Energy Aware Optimal Routing Protocol to Overcome Vampire Attacks in Wireless Ad Hoc Sensor Networks

[1] E. Gayathri , [2] Dr N. Geethanjali

[1] Research Scholar, Department Of Computer Science and Technology,
Sri Krishnadevaraya University, Anantapuramu,
Andhra Pradesh, India

[2] Professor, Department Of Computer Science and Technology,
Sri Krishnadevaraya University, Anantapuramu,
Andhra Pradesh, India

Abstract - A wireless adhoc sensor network consists of a number of sensors spread across a geographical area. A primary challenge in the design of Wireless adhoc sensor networks is to enhance the network lifetime and usage of low energy. Due to the resource constrained nature of sensor nodes, innovative techniques are required to extend the network lifetime in WSN`s. Nodes energy is considered as an important resource for sensor node which are battery powered based. The resource depletion attacks such as vampire attacks at the routing protocol layer, permanently disable the WSN`s by evacuating the battery power. This paper proposes an energy efficient routing protocol which finds the forwarding path between sensor nodes and sink to avoid energy consumption attacks (vampire attacks) by using heuristic function. An energy aware routing protocol is proposed that uses heuristic function and A* search algorithm to find an optimal route in case of battery depletion attacks. In addition to this, the low energy nodes are avoided for repetitive data transmissions that extends the network lifetime. Maximum energy efficiency, optimal route and the avoidance of data transmission by low energy nodes is achieved in the proposed system.

Keywords - *Wireless Adhoc Sensor Networks, Denial of Service, Balancing Energy Consumption, Energy-Efficient Routing, Throughput, Network Lifetime.*

1. Introduction

In software terms, energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs may be deployed in large numbers in various environments, including remote and hostile regions, where adhoc communications are a key component. For this reason, the issues such as increased lifespan, robustness and fault tolerance, self-configuration, lifetime maximization are addressed by the WSN algorithms and protocols. Energy/Power consumption of the sensing devices should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime. To preserve power, wireless sensor nodes normally power off both the radio transmitter and the radio receiver when not in use.

Wireless adhoc sensor networks require large no of sensor nodes, low energy usage, (the lifetime of a node determined by the battery life, so the minimization of energy expenditure is a major issue). The organization of the network must be able to periodically reconfigure itself to continue to transmit the packets from sensor nodes to the sink. Some of the nodes may fail due to lack of energy or from physical destruction and the new nodes may join the network. Moreover, the sensor nodes require a collaborative signal processing to transmit the packet. The main application of the adhoc wireless networks is pervasive on-demand computing power, continuous connectivity............

Due to the adhoc organization of the wireless adhoc networks, they are in great danger to DOS attacks , and more research work has been done to strengthen the survivability[2][5][14]. The schemes proposed by different authors can prevent attacks on the short term availability of a network, rather addressing the attacks that affect long term availability of the network. The most important denial of service attack is to wholly deplete nodes batteries. The vampire attacks are totally different from formerly studied DOS, RoQ and routing infrastructure attacks. The vampire attacks do not interrupt the availability but entirely disable a network by weakening the node batteries. Vampire attacks are not protocol specific, in that they do not depend on design properties or implementation faults of particular routing protocols, but rather make use of general properties of protocol classes such as link state, distance vector, source routing and geographic and beacon routing. These vampires do not flood the network with large amounts of data ,but rather they transmit little amount of data as possible to achieve the largest energy drain. These attacks are very difficult to predict and prevent as they drain the nodes battery power which slowly causes the network to end. Effective routing protocols have to be planned in order to maximize network lifetime and to guarantee balanced energy consumption. In most of the routing protocols, the best path is selected for data transmission. If the adversaries route the packets on the same route continuously through the weak forwarding nodes then those nodes battery deplete over a period of time [15][16][17].

2. Related Works

The draining of battery power is not new, but rather these attacks have been defined earlier. Attacks prevent nodes from entering a low power sleep cycle and deplete their batteries faster. These attacks are considered only at the MAC in Sleep Deprivation Torture[2]. The energy is wasted by restarting the packet in various parts of the network. Here, the adversaries deposit packets in arbitrary parts of the network. The node energy is consumed so that it cannot process the original packet in Directional Antenna Attack. According to Syn Flood attack [3], the adversaries make multiple connection requests to servers using network paths but cannot protect against vampires. The lifetime of power constrained networks increase by using less energy to transmit and receive the packets. Vampires will increase the energy usage even in minimal energy routing and power conserving MAC protocols, if minimum energy is used to transmit packets and each packet is still more expensive to transmit in case of vampires.

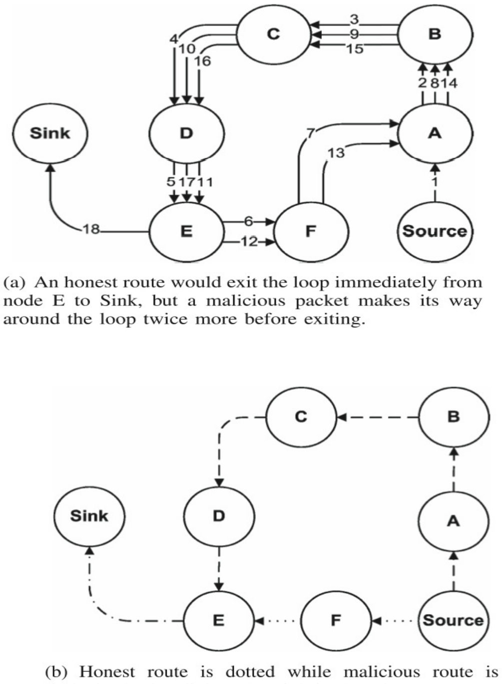
Local packet forwarding decisions are proposed by Karp et al. in Greedy Perimeter Routing (GPSR)[1] protocol which uses greedy algorithm. Greedy forwarding decisions are made by using the router 's immediate neighbors information in the network topology. In GPSR, packets may be trapped in holes due to lack of adequate sensor density or various obstacles. To overcome the problem, the algorithm routes data packets around the perimeter of the region. However, the protocol still may be trapped in blind alley if the planner sub-graph used by the GPSR's perimeter mode is not connected. To increase the lifetime of power-constrained networks by using less energy to transmit and receive packets (e.g., by minimizing wireless transmission distance) [21]is done in present minimal energy routing and is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios. Additional on power-conserving MAC, upper layer protocols, and cross-layer cooperation [23].

The source has to ensure that the route is valid at the time of sending, every node in the route is a physical neighbor of the previous route hop.Less forwarding logic at intermediate nodes and the entire route is sender authenticated using digital signatures in Ariadne[13]. Some of the routing protocols such as LEACH, EAD and Heed [4][5][6], offer energy balancing within clusters by choosing the cluster head but however there are limited solutions. S.K Das in [7] developed and proposed a non uniform node distribution strategy which achieves minimum balanced depletion. The energy aware routing in Rana et al. presented an A* algorithm based Energy Efficient Routing (ASEER) protocol to find optimal route in order to extend network lifetime [12]. In addition to '*h(n)' estimated* and cost-so-far '*g(n)*', ASEER's heuristic function introduces a new metric '*l(n)*' that denotes the path cost count of weak nodes having less energy.

The '*l(n)*' parameter is used to keep track of total number of low energy nodes in a current path. However, the protocol may not perform well if there exists multiple paths with same number of low energy nodes. As an example, if the *l(n)* value of two available paths is equal, then the path with least *f(n)* value will be selected. But, it may happen that the energy level of nodes in selected path is lower than the alternative path since ASEER protocol can't distinguish between the energy level of two nodes if both of them are below threshold level. F. Ren , J. Zhang et al proposed a design called (EBRP) energy balanced routing protocol[20] by constructing a mixed virtual approach which forces the packets to move towards the sink through the dense energy area thereby protecting the low energy nodes and routing loops.The main drawback of this protocol is less throughput. Delay aware energy balanced dynamic routing protocol by N.kaleswari and Dr k. Baskaran [22] proposed three phases, which finds the shortest path /best energy balanced based delay minimum optimal route. In the second phase alternate shortest path will be updated in the route table. This phase updates the new route if the working route is getting down.

3. Overview

In the rest of this paper, we present energy efficient routing protocol against vampire attacks that finds the forwarding path between the source and destination nodes, and suggested the optimal route. In source routing protocols , we show how a malicious packet source can specify paths through the network which are far longer than optimal, the energy is wasted at intermediate nodes who forward the packet based on the source route. In routing schemes, the forwarding decisions are made independently by each node. In directional antennas and worm hole attacks deliver the packets to process the nodes at remote network positions. Network wide energy is increased if the sink do not receive the packets normally. In vampire attacks draining life from wireless adhoc sensor networks, two attacks has been proposed. In the first attack, i.e. Carousel attack, an adversary composes packets with intentionally establishing routing loops. The carousel attack sends the packets in circles targeting the source routing protocols by making full use of resources. i.e. Single packet repeatedly traversing the same set of nodes. Several number of mitigation methods have been bounded the damage from vampire attacks. Carousel attack is very simple and negligible when compared to the stretch attack. An adversary constructs artificially long routes in the case of stretch attack, potentially traversing every node in the network. The assumption has been made that only messages originated by adversaries may have maliciously composed routes. In the stretch attack, the route diverts from the optimal path between source and destination, roughly doubling in length. Note that while the per-node energy consumption increase is not much when compared to the overall energy consumption than in the carousel attack, but spread more evenly over more network nodes.



(a) 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.

(b) Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

Fig. 1. Malicious route construction attacks on source routing: carousel attack (a) and stretch attack (b).

Wireless Sensor Networks (WSNs) consist of small nodes equipped with sensing, data processing and radio transmission units. Energy consumption and improving the network lifetime has become a primary issue when overcoming the attacks in WSN. A number of clustering, routing, power management and data aggregation protocols are specially designed for WSNs where energy consumption is an important design issue. Due to the resource constrained nature of sensor nodes, innovative techniques are required to extend the network lifetime in WSNs. This paper proposes an energy efficient routing protocol to find the forwarding path between source and destination node to avoid energy consumption attacks (vampire attacks) by using heuristic function and an search algorithm. This energy efficient protocol is also used for finding the route optimality.

Problems identified in the case of vampire attacks:

1) Improving network Lifetime
2) Route Optimality
3) A path to forward the packets by consuming less energy. i.e. Maximum energy efficiency.

In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss a new protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

4. Overcoming The Stretch Attack

4.1 Network Model Properties

We assume that a wireless adhoc sensor network consists of hundreds of node and the properties are

1. Power consumption constraints for nodes using batteries.
2. Every SN is assigned a unique node ID.
3. Every SN knows the location of BS as well as its own.
4. SNs periodically send the energy information to all of their neighbour nodes.
5. The network consists of multiple stationary/mobile nodes and the energy consumption is not uniform for all nodes.
6. SNs have different levels of transmission power and each node can dynamically adjust the power level [18].

4.2 Heuristic Function to Overcome the Stretch Attack

The classical methods are too slow , or may fail to find any exact solution in overcoming the stretch attack. So, a heuristic is a technique which is designed for solving a problem more fastly and to achieve optimality, completeness, accuracy or precision for speed. In other words, we can say it approximates the exact solution in avoiding the long routes.

4.2.1 Heuristic Function

A good guess is made by the heuristic function to find out of how far the destination node from the current node and thus helps to guide the search procedure. A number of parameters can be used in heuristic function that will collectively represent a numerical value. The searching process is to be proceeded in right direction as since heuristic search is dependent on the heuristic function. To overcome the stretch attack, the proposed protocol uses three different parameters to find the forwarding path. Longlife factor, distance from source node to current node and euclidean distance from current node to the BS are used to compute the heuristic value as follows:

$$f(n) = h(n) + g(n) + 100/LF \qquad (1)$$

Here, '*f(n)*' denotes heuristic value of node *n*, and is calculated according to the following equation:

$$f(n) = g(n)+h(n) \qquad (2)$$

'*h(n)*' is the estimated cost from node *n* to the Bs which should be always less than the actual cost. As, we have chosen the grid network model, h(n) is calculated as:

$$h(n) = \text{No of lines} / 2 \qquad (3)$$

'*g(n)*' is the cost from node *n* to current node and is calculated as follows:

$$g(n) = g(n)+cost(n,\text{current node}) \qquad (4)$$

The long life factor '*LF*' is calculated according to the following equation:

$$LF = (T * Eres)/Einit \qquad (5)$$

where, *T* is the sustainable time, Eres denotes the residual energy and Einit indicates the initial energy of SNs. The longlife factor is used to maximize the value of heuristic function when the energy of a forwarding node is below the threshold level.

4.2.2 A* Heuristic Search Algorithm

A* uses best-first- search technique to find a least-cost path from source to destination node. It first searches the path that appears to be most likely to lead towards the goal on the basis of heuristic function. The available node with the smallest value of '*f*' is the node that should be expanded next. To find an optimal path to the destination using A* search, '*h(n)*' should be any lower bound of the actual distance to the destination node [19]. Thus, for an application such as routing, '*h(n)*' might represent the Euclidean distance to the goal which is the shortest real distance between any two nodes. Here, we present the pseudocode of A * search algorithm.

By considering the network topology with fifty sensor nodes and one sink node the sensor nodes continuously send data packets to the sink. Each node is assigned a heuristic value 'f' used to guide the search process. A node computes the route according to the algorithm described in previous section before sending the packets.. Suppose, node 1 has to find a route to the Sink through heuristic function. Initially, from all its neighbors (2, 3 and 5), node 1 chooses one with the smallest heuristic value or f-value as its next hop. At this point, the energy level of each neighbor node is compared to the threshold level. If the energy of any node is below the threshold level, the heuristic value of that node is incremented according to energy-based heuristic function. Since, the node with least f-value is selected as the next hop to transmit the packet to avoid the less energy nodes. As mentioned in the VAMPIRE ATTACKS : DRAINING LIFE FROM WIRELESS ADHOC SENSOR NETWORKS , the energy is consumed more not due to the attacks but the path to transmit the packet is consuming the energy.

The below table provides how the nodes are choosing the best route through A* search heuristic function. By using the above equations we have calculated the g(n), h(n) and the f(n) values.

Table – 1 Calculation of Heuristic value

n	**g(n)**	**h(n)**	**f(n)**
~~S~~	~~0~~	~~2~~	~~2~~
~~1~~	~~1~~	~~1~~	~~2~~
2	1	1	2
3	1	2	3
5	1	2	3
~~2~~	~~2~~	~~1~~	~~3~~
3	2	2	4
5	2	2	4
3	3	2	5
~~6~~	~~3~~	~~1~~	~~4~~
~~7~~	~~3~~	~~1~~	~~4~~
7	4	1	5
~~8~~	~~4~~	~~0~~	~~4~~

The f value of 1 is smaller when compared to that of nodes 2, 3 and 5. So, the source node chooses the first node to route its packet in its first hop. After that the f-value of nodes 2, 3 and 5 are compared via node 1, the f-value of node 2 is smaller and so we choose the node 2 and update the routing table. Among nodes 3, 6 and 7 the f-value of node 6 is smaller. Finally, by comparing the f-values of nearest nodes we find a path. A * uses priority queues to perform the repeated selection of minimum(estimated) cost nodes to expand. This priority queues are known as the open set and closed set. At each step of the algorithm, the node with the lowest f(x) value is removed from the queue, the f and *g* values of its neighbors are updated accordingly, and these neighbors are added to the queue. The algorithm continues until a goal node has a lower f-value than any node in the queue (or until the queue is empty). The *f* value of the goal is then the length of the shortest path, since h at the goal is zero in an admissible heuristic. The smaller f-value nodes are placed in closed set until the source node reaches the sink node. Hence, the nodes in the closed set are 1, 2, 6 and 8.This route is considered as the best path.

Table – 3 Priority Queue

Open	**Closed**
S 1 2 3 4 5	S
2 3 5	1
3 6 7	2
7 8	6 8

The below function is for finding the optimality route by avoiding the weak energy nodes:

f(n) = cost of node n to sink + cost of node n to current node +100 / time * residual energy/initial energy (6)

After some time i.e 50 minutes, if the energy level of node 7 and 8 degrades to 60 and 80 joules respectively. Since, the energy level of node 7 is below the threshold level, node 6 recomputes the heuristic value of node 7 using the heuristic function. The new f-value of node 7 is: f(7) = 4 + 1 + 100/ ((50 * 60)/100) = 9. Since the value is greater than that of node 8 ,f(8) = 6.5; node 8 is selected as the forwarding node by node 6, as fvalue of 7 is greater than 8 after sometime i.e.50mins. If fvalue of node 10 and node 11 is same then it searches for alternative paths to avoid low energy node and thus extends the network lifetime. The main theme is that when a packet is transmitting in the network the low energy nodes are avoided and these nodes remain through out network lifetime. Thus, the proposed protocol follows optimal route when the nodes have sufficient level of energy. Otherwise, it searches for alternative paths to avoid low energy node and thus extends the network lifetime.

4.3 Pseudocode

```
sn,dn
lv={ };
nv={ };
tval=.25;
pathlist=emptynodelist;
gval[sn]=0;
if(eng[sn]<tval)
{
    fval[sn]=gval[sn]+hval[sn]+100/((t*res)/init);
}
else
{
    fval[sn]=gval[sn]+hval[sn];
}
while(nv!=0)
{
    cn=the node in nv with lowest fval[];
    if(cn==dn)
    {
        return createpathlist(pathlist,dn);
    }
    remove cn from nv;
    add cn to lv;
    for(each neighbor in neighbornodes[cn])
    {
        tetgval=gval[cn]+distbw(cn,neighbor)
        if((neighbor in lv) or (tetgval<gval[neighbor])
        {
            pathlist[neighbor]=cn;
            gval[neighbor]=tetgval;
            if(eng[neighbor]<tval)
            {
                fval[neighbor]=gval[neighbor]+hval[neighbor]+100/((t*res)/init);
            }
            else
            {
                fval[neighbor]=gval[neighbor]+hval[neighbor];
        }}
        if (neighbor not in nv)
        {
            add neighbor to nv;
        }
}
}
createpathlist(pathlist,cn)
{
if (cn in pathlist)
p=createpathlist(pathlist,pathlist[cn]);
return(p+cn);
else
return cn;
}
```

5. Simulation Analysis

We have simulated the proposed algorithm and compared the results with that of existing AODV protocol as since both can be used in the wireless adhoc sensor networks. For our experiments, we have used 50 nodes in a 250*250(m) simulation area. The transmission range of sensor nodes is fixed to 250m. Here, we have analyzed the total energy utilized, no of packets dropped due to drained nodes, lifetime of the network and the throughput.

5.1 Simulation Setup

Table-3 Simulation Parameters

Parameters	Values
Simulation area	250*250(m)
Initial Energy	100J
Node mobility model	8 packets/sec
Transmission Range	250m
Data Packet Size	512bytes
Broadcast Packet Size	120bytes
No of Runs	580
Packet Header Size	32bytes

Fig. 1 shows the total energy used for both the protocols. The existing protocol utilizes more energy than the proposed protocol, since more nodes are alive and send the information to the sink. In most of the wireless adhoc sensor applications send data packets to the sink through multipath routing. If any node in the routing path drains the power quickly, it may partition the network. The other nodes that forward information via depleted nodes may unable to communicate with the sink even though they are capable to communicate. But, in this protocol the exhausted nodes are not used for communication. They are made to live through out the network lifetime.

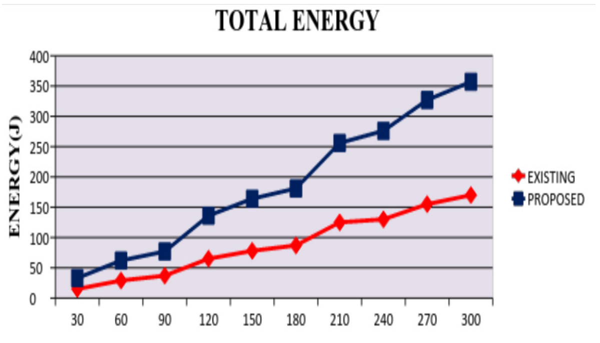


Fig.1 Total Energy Dissipation

The Fig. 2 indicates the number of affected nodes in existing is higher than proposed protocol. The low energy nodes are avoided in the proposed protocol as there exists alternative path to route the data packets. As a result, the number of effected nodes are minimized and nodes remain alive for more rounds. For example, the 10th node of existing protocol is affected in 115 round whereas in proposed the 10th node runs out of its battery power at 125h round.

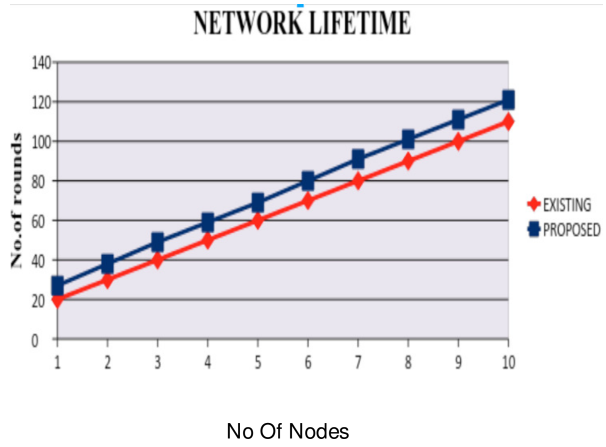


Fig.2 Network Lifetime.

In Fig. 3, the amount of unused energy in existing and proposed protocols is represented. From the graph, we see that more energy is unused in existing compared to proposed routing scheme. This is because the failure of a node divides the entire network, the remaining energy of the disjointed nodes is completely unused if the network path can not be repaired.

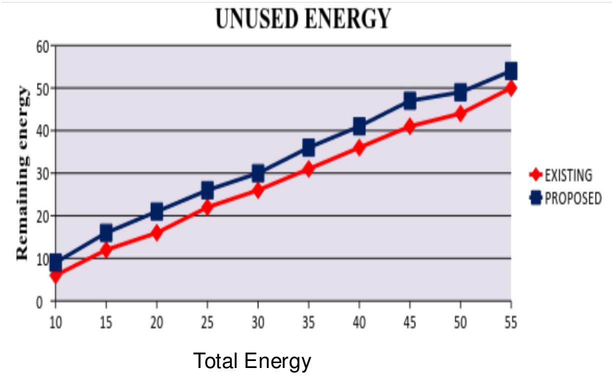


Fig. 3 Unused Energy

Finally, the packet delivery has been examined in our proposed protocol by sending different number of data packets to the BS in Fig. 4. In the first phase, the sensor nodes sent a total of 1000 data packets. In existing protocol, the BS successfully received 960 of these packets, resulting a good packet delivery. For the same number of data packets, the BS in proposed protocol received 986, resulting a good and better packet delivery.

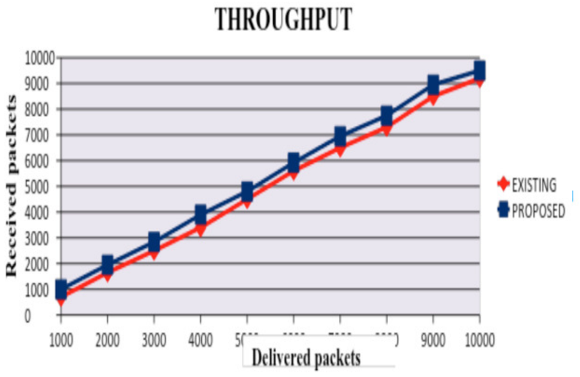


Fig. 4 Throughput

The simulation results show that the packet delivery in proposed is higher than that of existing. The reason is that some of the forwarding nodes in existing protocol quickly loose power. As a result, the packets transmitted by the nodes of disjointed area are not received by the BS.

6. Conclusion

In this paper, we defined Vampire attacks, resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by evacuating nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. A number of protocols and challenges have been made to overcome the carousel attack but less concentration is shown towards the stretch attack. We measured their attack success on a randomly generated topology of 50 nodes. In this paper, to overcome the stretch attack an energy aware heuristic-based routing protocol is proposed that uses heuristic function and A * search to find an optimal and minimal route. In addition to the heuristic function and A* search the longlife factor is used as one of the route selection parameter in our proposed algorithm. Hence, PLGPa protocol, the first sensor network routing protocol proposed, always avoids the low-energy nodes if there exists alternative paths in the network. Our proposed routing scheme extends network lifetime and degrades the chance of network partition in the presence of malicious nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase are far better than the existing. We have not offered totally a good solution for Vampire attacks during the topology discovery phase, but proposed some ideas about damage limitations caused in the adhoc sensor networks.

References

[1] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, 2000.

[2] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," Proc. Int'l Workshop Security Protocols, 1999.

[3] Eugene Y. Vasserman and Nicholas Hopper. (FEBRUARY 2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *IEEE*. 12 (2), p318-332.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy- Efficient Communication Protocols for Wireless Microsensor Networks," Proc. Hawaiian Int'l Conf. Systems Science, 2000.

[5] Boukerche, X. Cheng, and J. Linus, "Energy-Aware Data- Centric Routing in Microsensor Networks," Proc. Sixth ACM Int'lWorkshop Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWIM' 03), pp. 42-49, 2003.

[6] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks," IEEE Trans. Mobile Computing, vol. 3, no. 4, pp. 366-379, Oct.-Dec.2004.

[7] X. Wu and G. Chen, and S.K. Das, "Avoiding Energy Holes in Wireless Sensor Networks with Nonuniform Node Distribution," vol. 19, no. 5, pp. 710-720, 2008.

[8] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.

[9] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.

[10] J.R. Douceur, “The Sybil Attack,” Proc. Int’l Workshop Peer-to-Peer Systems, 2002.

[11] R.C. Shah and J.M. Rabaey, “Energy Aware Routing for Low Energy Ad Hoc Sensor Networks,” Proc. IEEE Wireless Comm. and Network Conf. (WCNC), 2002.

[12] K. M. Rana and M. A. Zaveri, “ASEER: A routing method to extend life of two-tiered wireless sensor network”, *in Int. J. Adv. Smart Sensor Netw. Syst.*, vol. 11(2), pp. 1 –16, 2011.

[13] J. Park and S. Sahni, “An online heuristic for maximum lifetime routing in WSNs”, *in IEEE Trans. Comput.*, vol. 55, pp. 1048–1056, 2006.

[14] Y.-C. Hu, D.B. Johnson, and A. Perrig, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Proc. MobiCom, 2002.

[15] H. Zhang and H. Shen, ”Balancing energy consumption to maximize network lifetime in data-gathering sensor networks”, *in IEEE Trans. Parallel Distrib. Syst.*, vol. 20, pp. 1526—1539, 2009.

[16] K. Akkaya and M. Younis, ”A survey of routing protocols in wireless sensor networks”, vol. 3(3), pp. 325–349, 2005.

[17] F. Ren , J. Zhang , T. He , C. Lin and S. K. Das, ”EBRP: Energy-balanced routing protocol for data gathering in wireless sensor networks”, *in IEEE Trans. Parallel Distrib. Syst.*, vol. 22, pp. 2108 –2125, 2011.

[18] K. M. Passino and P. J. Antsaklis, “A metric space approach to the specification of the heuristic function for the algorithm”, *in IEEE Trans. on System, MAN and Cybernetics*, vol. 24(1), pp. 159–166, 1994.

[19] S. Singh, M. Woo, and C.S. Raghavendra, “Power-Aware Routing in Mobile Ad Hoc Networks,” Proc. ACM MobiCom, 1998.

[20] F. Ren , J. Zhang , T. He , C. Lin and S. K. Das, ”EBRP: Energy-balanced routing protocol for data gathering in wireless sensor networks”, *in IEEE Trans. Parallel Distrib. Syst.*, vol. 22, pp. 2108 –2125, 2011.

[21] J.-H. Chang and L. Tassiulas, “Maximum Lifetime Routing in Wireless Sensor Networks,” IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[22] N.Kaleeswari and Dr.K.Baskaran "Implementation of energy balancing in wireless sensor networks", IJCSI International journal of computer science, vol 9, issue 3, no 2, May 2012.

[23] A.J. Goldsmith and S.B. Wicker, “Design Challenges for Energy- Constrained Ad Hoc Wireless Networks,” IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002