I J C T A, 9(16), 2016, pp. 8213-8223
© International Science Press

Node Failure Identification and Recovery algorithm to enhance the Lifetime & Defending Vampire Attack in WSNs

Yerneni Devi Priya Poojitha*, Pasumarthy Rambabu* and Maganti V.S.S. Nagendranath*

ABSTRACT

In this paper Node Failure Identification and Recovery Algorithm to Enhance the Lifetime & Defending Vampire Attack in WSNs is, to replace the sensor nodes which are ceased due to the operational threshold or exhausted battery power. This paper also focuses on the maintenance of pre-existing surveillance specifically on the denial of communication at the routing levels. The proposed algorithm is used to substitute the failed nodes with the nodes that are contrived by fusing grade diffusion and genetic algorithms. These nodes help in reducing resource depletion attacks at the routing protocol layer and also in reusing the routing path. The Vampire attacks which are destructive and tricky to detect by nature, can become weakened by authenticating the malicious node in the network.

In this paper, the recommended algorithm helps to increase the number of active nodes and reduce the rate of data loss, energy consumption and also reduces the effect of vampire in the network. This algorithm also contributes in efficient battery usage in the network when compared to the current system.

Index Terms: Genetic Algorithm, Directed Diffusion (DD), and Grade Diffusion (GD), Wireless Sensor Network (WSN), Denial of Service, Security, Routing, Node Failure Identification and Recovery (NFIR).

1. INTRODUCTION

A wireless sensor network is organized by the combination of sensor nodes in a cooperative network with Decentralized type of network. Decentralized network itself says that the network does not depend on the pre-existing framework such as routers in wired networks and access points in various managed wireless networks, where each and every node in the network participates in routing to forward the packets. All the nodes which were in the network or the device will have equal status in the network. The main use of the sensor nodes in the network are used to collect data from the outside environment where ever needed.[1]

Each network is a combination of nodes and each node in the network is a combination of multiple detection stations which are called as sensor nodes. The nodes in the network are minute, light weight and manageable. Each and every node in the network is connected through the wireless communication channels those which are used to sense data, process data and send it to the other nodes in the network. These networks are delimited by the nodes battery power in the network. Every node in the network is organized with a transducer, microcomputer, transceiver and power source. [1]

The nodes which are organized with transducer, microcomputer, transceiver exhibits their own functionalities such as, transducer generate electrical signals based on sensing the physical effects and phantasm(phenomena), microcomputer deals with the operations and stores the sensed data of the sensor nodes, coming with the transceiver which is of type wireless, accepts the data from central computer and forwards the data to that computer, and finally last but not least the power for each sensor node in the network is procured from battery power or from electrical utility. Wireless sensor networks (WSN) usually

* Dept. of CSE, Sasi Institute of Technology and Engineering, Tadepalligudem-534101, (AP), INDIA, *Emails: ypuji57@gmail.com; rambabupasumarthy@gmail.com; hodcse@sasi.ac.in*

have a delimited energy and communication capacity, which can't be balanced for the transmission of a large amount of data huddled by the sensor nodes in the network. [1].

Vampire attack: vampire attack is a type of attack, which creates and sends information through malicious node as an authorized node in the network that which causes huge amount of energy consumption by network which leads to quick depletion of nodes battery power. [2]

Features of Vampire Attack:

1. Vampire attacks are not protocol specific.
2. They don't disrupt immediate availability.
3. Vampires use protocol compliant messages.
4. Transmit little data with largest energy drain.
5. Vampires do not disrupt or alter discovered paths.

The motivation of the present work is done based on the battery depletion of sensor nodes in the network. In a network, each sensor node has bounded wireless computational power to progress the data and to transfer the live data which was gathered by the sensor nodes in the network to the base station [3], [4], [5]. Therefore, to increase the sensor and the transmission area [6], [7], the wireless network generally consist multiple sensor nodes. Generally, each sensor node in the network has a low level of battery power that which cannot be replenished. When the energy of a sensor node is exhausted in the network leaks will appear, and the failed nodes existed in the network will not be able to transfer the data to the other nodes in the network so that it increases the burden on the other sensor nodes in the network.

Existing work: Secure routing attempts to ensure that the attackers were unable to discover the path to return an invalid network path, but vampire does not disrupt the discovered path instead using the existed valid network path and protocol complaint messages. By this protocol complaint messages it was unable to identify the node behavior and malicious actions of node thus will lead to maximum power consumption.

2. RELATED WORK

2.1. Directed Diffusion Algorithm

The progression of routing algorithms [8], [9] in wireless sensor networks was proposed in recent years. The Directed Diffusion algorithm which was used to ruin the relay of data transmission counts for power management was presented by C. Intanagonwiwat et al. in the year 2003. The DD algorithm is a transmission protocol which is of type query-driven. The data which is collected by the nodes is allowed to transmit from nodes to sink if and only if it matches the query which was posed by the sink node. In this algorithm, the query which was posed by the sink to the nodes in the network to request data will be in the form of attribute-value pairs by broadcasting the query packets to the entire network. Finally, the nodes forward the data packets back to the sink only when it is apt to the queries.

2.2. Grade Diffusion Algorithm

H. C. Shih et al. has presented the Grade Diffusion (GD) algorithm [11] which was used to report some information regarding the data transmission in the network between nodes in the year 2012 and later enhance with ladder diffusion algorithm using ant colony optimization (LD-ACO) for wireless sensor networks [12]. This algorithm not only establishes the routing path for nodes in the network but also recognizes a set of neighboring nodes to improvise the transmission load. Each node in the network is supposed to select a set of neighboring nodes because those neighboring nodes will be helpful when its grade table was unable to progress the broadcast. Sensor nodes can also be allowed to select the nodes with lighter load or the nodes with more energy to operate the supplementary operations in the network.

Thus GD algorithm regenerates the routing path in real time and also shows how the data is allowed to send to sink instantly with atmost accuracy.

The routing paths which were established in the network between nodes are as shown in Fig. 1. and Fig. 2.

2.3. Genetic Algorithm

Genetic algorithm is probably the trendiest evolutionary algorithm in terms of diversity practice, which is used to reputable maximization problem and has demonstrated by genetic algorithm which is based on the population.

A Population of 2n to 4n trial solutions is used (n-No. of Variables).Each solution commonly symbolized by a string of binary variables, corresponding to the chromosomes in genetic. After the trial solutions are selected, a new generation (a new set of strings) is produced by selecting, using stochastic principle. Some arbitrary transformations of binary digits in a string reproduce the (advantageous and disadvantageous) effects of mutations. To overcome this new strategy called “ELITISTIC STRATEGY” was developed. The other technique is “PSO-PARTICLE SWARM OPTIMIZATION”.

The Genetic algorithm mainly involves with Initialization, Fitness Calculation, Selection, Crossover, and Mutation as described below.

Initialization: Initially, several numbers of elucidations were randomly generated to form an initial population. The population size of chromosome depends on the complexion of the problem. The total number of chromosome which was considered initially will be the number of dead nodes in the network. The values of gene which was generated will be in boolean format i.e., 0’s or 1’s.

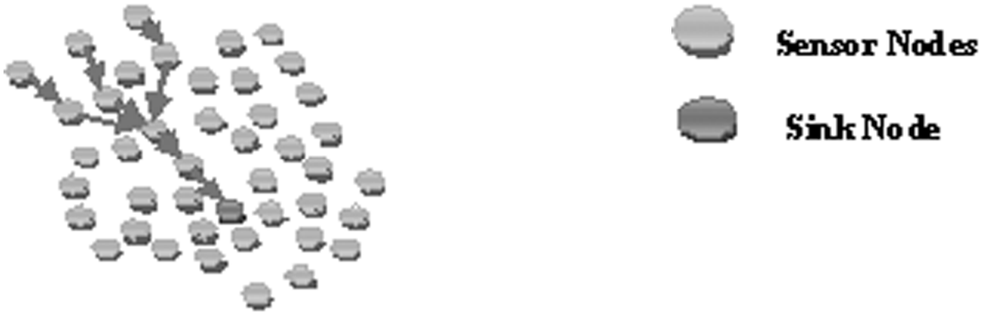


Figure 1: Routing path when all the nodes in the network are functioning.

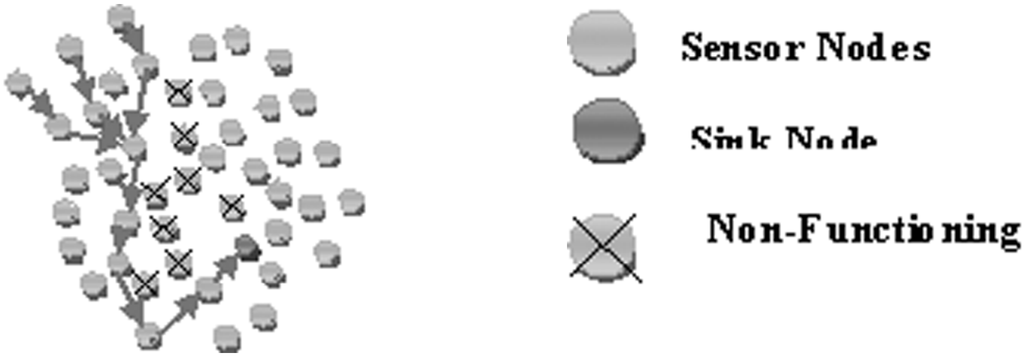
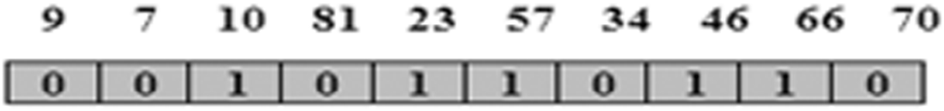


Figure 2: Routing path when some of the nodes in the network are not functioning.



9	7	10	81	23	57	34	46	66	70
0	0	1	0	1	1	0	1	1	0

Figure 3: Chromosome and its gene.

Fitness Calculation: The next step of the algorithm is Fitness calculation. Here in this stage fitness values were evaluated with the help of fitness function. The fitness function is characterized over the genetic representation and it amplifies the quality of the illustrated solutions.

$$f_n = \sum_{i=1}^{\max(Grade)} \frac{P_i * TP^{-1}}{N_i * TN^{-1}} * i^{-1} \tag{1}$$

where

N_i = Count of replaced sensor nodes with grade value at i.

P_i = Count of re-usable routing paths from sensor nodes with their grade value at i.

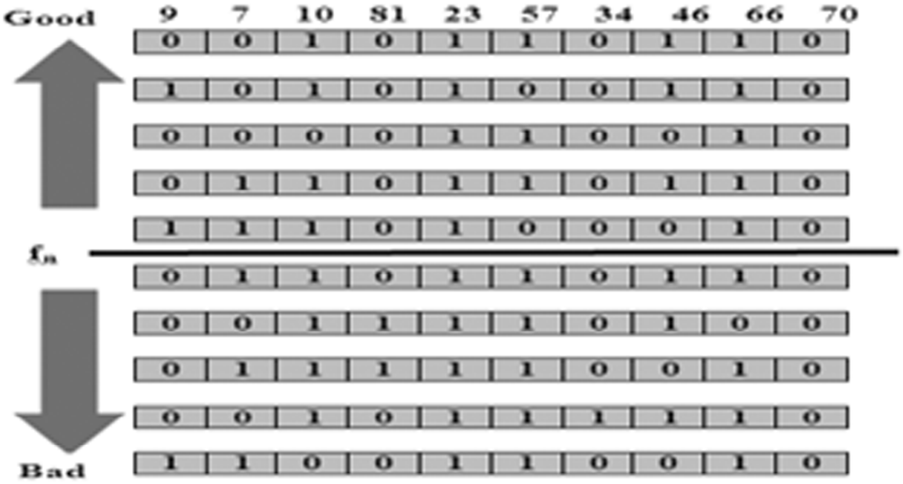
TN = Gross count of sensor nodes in the original WSN.

TP = Gross count of routing paths in the original WSN.

Selection: The primary intention is to finger the chromosome which was having high fitness value. Firstly it selects a pair of chromosomes from the node selected and eradicates the chromosome with lowest fitness value from high fitness value and it is allowed to send to mating pool to produce a new set of chromosome.

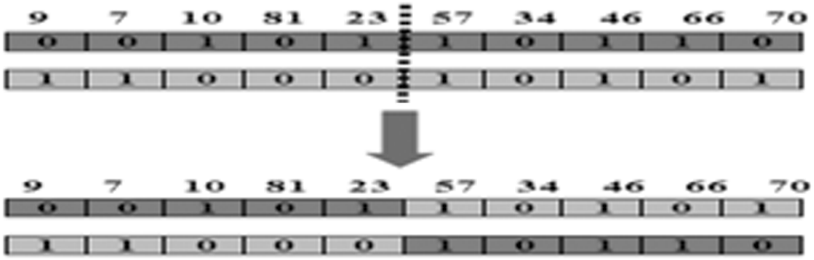
Crossover: In this strategy two individual chromosomes are allowed to select from the mating pool to generate a new set of offspring's. A crossover point is selected between two parents and then the fraction of each individual will be allowed swap accordingly to crossover mechanism.

Mutation: In this algorithm, the next stage is mutation, the main aim is to flip a gene randomly in the chromosome those which were filtered from the crossover stage. The chromosome with the genes of 1 replaces the sensor node to extend the network lifetime.



9	7	10	81	23	57	34	46	66	70
0	0	1	0	1	1	0	1	1	0
1	0	1	0	1	0	0	1	1	0
0	0	0	0	1	1	0	0	1	0
0	1	1	0	1	1	0	1	1	0
1	1	1	0	1	0	0	0	1	0
0	1	1	0	1	1	0	1	1	0
0	0	1	1	1	1	0	1	0	0
0	1	1	1	1	1	0	0	1	0
0	0	1	0	1	1	1	1	1	0
1	1	0	0	1	1	0	0	1	0

Figure 4: Selection Step



9	7	10	81	23	57	34	46	66	70
0	0	1	0	1	1	0	1	1	0
1	1	0	0	0	1	0	1	0	1

9	7	10	81	23	57	34	46	66	70
0	0	1	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	0

Figure 5: Crossover Step.

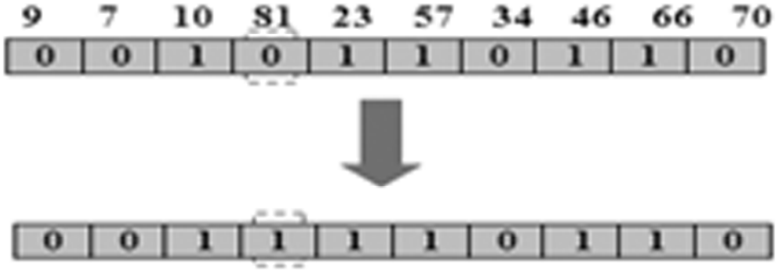


Figure 6: Mutation Step.

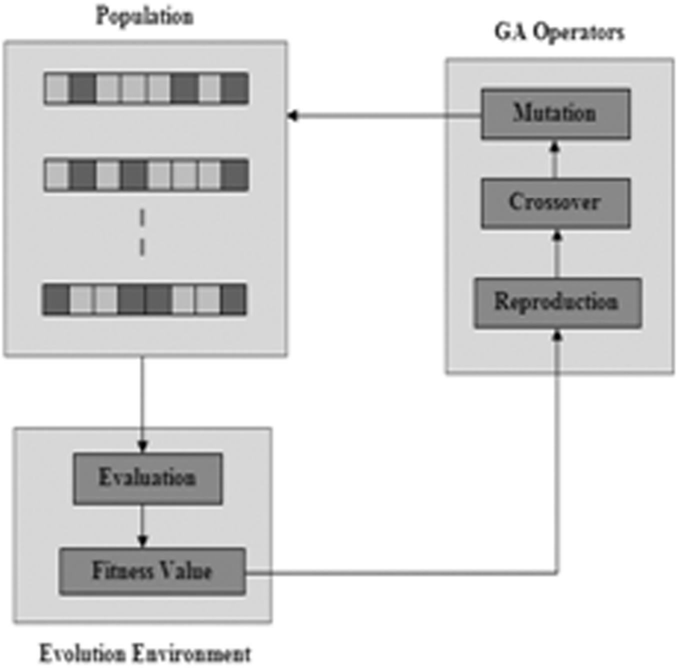


Figure 7: Evolution Environment of Genetic Algorithm.

The Evolutionary Environment of Genetic Algorithm is as shown:

There are proportionate provocations posed by the resource circumspection in the wireless sensor networks due to the conscience that may occur due to dynamic behavior of networks. The obstacle of security has acknowledged substantial study by researchers in networks. There are many different kinds of attacks that eventuate in wireless sensor networks. There are precautionary measures for these attacks in the MAC layer. Some of the techniques are described below:

A. *Wormhole attack:* In wormhole attack, the malicious nodes fabricates the path of data that which was allowed to send from source to destination and allows to transfer the data via the attackers path which can customize the constituents of the packets before sending it to the destination node. To prevent this we use a new technique called packet leashes.

B. *Denial of Service attack:* Denial-of-service attack (DoS attack) is also called as distributed denial-of-service attack (DDoS attack). DoS attack attempts to cause a network or a machine services nonexistent to the intended user who wants to use its services

C. *Resource depletion attack:* This attack mainly focuses on diminishing the quantity of resources used by nodes like battery potential, cache, memory etc thus downsizing the overall amplitude of the network. There are many kinds of attacks that which lead to resource depletion attacks. They are such as carousel attack, stretch attack, etc.

3. NODE FAILURE IDENTIFICATION AND RECOVERY ALGORITHM

The node failure identification and recovery algorithm is used to identify and replacing the fault node. The NFIR algorithm is designed by the integration of grade diffusion algorithm and genetic algorithm. The grade value, neighbor nodes, routing table that which is used to determine to where drop the data packet over an IP and the payload value for each sensor node is created using the GD algorithm in the NFIR algorithm. During the transfer of data in the WSN, the number of nonfunctioning sensor nodes is calculated in the NFIR algorithm. The flowchart of the Node Failure Identification and Recovery Algorithm is as shown in Fig.8.

The NFIR algorithm is based on the bandwidth calculation and the bandwidth B^{th} value can be calculated by using the equation,

$$B^{th} = \sum_{i=1}^{\max\{Grade\}} T_i \tag{2}$$

Where

$$T_i = \begin{cases} 1, \dfrac{N_i^{Now}}{N_i^{Original}} < \beta \\ 0, \ Otherwise \end{cases}$$

Where

$\mathbf{N_i^{Now}}$ = Count of functioning Sensor Nodes with grade value *i*, $\mathbf{N_i^{Original}}$ = Count of sensor nodes with grade value i, β is a parameter set given by the user between 0 to 1.

The count of functioning sensor nodes to the gross count of sensor nodes for each nodes grade value is less than β, T_i alters to 1 and the B^{th} will be also be greater than 0, then the NFIR algorithm that is designed by the integration of grade diffusion algorithm and genetic algorithm is called and the nonfunctioning sensor nodes which were existed in the network were replaced by functioning sensor nodes in WSN by using genetic algorithm.

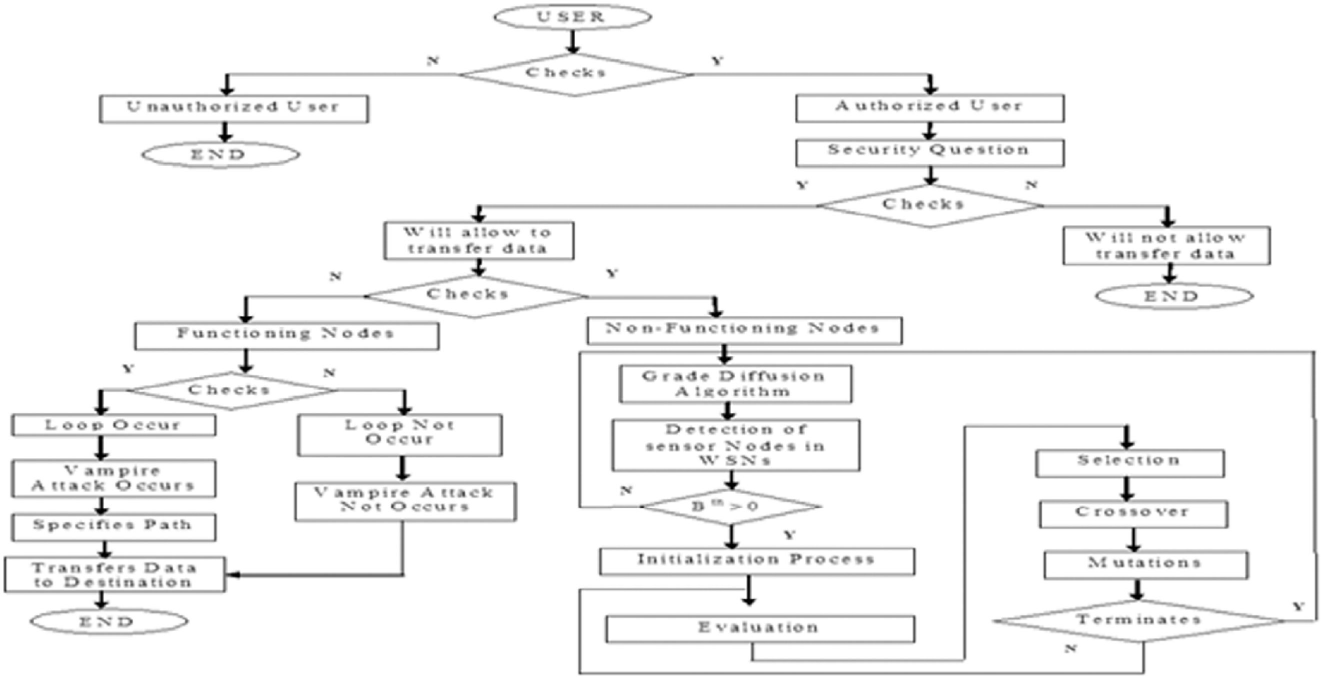


Figure 8: Node Failure Identification and Recovery Algorithm Flow Chart

The Fitness function can be calculated by using the equation,

$$f_n = \sum_{i=1}^{\max(Grade)} \frac{P_i * TP^{-1}}{N_i * TN^{-1}} * i^{-1} \tag{3}$$

where

N_i = Number of sensor nodes those which are replaced with their grade values at i., P_i = Number of routing paths which are re-usable by sensor nodes with their grade value at i., TN = Gross count of sensor nodes in the original WSN, TP = Gross count of routing paths in the original WSN.

In the remaining fragment of the paper, we present a series of attacks, the routing depletion and resource depletion attack. The routing depletion attacks usually affect the routing path but the resource depletion attack affect bandwidth, power, and energy consumption. These types of attacks are also known as “Vampire Attacks” [13]. They are difficult to be detected since they are protocol compliant and are orthogonal to them [14] and are not protocol specific.

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node’s battery life. The vampire attacks can be classified has two types. There are: one is Carousel attack and other is Stretch attack.

A. *Carousel Attack*: In the Carousel attack, attackers allow some recommended packets within a route as a sequence of loops, such that the same node appears in the route of communication many times. This attack increases the routing length and delay time of packet which is transferred from source to destination in the network.

B. *Stretch Attack*: In this type of attack, a malicious node fabricates artificially long routes from the source to destination in spite of shorter routes being available. It increases packet path length, causing packets to be processed by a number of nodes.

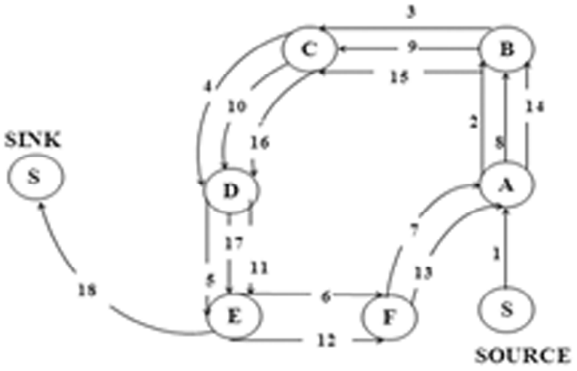


Figure 9: An honest Route would exit the loop immediately from node E to sink, but a malicious packet makes its way around the loop twice more before exiting.

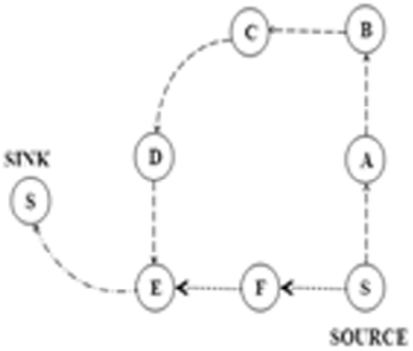


Figure 10: Honest route is dashed while malicious route is dotted. The last link to the sink is shared.

4. SIMULATION

A simulation of node failure identification and recovery algorithm is down in JAVA platform and is described as shown in Section 3 was performed to verify the method.

From the above paper i.e, Node Failure Identification and Replacement Algorithm to Enhance the Lifetime & Defending Vampire Attack in Wireless Sensor Networks we distinguish the non-functioning nodes from functioning nodes inorder to increase the number of active nodes, to enhance on an average after the replacement of sensor nodes, reduces the rate of data loss and rate of energy consumption, and including it also scrutinizes resource depletion attacks at the routing protocol layer, that which completely paralyze the network by rapidly exhausting nodes due to low battery power.

The results of the project i.e., Node Failure Identification and Recovery Algorithm to Enhance the Lifetime & Defending Vampire Attack in WSNs was as shown below:

While comparing with previous algorithm ie., Directed diffusion and Grade diffusion algorithm the number of active nodes counts is far better in Grade diffusion algorithm combined with genetic algorithm i.e., in NFIR algorithm. By the proposed algorithm, Grade diffusion algorithm combined with genetic algorithm i.e., in NFIR algorithm there is an increase in number of active nodes upto 8.7 times.

When compared with the results of existing algorithms i.e., Directed diffusion and Grade diffusion algorithm the energy consumption while transferring the data to the nodes in the network there will be a

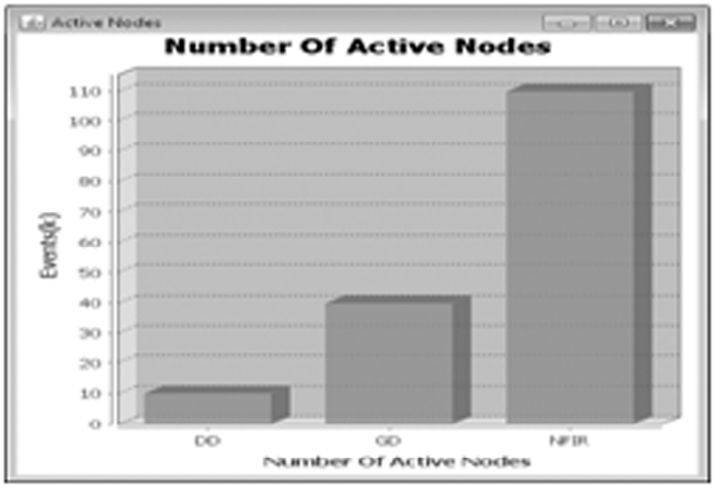


Figure 11: Number of active nodes.

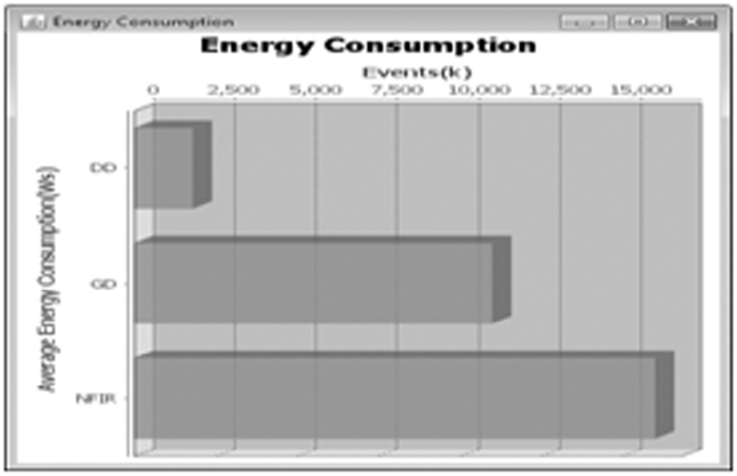


Figure 12: Total Rate of Energy Consumption.

sharp cutoff with the proposed algorithm, Grade diffusion algorithm combined with genetic algorithm i.e., in NFIR algorithm. By the recommended algorithm, there will be a sharp reduction in rate of energy consumption of nodes in the network by 31.1%.

Were as comparing with the preceding algorithms i.e., Directed diffusion and Grade diffusion algorithm, This shows the number of sensor nodes which were recovered in the network by implementing the recommended algorithm i.e., NFIR algorithm.

On reviewing the result of previous algorithms i.e., Directed diffusion and Grade diffusion algorithm the data loss while transferring the data to the other nodes in the network there is a drastic change in the data loss when compared to existing algorithms. In the proposed algorithm, Grade diffusion algorithm combined with genetic algorithm i.e., in NFIR algorithm there exists a reduction rate of data loss by approximately 98.8%.

By using the NFIR algorithm there will be a change in the energy consumption of nodes in the network. But by using the stretch attack and carousel attack the energy consumption by the nodes in the network is very low when compared the energy of nodes in the network by honest path. The energy consumption of nodes in the network with honest path and the energy consumption of nodes in the network with stretch attack and carousel attack are as shown below:

The energy consumption of nodes in the network with various algorithms is as shown below:

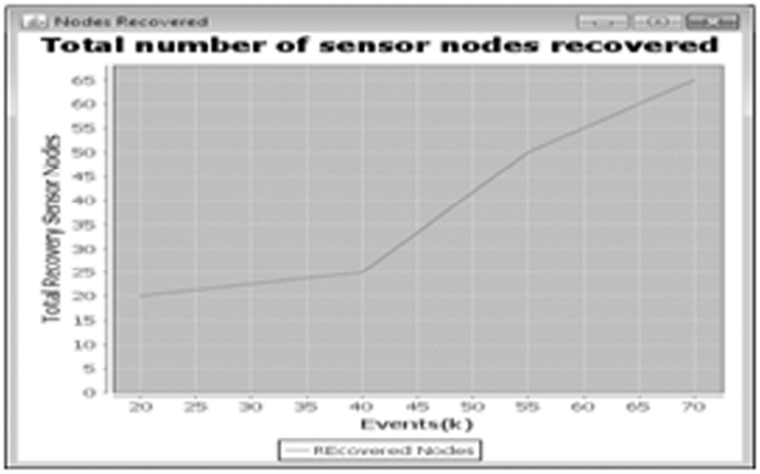


Figure 13: Total Number of sensor nodes recovered.

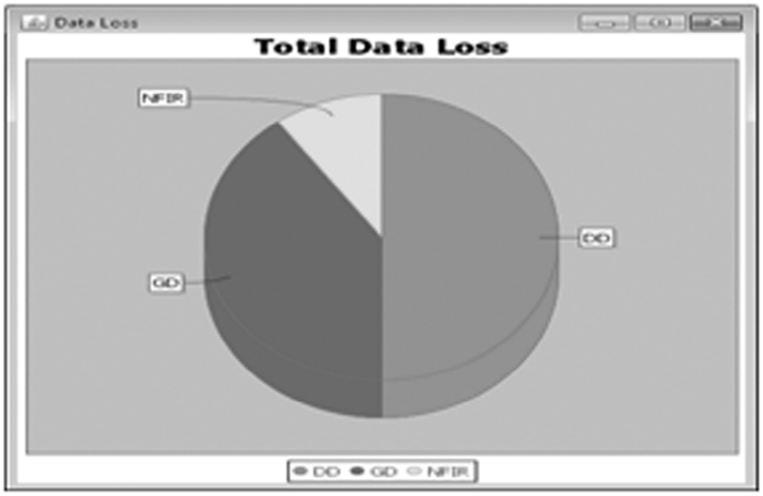


Figure 14: Total Rate of Data Loss

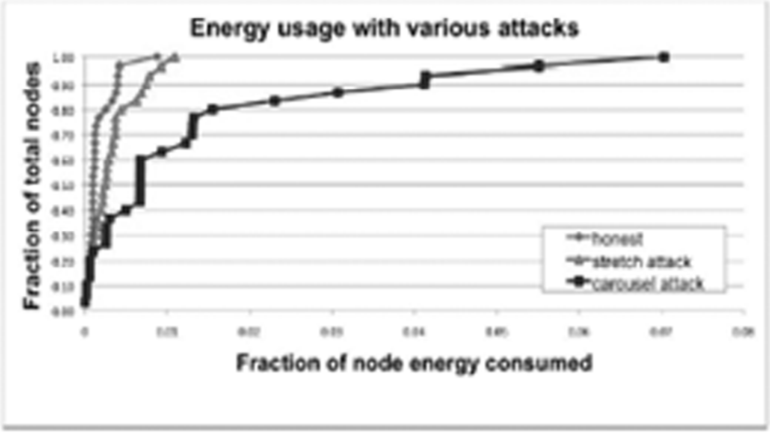


Figure 15: Energy Usage with Various Attacks

Algorithm	*10^{-3}Nodes/unit^3*	*$2*10^{-3}$Nodes/unit^3*	*$3*10^{-3}$Nodes/unit^3*	*$4*10^{-3}$Nodes/unit^3*
DD	3540.51Ws	3517.18 Ws	3495.17 Ws	3505.48 Ws
GD	3132.4Ws	3300.77 Ws	3298.29 Ws	3316.07 Ws
NFIR	2969.5Ws	2790.82 Ws	2407.68 Ws	2393.06 Ws

5. CONCLUSION

In this replica, the recommended algorithm increases the number of active nodes up to 8.7 times, it can enhance 3.16 times on average after the replacement of sensor nodes by 32 in number, Reduces the data loss rate by approximately 98.8% and Reduces the energy consumption rate by 31.1% Therefore, the NFIR algorithm not only used to replace the sensor nodes which are not functioning but also reduces the cost of replacing sensor nodes. Including that we define a Vampire attack, a new class of consuming resource attack that uses routing protocols to permanently disable wireless sensor networks by depleting battery power of sensor nodes. These attacks do not depend on particular protocol or implementation, but rather discloses burden in a number of popular protocol classes.

Theoretically in worst case, energy usage can increase by as much as a factor of O (N) per adversary per packet, where N is the network size. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

REFERENCES

[1] http://www.slideshare.net/PavithraRShettigar/fault-detection-in-wireless-sensor-network http://www.slideshare.net/augustinjose7/vampire-attacks

[2] F. C. Chang and H. C. Huang, “A refactoring method for cache-efficient swarm intelligence algorithms,” Inf. Sci., vol. 192, no. 1, pp. 39–49, Jun. 2012.

[3] Z. He, B. S. Lee, and X. S. Wang, “Aggregation in sensor networks with a user-provided quality of service goal,” Inf. Sci., vol. 178, no. 9, pp. 2128–2149, 2008.

[4] T. P. Hong and C. H. Wu, “An improved weighted clustering algorithm for determination of application nodes in heterogeneous sensor networks,” J. Inf. Hiding Multimedia Signal Process., vol. 2, no. 2, pp. 173–184, 2011.

[5] J. A. Carballido, I. Ponzoni, and N. B. Brignole, “CGD-GA: A graphbased genetic algorithm for sensor network design,” Inf. Sci., vol. 177, no. 22, pp. 5091–5102, 2007.

[6] J. Pan, Y. Hou, L. Cai, Y. Shi, and X. Shen, “Topology control for wireless sensor networks,” in Proc. 9th ACM Int. Conf. Mobile Comput. Netw., 2003, pp. 286–299.

[7] W. H. Liao, Y. Kao, and C. M. Fan, “Data aggregation in wireless sensor networks using ant colony algorithm,” J. Netw. Comput. Appl., vol. 31, no. 4, pp. 387–401, 2008.

[8] H. C. Shih, S. C. Chu, J. Roddick, J. H. Ho, B. Y. Liao, and J. S. Pan, “A reduce identical event transmission algorithm for wireless sensor networks,” in Proc. 3rd Int. Conf. Intell. Human Comput. Interact., 2011, pp. 147–154.

[9] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, “Directed diffusion for wireless sensor networking,” IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 2–16, Feb. 2003.

[10] J. H. Ho, H. C. Shih, B. Y. Liao, and J. S. Pan, “Grade diffusion algorithm,” in Proc. 2nd Int. Conf. Eng. Technol. Innov., 2012, pp. 2064–2068.

[11] J. H. Ho, H. C. Shih, B. Y. Liao, and S. C. Chu, “A ladder diffusion algorithm using ant colony optimization for wireless sensor networks,” Inf. Sci., vol. 192, pp. 204–212, Jun. 2012.

[12] Eugene Y.Vassermann and Nicholas Hopper “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks” IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.

[13] B. Karp and H. T. Kung, “GPSR: greedy perimeter stateless routing for wireless networks.” In mobile Computing and Networking, 2000, pp. 243-254.