Middle-East Journal of Scientific Research
24 (Recent Innovations in Engineering, Technology, Management & Applications): 41-47, 2016
ISSN 1990-9233; © IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.RIETMA108

Genetic Algorithm Based an Optimized Trust Based Traffic Analyzer for Wireless Sensor Networks to Detect Malicious Activities

S. Vijayarangan, S. Suresh and J. Megalai

Department of Computer Science and Engineering,
Priyadarshini Engineering College, Vaniyambadi, India

Abstract: Wireless sensor network is dynamic and follows multi-hop based communication, it is essential to provide an IDS software to avoid malicious behavior and data loss. The existing software like packet sniffer can sniff all or just parts of the traffic from a single node in the network. A few methods were proposed to avoid traffic narrowing using switches to gain access to traffic from other systems on the network but it is taking more time and cost. This paper discussed an Optimized Trust Based Traffic Analyzer (OTBTA) for wireless sensor networks in order to provide an efficient intrusion detection system where the optimum trusted traffic is obtained by Genetic Algorithm. OTBTA used as optimal intrusion detection system where it focuses on the packet sniffing and its working only for best trusted nodes in the network. OTBTA observe the working behavior, packet format, timing and mainly optimally whether the nodes are trusted nodes or not. The simulation of OTBTA is carried out in Network Simulation software and the results are compared with the existing IDS such as LBIDS and DAD results to evaluate the performance.

Key words: Intrusion Detection System · Packet Analyzing · Traffic Analyzer · Wireless Sensor Network · Trust Management

INTRODUCTION

Background Study: Wireless sensor networks are classified into ad-hoc networks, cellular networks and hybrid networks. Ad-hoc networks are independent to infrastructure and use multi-hop communication, cellular networks are depending on infrastructure and uses single-hop links. While transmitting data through single-hop or multi-hop it is known that some of the un-known nodes are participating in the data transmission. Un-known nodes may change its behavior as malicious by itself or compromised by other malicious nodes occur in the network. WSN networks are applied in various serious areas such as military, ecology, building and industrial automation, surveillance monitoring and wild-life monitoring. In order to improve the efficiency of the WSNs as secured, the security aspects of the WSN should be considered. Because of the characteristics of the WSN, the available security methods are utilized only in traditional networks which cannot be applied directly into the network. This affects the research which aims to propose a novel high secured solution to WSN.

The attacks in WSN are divided into external and internal attacks. The internal attacks performed from the devices inside the network, whereas the external attacks performed from the devices outside the network [1]. By applying authentication authorization, providing public key, private key these attacks can be controlled. Also the attacks can be classified into passive and active attacks [2]. Passive attacks are concentrating on collecting the sensitive information to destroy the data, whereas active attacks destroy the data directly. One of the main and important attacks behaves as active as well as passive is jamming attack [3, 4].

Various research studies presented different mechanisms, techniques and IDS for providing secured data transmission in WSN. Some of the metrics decides the level of the software which decides the performance. According to the load of the system the grad of service (GoS) [5], performance metrics quality of service (QoS) [6, 7] is adopted to evaluate the systems. Most of the authors [8-10] concentrated on analyzing the data flow from source to destination instead of analyzing each individual node in the network. The behavior of the

Corresponding Author: S. Vijayarangan, Department of Computer Science and Engineering,
Priyadarshini Engineering College, Vaniyambadi, India.

individual nodes can be analyzed by computing the attitude of the nodes. Leung et al [8] proposed a deterministic fluid model for analyzing the traffic of WSN. But this model avoids the behavior of the individual nodes and treats them as continuous fluid and it takes more time only for analyzing process. Gribaudo *et al*. [9] proposed a method which monitors the behavior of large-scale WSN which is more complex to analyze, where the existing fluid approach finds difficult to analyze the traffic flow. Silvester *et al*. [11] proposed a slotted aloha protocol to employ the traffic flow among huge number of nodes in large-scale network. Franceschetti *et al*. [12] used a contention slot based data transmission to monitor the packets.

Various studies discussed about the WSN deployment where those studies used for estimating the network lifetime [13-15]. Few existing studies also discussed about the network lifetime estimation [13, 16]. The works discussed in [13, 16] was extended for multi-hop communication described in [17]. The author in [18] set a lower bound and upper bound values to investigate the network lifetime. A duty cycle based WSN is investigated by the author in [19]. A new MAC protocol discussed in [20] analyzes the issues in terms of network lifetime in WSN.

Problem Statement: Several approaches were proposed as intrusion detection system, but all the systems so far are not completely flawless. So still finding a good solution for intrusion detection continues. In this searching, here it is aimed to propose a complete solution through a trust based IDS where nodes are completely converted as trusted nodes during the communication and then traffic data, function and participating nodes are analyzed among source and destination nodes. The existing GA based IDS [21] evaluate the parameters as optimum in order to filter only the traffic data with low complexity. But GA based IDS suites mainly for large scale networks and there is a need for a common solution suitable to all kind of networks (small scale to large scale).

Some of the existing approaches use GA for deriving classification rules [22-25]. GA always utilized to select the optimum features than other artificial intelligence techniques were used to derive acquisition of rules [26-28]. Some of the other papers [29-32] proposed methodologies related IDS, having certain level of impact in network security. But in this paper, the proposed OTBTA - IDS have two main stages such as: (i). collecting the optimum trusted nodes to discover the route in order to eliminate malicious nodes in the network and (ii). Analyzing the network traffic data for eliminate malicious packet.

Proposed System: The proposed system comprises of two main stages as finding the optimum nodes are trusted nodes and investigating the traffic data in order to detect and eliminate the malicious activities in the network. The entire functionality of the proposed model is shown in Figure-1 given below.

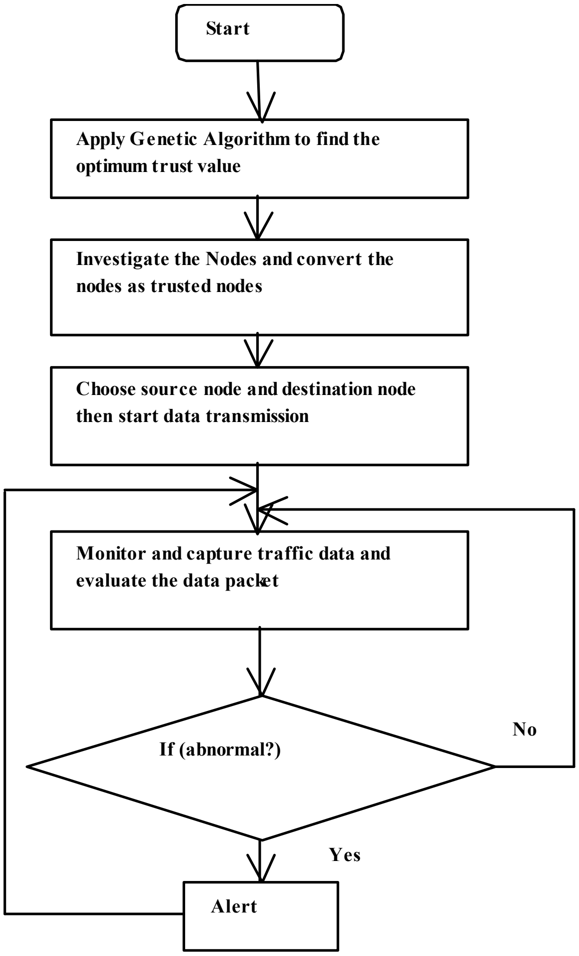
Start
Apply Genetic Algorithm to find the optimum trust value
Investigate the Nodes and convert the nodes as trusted nodes
Choose source node and destination node then start data transmission
Monitor and capture traffic data and evaluate the data packet
If (abnormal?)
No
Yes
Alert

Fig. 1: Proposed System Model

The proposed system is designed according to the trust nature of the nodes and the traffic data. It is considered that the network G has deployed with N number of nodes within the area [X, Y] randomly. All the nodes N_i where i=1,2,…, k is assigned with a trust value=0. The trust value is verified by the location, response time, neighbour node support value and trust value of load transmitted in the network. The optimum trusted nodes are selected by Genetic Algorithm by comparing their parameters with the fitness function values. The optimum node selection by GA is shown in Figure-2. The network is represented as:

$G= \{N_1,N_2,. . .,N_k,\} \ \forall i = 1 \ to \ k$

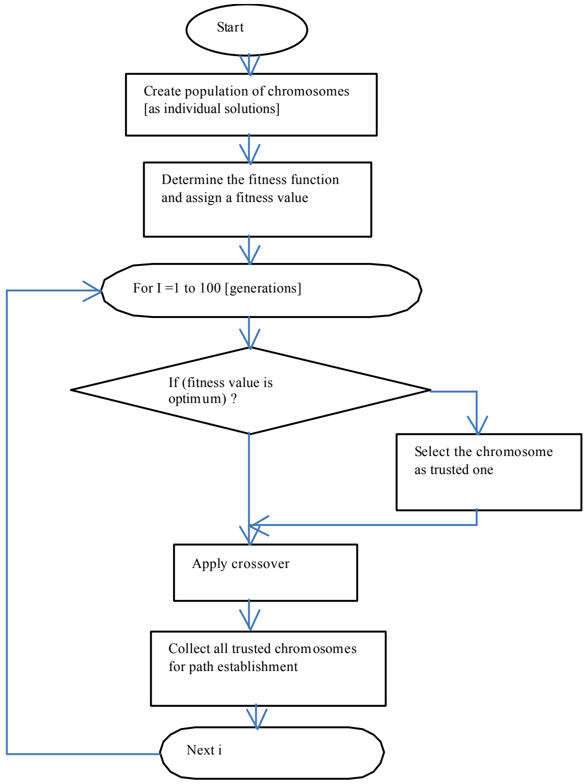
Start
Create population of chromosomes [as individual solutions]
Determine the fitness function and assign a fitness value
For I =1 to 100 [generations]
If (fitness value is optimum) ?
Select the chromosome as trusted one
Apply crossover
Collect all trusted chromosomes for path establishment
Next i

Fig. 2: Genetic Algorithm Based Trusted Node Selection

Each node is deployed in the location, where (x_i, y_i) is the location of the ith node. The deployed location by the base station is fixed and it is stored in a database for verification, but the node can move within the network region. All the nodes received a HELLO message from BS and it compel to reply a HI response message. The response time of each node is also stored in database for further verification. Then each node is assigned with a unique IP address for identification. While deploying the nodes in the network, the packet format is also assigned in a specific manner where the network follows. Here it is considered that a wireless multi-hop network with a limit where the number of nodes is extremely large. So that, the route discovery can contains a large number of intermediate nodes among source and destination nodes. To provide a complete common solution to detect malicious activities the distance among the source and destination nodes and the mean distance between the neighboring nodes are separated strongly. The load assigned to each node is limited within a lower and an upper bound values (for example: lower bound is 10 KB and the upper bound is 20 KB). The database structure is shown in Table-1 and the calculation of the trust value is given below.

The trust value of each node can be computed as

$$TV_t = TV_{loc} + TV_{restime} + TV_{nnsup} + TV_{load} + TV_{intttime} \qquad (1)$$

where

$$\begin{cases} TV_{inittime} = 1 \\ TV_{loc} = 1 \quad if\ (Node_i(loc) == Reg(loc))then \\ \quad else \\ \quad TV_{loc} = 0 \\ TV_{restime} = 1 \quad if(Node_i(RES - TIME) < res_{time}) \ then \\ \quad else \\ \quad TV_{restime} = 0 \\ TV_{nnsup} = 1 \quad if\ (Node_i(nnsup) == \text{"Good"}\ ) \ \text{then} \\ \quad else \\ \quad TV_{nnsup} = 0 \\ TV_{load} = 1 \quad if\ (Node_i(load) \leq preKB\ ) \quad then \\ \quad else \\ \quad TV_{load} = 0 \end{cases} \qquad (2)$$

The total trust value of a trusted node is the sum of the trust values calculated dynamically using the equation (1) where the trust dependent values are calculated using equation (2). If the trust value of a node is 5 then the node is a trusted node, else it is un-trusted node. The trusted node is elected in terms of their trust value and it is done by applying the fitness function. The main objective function OF is selecting the minimum distance based trusted path between S and D.

Objective Function (OF) = minDist(trusted-path, S, D)

The individual optimum nodes are selected by evaluating the fitness function as: Fitness Function (FF) = [Node (TV_i = **5**].

Once the node trust value is matched with the FF value then it can be selected as optimum trusted node in the network. The routing protocol used in this paper is AODV since the network used in this simulation is WSN. Here the proposed IDS deployed with the AODV discover the route only through trusted nodes. Once route discovered through trusted nodes, data transmission is started.

Table 1: Database Structure

Node-number	Node-Location	Node-IP address	Node Response Time	Node-Trust Value

Simultaneously, the traffic data is analyzed by the proposed IDS mechanism. During the data transmission, the IP address of each node is verified initially. Each time while discovering the route all the intermediate nodes are compulsorily asked to submit their node number, IP address and location of the nodes which will be compared with the database values. If the values are matched one another than the node trust value will be calculated. During the trust value calculation, the neighbor node trust value is verified. If the trust value of the neighbour node is 1, then the present nodes *nnsup* = 1, else *nnsup* = 0. Similarly the route is discovered between the source node and the destination node only with the nodes having trust value is 5. If the route is having only trusted nodes then the data transmission is permitted. During the data transmission, the packet analyzation method is applied to identify abnormal packets.

The process of capturing network traffic and inspecting them closely to identify what is happening in the network. The inspection is on data packets, next hop ID, packet size, packet series number and flow id. If any mismatched values are detected in the traffic then it is recognized as abnormal data transmission. It mainly focuses on the pattern of the communication which represents the network activities. The traffic analysis mainly detects the abnormality in the traffic. Also time based request and response is verified among all the nodes and the base station. The packets, which node communicates with which node, when the nodes are communicating, the type of the messages, length of the messages and the time duration of the communication are mainly verified.

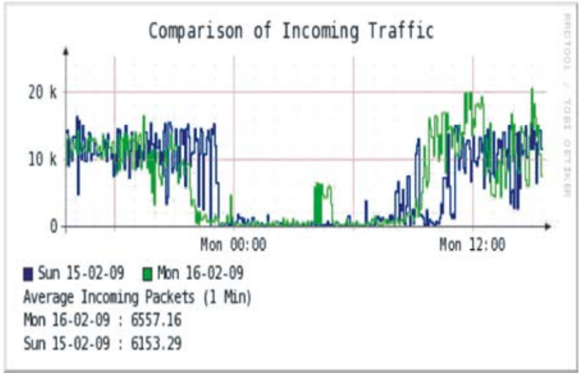

Fig. 2: Day wise Comparison of Incoming Traffic

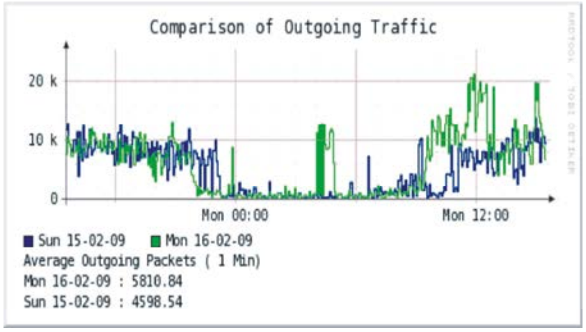

Fig. 3: Day wise Comparison of Outgoing Traffic

According to the traffic analysis, the abnormality is detected in terms of variation on the comparison parameters. The entire OTBTA is given in the form of an algorithm where it can be program in any computer language and it helps to evaluate the performance.

Algorithm_OTBTA ( )

```
{
    1.  Construct a network (G) where N numbers of
        nodes are deployed randomly.
    2.  Initialize all the parameters for all the nodes //
        parameters is given in Table-1
    3.  Choose source node S and destination node D
    4.  Use AODV algorithm to discover a route
    5.  do
    6.  apply GA to choose optimum nodes in the route
    7.  compute the trust values of each node
    8.  make the intermediate nodes to submit their data
        information
    9.  compare with database values
    10. If (any mismatched values found) then
    11. choose another intermediate node and GOTO 5
    12. else
    13.  establish connection from previous trusted
        node to the present trusted node
    14. while (destination reached)
    15. start data transmission
    16. for I = 1 to (total number of packets)
    17. analyze the packets
    18.  if (any mismatches between incoming packets
        and outgoing packets) then
    19.  Alert " Malicious occur"
    20.  else
    21.  next I
    22. Stop
}
```

The above algorithm is coded in TCL language and executed in network simulator environment. The simulation parameters are given in the following Table-2.

Simulation Settings:

Table 2: Simulation Parameters

Parameter	Level
Area	1200m x 1200m
Speed	1 to 25 m/s
Radio Propagation Model	Two-ray ground reflection
Radio Range	250 to 350 m
Number of Nodes	100, 200, 300, 400 and 500
MAC	802.11
Application	CBR, 100 to 500
Packet size	50
Simulation Time	100 s
Placement	Random
Malicious Population	Up to 5%

To prove that the OTBTA method is more effective and efficient than the existing method, the OTBTA algorithm is simulated in NS2. The network area size is 1200 x1200 and the number of nodes taken for simulation is 100 and the front end of the simulation is written in TCL and backend coding is written in. cc code. To evaluate the performance of the proposed approach the number of nodes is changed continuously and simulation results are verified.

RESULTS AND DISCUSSION

The simulation results include the number of malicious activity before and after deploying the OTBTA approach. Initially a visual interface for network topology is presented. In this interface, the OTBTA algorithm confirmed and detects the malicious node according to the node trust value and the packet comparison.

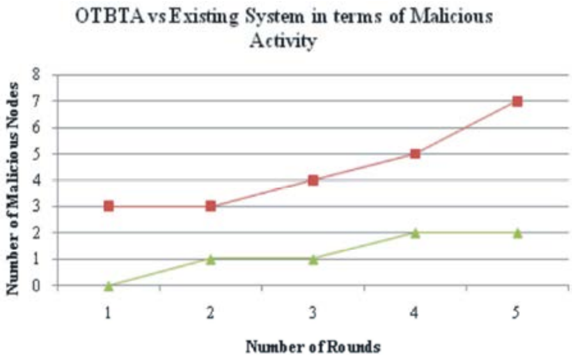

Fig. 4: OTBTA Vs. Existing System comparison in Malicious Activity

Figure-4 shows the number of malicious behavior occur in the network before and after implementing OTBTA. In order to detect malicious node all the parameters given in Table-1 and the data packets are investigated. The proposed system maintains and compares a DB to compare the parameters of each node in the network. When a node is detected as malicious then the node is blocked and an alert message is given to all the other nodes in the network. The malicious is reduced 10% lesser than the existing approach because OTBTA provide more preventing instead of detection.

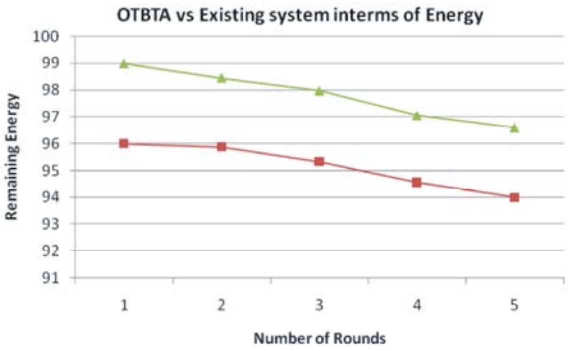

Fig. 5: OTBTA Vs. Existing System comparison in Energy

Figure-5 shows the remaining energy of each round where the number of nodes deployed is 10, 20, 30, 40 and 50. It shows that the OTBTA approach has longer life time then the existing system. This is because of unwanted node communication and data transmission is avoided by key comparison. Since nodes cant transmit data if they are not submitting valid ID and valid key and energy remains the same. The energy remains of the existing system in the 5th round is 95.12% where the remaining energy of OTBTA in the 5th round is 96.59%. Hence OTBTA saves more energy than the existing system.

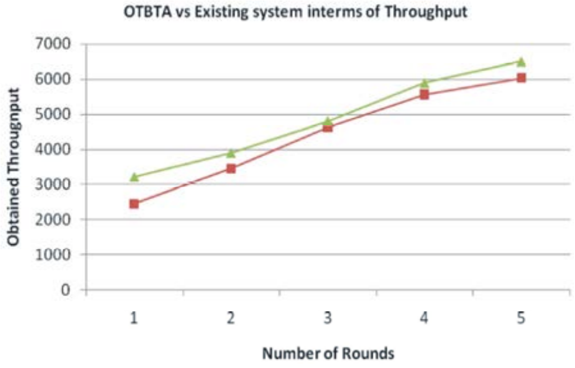

Fig. 6: OTBTA Vs. Existing System comparison in Throughput

The data transmission successfully is sending and receiving is named as throughput. The obtained throughput using OTBTA is better than the existing approach. Since more malicious activities occur in existing system, it spoils the data success transmission. Figure-6 shows the obtained throughput of each round. The throughput obtained by the existing system in the 5th round is 6123 packets where the OTBTA obtained in the 5th round is 6400 packets. Hence OTBTA obtained better throughput than the existing system.

CONCLUSION

OTBTA technique is derived from an existing LBIDS approach and it is used to verify the mutual authentication among the pair of nodes, going to transmit and receive their data. Since OTBTA uses the unique values for the entire node can provide proper investigation on the nodes and it cannot be duplicated by malicious node. The output of the OTBTA approach much more useful to the Wireless Networks based applications. This approach improves the quality of the network. The parameter comparison steps are preprocessing approach in a network to make the network is a trustable network and provides protection to the network. OTBTA simulation has proved that it is a general solution which prevents the data from malicious people by transfer the data only to the authorized people. This approach can produce good result in over-sized network also. OTBTA can give security without affecting the network quality in terms of throughput, energy and delay.

REFERENCES

1. Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks, 1(23): 293-315.
2 Roosta, T., S. Pai, P. Chen, S. Sastry and S. Wicker, 2007. Inherent security of routing protocols in ad-hoc and sensor networks, In Global Telecommunications Conference, GLOBECOM '07, pp: 1273-1278.
3 Xu, W., W. Trappe, Y. Zhang and T. Wood, 2005. The feasibility of launching and detecting jamming attacks in wireless networks, In Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, pages 46-57, New York, NY, USA, 2005. ACM.
4. Xu, W., K. Ma, W. Trappe and Y. Zhang, 2006. Jamming sensor networks: attack and defense strategies, IEEE Network Magazine, 20(3): 41-47.
5. Stasiak, M., M. Głabowski, A. Wiœniewski and P. Zwierzykowski, 2011. Modeling and Dimensioning of Mobile Networks: From GSM to LTE", New York: Wiley.
6. Cena, G., L. Seno, A. Valenzano and C. Zunino, 2010. On the performance of IEEE 802.11e wireless infrastructures for soft-real-time industrial applications, IEEE Trans. Ind. Informat., 6(3): 425-437.
7. Cucinotta, T., L. Palopoli, L. Abeni, D. Faggioli and G. Lipari, 2010. On the integration of application level and resource level QoS control for real-time applications, IEEE Trans. Ind. Informat., vol. 6, no. 4, pp: 479-491.
8. Leung, K., W. Massey and W. Whitt, 1994. Traffic models for wireless communication networks, IEEE J. Sel. Areas Commun., 12(8): 1353-1364.
9. Gribaudo, M., C. Chiasserini, R. Gaeta, M. Garetto, D. Manini and M. Sereno, 2005. A spatial fluid-based framework to analyze large-scale wireless sensor networks, in Proc. 2005 International Conference on Dependable Systems and Networks, pp: 694-703.
10. Toumpis, S. and L. Tassiulas, 2005. Packetostatics: deployment of massively dense sensor networks as an electrostatics problem, in Proc. 2005 INFOCOM, 4: 2290-2301.
11. Silvester, J. and L. Kleinrock, 1983. On the capacity of multihop slotted ALOHA networks with regular structure, IEEE Trans. Commun., 31(8): 974-982.
12. Franceschetti, M., O. Dousse, D. Tse and P. Thiran, 2004. Closing the gap in the capacity of random wireless networks, in Proc. 2004 International Symposium on Information Theory, pp: 438.
13. Bhardwaj, M., T. Garnett and A.P. Chandrakasan, 2001. Upper bounds on the lifetime of sensor networks, In Proc. IEEE Int. Conf. Communication, pp: 785-790.
14. Zhang, H. and J.C. Hou, 2005. On the upper bound of *á*-lifetime for large sensor networks, ACM Trans. Sens. Netw., 1(2): 272-300.
15. Olariu, S. and I. Stojmenovic, 2006. Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting, in Proc. IEEE Int. Conf. Comput. Commun., pp: 1-12.
16. Bhardwaj, M. and A.P. Chandrakasan, 2002. Bounding the lifetime of sensor networks via optimal role assignments, in Proc. INFOCOM, pp: 1587-1596.
17. Azad, A.P. and A. Chockalingam, 2006. Wlc12-2: Bounds on the lifetime of wireless sensor networks employing multiple data sinks, in Proc. GLOBECOM, pp: 1-5.

18. Blough, D.M. and P. Santi, 2002. Investigating upper bounds on network lifetime extension for cell-based energy conservation techniques in stationary AD HOC networks, in Proc. MobiCom, pp: 183-192.
19. Rout, R.R. and S.K. Ghosh, 2013. Enhancement of lifetime using duty cycle and network coding in wireless sensor networks, IEEE Trans. Wireless Commun., 12(2): 656-667.
20. Neugebauer, M. and K. Kabitzsch, 2004. A new protocol for a low power sensor network, in Proc. IEEE Int. Conf. Perform., Computer. Communication, pp: 393-399.
21. Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu NaserBikas, 2012. An Implementation Of Intrusion Detection System Using Genetic Algorithm, International Journal of Network Security & Its Applications (IJNSA), 4(2).
22. Chittur, A., 2005. Model Generation for an Intrusion Detection System Using Genetic Algorithms.
23. Li, W., 2004. Using Genetic Algorithm for Network Intrusion Detection. A Genetic Algorithm Approach to Network Intrusion Detection, SANS Institute, USA.
24. Lu, W. and I. Traore, 2004. Detecting New Forms of Network Intrusion Using Genetic Programming, Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp: 475-494.
25. Pillai, M.M., J.H.P. Eloff and H.S. Venter, 2004. An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms, Proceedings of SAICSIT, pp: 221-228.
26. Bridges, S.M. and R.B. Vaughn, 2000. Fuzzy Data Mining And Genetic Algorithms Applied to Intrusion Detection, Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp: 109-122.
27. Gomez, J. and D. Dasgupta, 2002. Evolving Fuzzy Classifiers for Intrusion Detection, Proceedings of the IEEE.
28. Middlemiss, M. and G. Dick, 2003. Feature selection of intrusion detection data using a hybrid genetical gorithm/KNN approach, Design and application of hybrid intelligent systems, IOS Press Amsterdam, pp: 519-527.
29. Srinivas Mukkamala andrew H. Sung and Ajith Abraham, 2005. Intrusion detection using anensembleof intelligent paradigms, Journal of Network and Computer Applications, 28(2): 167-182.
30. Peddabachigari, S., C. Ajith Abraham, Grosan J. Thomas, 2007. Modeling intrusion detection system using hybrid intelligent systems, Journal of Network and Computer Applications, 30(1): 114-132.
31. Saniee Abadeh, M., J. Habibi and C. Lucas, 2007. Intrusion detection using a fuzzy genetics-based learning algorithm, Journal of Network and Computer Applications, 30(1): 414-428.
32. Tao Peng, C. Leckie and Kotagiri Ramamohanarao, 2007. Information sharing for distributedintrusiondetection systems, Journal of Network and Computer Applications, 30(3): 877-899.