitted packets

The appropriate choice of the CH in the WSN, can be problematic, especially in the high density networks. Genetic algorithms can select the CH appropriately in crowded areas. GA has the property that if one of the operators fails to reach the optimum solution, it can be optimized by another operator.

4.4. Approaches based on the identification of healthy nodes

In the WSN, the main goal is data aggregation by nodes and send them to the BS. A node wastes a lot of energy if it tends to send data to the BS separately. It is better that the node closer to the BS collects information from farther away nodes. This method has a main problem: There may be a malicious node in the way data transmission. This node can inject the false data in the network. Also, this node can change information of other nodes. This makes an incorrect data aggregation. One of the approaches to addressing this problem is that previous nodes do not send any information to malicious nodes. The GA can solve this problem by selecting suitable cluster heads. Because the GA selects more than one CH during the downtime, replace the next CH.

4.5. Energy-aware data aggregation algorithms

One of the fundamental problems in wireless sensor network is high node energy. This problem emerges in clusters. It is better that clustering algorithms be aware of each energy level. This method is effective when the primary energy set for the nodes is considered small. The GA can better select high energy nodes. One example of these methods is that the common nodes equal to zero bit and cluster heads equal to one bit.

4.6. The use of hybrid algorithms

The hybrid approach is a method based on hybrid parameters. One of the hybrid ideas can be improved in the previous methods. So, new methods are based on new parameters, including: distance - energy, distance - density and density - energy. Hybrid algorithms have high runtime, but they can improve the data aggregation. For example, ant colony and bee colony methods can achieve a significant improvement.

4.7. Density-based clustering

This type of clustering methods is based on the principle that the clusters are areas with high density that a high density area covers low density areas. So the issue of data security in the high density areas is solvable. To implement clustering in the high density networks, we must pay attention to the following:

- Density of local points
- Density in the direct access

The GA is the best choice in the high density areas. For example, we can draw upon the idea of the GA for replacement of a node. Important advantages of the GA are as follows:

- Clusters can be of arbitrary shapes.

- The number of clusters is determined by the clustering operation automatically and simultaneously.
- Noise detection is very efficient.
- Security increases, especially where the auxiliary nodes are used.

4.8. The Use of combination genetic algorithms

Recently, with more ways that have been proposed about data security, they assume only one parameter. For example, the use of parallel genetic algorithms (PGAs) or serial genetic algorithms (SGAs). The issues such as data security, distance, energy, density are the issues that must be examined together and this is not possible by the single genetic algorithms. One of the ideas that can be offered is the use of the PGAs and the SGAs Simultaneously. For example, one of them assumes the issues such as distance or energy and the other method assumes data security.

4.9. The volume of data

Most of the proposed methods that can assume the data security are only able to transmit small amounts of data. The GA can solve this problem easily. The reason is that the GA can select nodes that have more energy or better position than other nodes. In addition, as nodes' energy increases, the sent and received data size increases. So the network can increase the volume of sent and received data. It should be noted that this method is suitable for the methods that have used the data security.

4.10. Using previous similar methods

There are many methods that follow the data security seriously. The methods based on the GA have a cost function. Often, the function of cost, is called fitness function. We can improve the fitness function in previous methods.

5. Conclusion

In this research, we, with the aid of new ideas in the previous similar methods, made an attempt to present a new solution. The issues such as network lifetime, data security, vital cluster heads and data aggregation were studied. So, we tried to present new ideas. We had more focus on the GA-based methods. For this reason, we reviewed several methods based on GA. Finally, we provided optimal solutions, using the strengths and weaknesses of the methods.

References

Abbasi Dezfouli, M., Mazraeh, S., Yektaie, M.H., 2012. The new method of concealed data aggregation in wireless sensor: A case study. World. Acad. Sci. Eng. Technol., 61.

Almamani, I., Almashakbeh, E., 2010. A power efficient secure routing protocol for wireless sensor networks. WSEAS Trans. Comput., 9, 1042-1052.

Anindita, R., Debashis, D., 2012. Data aggregation techniques in wireless sensor network: A survey. Int. J. Eng. Innovat. Res., 1(2), ISSN: 2277-5668.

Bandyopadhyay, S., Coyle, E.J., 2003. An energy efficient hierarchical clustering algorithm for wireless sensor networks. In Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies, San Francisco, Calif, USA, April, 1713-1723.

Basavaraj, S.M., Siddarama, R.P., Mytri, V.D., 2012. An adaptive energy efficient forwarding data aggregation and QoS protocol for wireless sensor networks. Int. J. Comput. Appl., 46(20), 0975-8887.

Bhoopathy, V., Parvathi, R.M.S., 2012. Secure authentication technique for data aggregation in wireless sensor networks. J. Comput. Sci., 8(2), 232-238.

Bhoopathy, V., Parvathi, R.M.S., 2012. Securing node capture attacks for hierarchical data aggregation in wireless sensor networks. Int. J. Eng. Res. Appl., 2(2), 466-474.

Chamam, A., Pierre, S., 2010. A distributed energy-efficient clustering protocol for wireless sensor networks. Comput. Elect. Eng., 36, 303–312.

Cheng, M.X., Yin, L., 2008. Energy-efficient data gathering algorithm in sensor networks with partial aggregation. Int. J. Sensor. Network., 4(1-2), 48-54.

de Meulenaer, G., Standaert, F.X., 2010. Stealthy compromise of wireless sensor nodes with power analysis attacks. MOBILIGHT, 229-242.

Elangovan, G., Perinbam, J.R., 2012. Wideband eshaped microstrip antenna for wireless sensor networks. Am. J. Appl. Sci., 89-92.

Eldefrawy, M.H., Khan, M.K., Alghathbar, K., 2010. A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. International conference on anti-counterfeiting security and identification in communication (ASID), 1-6.

Faye, S., Myoupo, J.F., 2011. An ultra hierarchical clustering based secure aggregation protocol for wireless sensor networks. Adv. Inform. Sci. Serv. Sci., 3(9), 309-319.

Gugelmann, D., Sommer, P., Wattenhofer, R., 2010. Poster abstract: Reliable and energy-efficient bulk-data dissemination in wireless sensor networks. In Proceedings of SenSys'10, November, 3-5.

Han, J., Kamber, M., Pei, J., 2006. Data mining concepts and techniques. Second edition. Elsevier Inc.

Heinxelman, W., Chandrakasan, A., Balakrishnan, H., 2000. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33th Hawaii International Conference on System Science.

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.

Hevin Rajesh, D., Paramasivan, B., 2012. Fuzzy based secure data aggregation technique in wireless sensor networks. J. Comput. Sci., 8(6), 899-907.

Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., Silva, F., 2003. Directed diffusion for wireless sensor networking. IEEE/ACM Transactions on Networking, 11(1), 2-16.

Kohno, E., Ohta, T., Kakuda, Y., Aida, M., 2011. Improvement of dependability against node capture attacks for wireless sensor networks. IEICE Transactions, 94-D(1), 19-26.

Kuhn, F., Moscibroda, T., Wattenhofer, R., 2004. Initializing newly deployed ad hoc and sensor networks. In Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom'04), September, 260-274.

Ren, K., Lou, W., Zhang, Y., 2008. LEDS: Providing location-aware end-to-end data security in wireless sensor networks. IEEE Transactions on Mobile Computing, 7(5), 585-598.

Li, D., Zhu, Q., Chen, W., 2011. Efficient algorithm for maximum lifetime many-toone data aggregation in wireless sensor networks. Int. J. Sensor. Network., 9(2), 61-68.

Li, H., Lin, K., Li, K., 2010. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. Comput. Comm.

Li, N., Li, S., Fang, X., 2010. Adaptive data aggregation mechanism based on LEACH protocol. Proceedings of AIAI.

Madden, S., Frankin, M.J., Hellerstein, J., Hong, W., 2002. TAG: A tiny aggregation service for ad-hoc sensor networks. In Proceedings of the 5th Symposium on Operating Systems Designand Implementation (OSDI '02), Boston, Mass, USA, December, 131-146.

Maraiya, K., Kant, K., Gupta, N., 2011. Efficient cluster head selection scheme for data aggregation in wireless sensor network. Int. J. Comput. Appl., 23(9), 0975-8887.

Matrouk, K., Landfeldt, B., 2009. Prolonging the system lifetime and equalising the energy for heterogeneous sensor networks using RETT protocol. Int. J. Sensor. Network., 6(2), 65-77.

Mhatre, V., Rosenberg, C., 2004. Design guidelines for wireless sensor networks: Communication, clustering and aggregation. Ad Hoc Networks, 2(1), 45-63.

Muthukarpagam, S., Niveditta, V., Neduncheliyan, S., 2010. Design issues, topology issues, quality of service support for wireless sensor networks. Survey and Research Challenges' International Journal of Computer Applications, 1(6), 1-4.

Ozgu¨r Tan, H., Korpeoglu, I., Stojmenovic, I., 2011. Computing localized power-efficient data aggregation treesfor sensor networks. IEEE Transactions on Parallel and Distributed Systems, 22(3), 489-500.

Ozgu¨r Tan, H., Korpeoglu, I., Stojmenovic, I., 2011. Computing localized power-efficient data aggregation trees for sensor networks. IEEE Transactions on Parallel and Distributed Systems, 22(3), 489-499.

Patil, N.S., Patil, P.R., 2010. Data aggregation in wireless sensor network. IEEE International Conference on Computational Intelligence and Computing Research.

Ray, A., De, D., 2012. Energy efficient cluster head selection in wireless sensor network. Proc. IEEE Recent Advances in Information Technology (RAIT), ISM Dhanbad-March.

Sethi, H., Prasad, D., Patel, R.B., 2011. EIRDA: An energy efficient interest based reliable data aggregation protocol for wireless sensor networks. In Proceedings of International Journal of Computer Applications, 22(7).

Sicari, S., Alfredo Grieco, L., Boggia, G., Coen-Porisini, A., 2012. DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks. Preprint Submitted to Elsevier, 22.

Su, T.S., Huang, M.W., Li, W.S., Hsieh, W.S., 2012. Aggregation scheme with secure hierarchical clustering for wireless sensor networks. Int. J. Distr. Sensor. Network., Article ID 162347.

Sun, L., Li, J., Chen, Y., Zhu, H., 2005. Wireless sensor networks (in Chinese). Tsinghua University Press, 5.

Vamsi Krishna Venkata Naga Nandanavanam, 2010. Energy-efficient reliable sensor-to-sink data transfer for wireless sensor networks. Scholar Works, Boisestate.

Vass, D., Vidacs, A., 2007. Distributed data aggregation with geographical routing in wireless sensor networks. Pervasive Services, IEEE International Conference on July.

Wu, D., Hon Wong, M., 2011. Fast and simultaneous data aggregation over multiple regions in wireless sensor networks. IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews, 41(3).

Wu, K., Dreef, D., Sun, B., Xiao, Y., 2007. Secure data aggregation without persistent cryptographic operations in wireless sensor networks. Ad Hoc Networks, 5(1), 100-111.

Wu, K., Liu, C., Xiao, Y., Liu, J., 2009. Delay-constrained optimal data aggregation in hierarchical wireless sensor networks. Mobile Networks and Applications, 14(5), 571-589.

Yang, Y., Cardei, M., 2010. Delay-constrained energy-efficient routing in heterogeneous wireless sensor networks. Int. J. Sensor. Network., 7(4), 236-247.

Younis, O., Fahmy, S., 2004. HEED: A hybrid energy-efficient distributed clustering approach for ad hocsensor networks. IEEE Trans. on Mobile Computing, 3(4), 660-669.

Yu, Y., Krishnamachari, B., Prasanna, V.K., 2008. Energy-Latency tradeoffs for data gathering in wireless sensor networks. Proceedings of International Journal of Sensor Networks, 4(1/2), 48-54.

Zhang, J., Zhang, H., Jia, X., 2012. A data-aggregation-centric wireless Sensor Network. Routing Architecture. J. Inform. Comput. Sci., 9(3), 635–642.

How to cite this article: Abbasi, N., Hekmat, S., Heidaryan, A., Torghi Haghighat, A., 2016. New methods based on genetics in wireless sensor networks with contemplating data security. Scientific Journal of Review, 5(10), 464-473.