IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 14, Issue 2, Ser. I (Mar.-Apr. 2019), PP 30-36
www.iosrjournals.org

Improved Network Lifetime And Secured Routing Against Blackhole Attack In Wireless Sensor Networks Using SRR.

Kaveri Sawant[1], Dattatray Sawant[2]
[1]*Assistant Professor, Universal College of Engineering, Vasai*
[2]*Assistant Professor, MPSTME,NMIMS University, Vile Parle*
Corresponding Author: Kaveri Sawant

Abstract: *Wireless sensor networks have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security. Energy efficiency and improving the network lifetime are the fundamental challenges in wireless sensor networks. Lack of centralized administration and coordinator are the reasons for wireless sensor networks to be vulnerable to active attack like black hole. The affected node, without knowing a reliable route to destination, spuriously replies to have shortest reliable route to destination and entice the traffic towards itself to drop it. Network of such nodes may not work according to the protocol being used for the routing . Use of multiple sinks can improve the data collection resulting in improved throughput, reduced delay and congestion but due to blackhole attack the overall performance of the network is reduced. In this paper a data collection algorithm using least cost path and ant colony optimization is used to address this issue which increases the network throughput and conserves energy resulting in maximum network lifetime and also designed a mechanism to tackle blackhole attack. A zone based partition is applied to implement the shortest path using ant colony optimization and a mechanism to detect a blackhole attack and the affected routes at an early stage. The residual energy of each node is calculated and the shortest path is selected using least cost and ant colony optimization A valid value is attached with RREP which ensures that there are no attacks occurring along the path. This approach is validated through the simulations in NS2.*
Index terms: *The work deals with the improvement in energy efficiency of the wireless sensor network using shortest reliable route and thus improving the throughput, delay and packet loss of the network and network secured with blackhole attack.*
Keywords: *Mobile sink, constrained path, residual energy, delay, throughput, least cost path, blackhole attack.*

Date of Submission: 27-03-2019 Date of acceptance: 11-04-2019

I. Introduction

Existing work shows the MULE architecture where the sensors transmit data only over a short range that requires less transmission power [1]. Lets consider in a city traffic monitoring application vehicles can act as MULES , in a habitat monitoring scenario, the role can be served by animals, in a national park monitoring scenario and people can be MULES [6]. In the scenarios where the trajectories of the mobile sinks are constrained or predetermined, efficient data collection problems are often concerned to improve the network performance [2] [3] [4]. The sink mobility can improve the performance of wireless sensor networks; where mobile sinks are mounted on some people or animals moving randomly to collect information of interest sensed by the sensor nodes where the sink is at random. The path constrained sink mobility is used to improve the energy efficiency of single hop sensor networks which may be in feasible due to the limits of the path location and communication power. This paper focuses on dense WSNs with path constrained mobile sinks that may exists in real world applications, such as ecological, environment monitoring and health monitoring. The mobile sink collects data from the sensor nodes while moving close to them. According to the communication range the monitored region can be divided into two parts, the direct communication area (DCA), and multihop communication area (MCA) for far off sensors. Sensor nodes with DCA, called subsinks can directly transmit data to the mobile sink due to their close proximity of the trajectory. On the other hand sensors with MCA, called members must first relay the data to the subsinks which completes the final data transmission to the mobile sink. The throughput depends on the data collected and the number of members belonging to each subsink.

II. Related Work

The existing research on sink mobility can be classified into the following categories: random path, controllable path and constrained path.

Various attacks against WSNs is explained in the literature.Various measures were proposed to face these attacks . The attacks are classified as passive attacks from the active attacks. The passive attacks are limited to listening and analyzes exchanged traffic. This type of attacks is easier to realize and it is difficult to detect. Since, the attacker is not allowed to make any modification on exchanged information. The intention of the attacker is the cluster head node and confidential data.In the active attacks, an attacker modifies the message in the network. He can also modify his own traffic or replay of old messages in order to disturb the operation of the network or to cause a denial of service. The active attacks are as follows:

Tampering: is the result of physical access to the node by an attacker; whose purpose will be to recover cryptographic material. [3]. Black hole: a node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network [1]. Selective forwarding: as mentioned above, a node play the role of router, in a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them. Sybil attack: Newsome et al. [5] attacker can use the identities of the others nodes in order to take part in distributed algorithms such as the election. HELLO flood attack: many routing protocols use "HELLO" packet to discover neighboring nodes and thus to establish a topology of the network. The simplest attack for an attacker is sending a flood of data to flood the network and to prevent other messages from being exchanged. Jamming: it consists in disturbing the radio channel by sending useless information on the frequency band used. This jamming can be temporary,or permanent [6]. Blackmail attack: In this a malicious node announces that another legitimate node is malicious to eliminate this last from the network. If the malicious node is successful in managing to tackle a significant number of nodes, it will be responsible to disturb the operation of the network.

A. Random path sink mobility

In random path the mobile sinks are placed on randomly moving creatures like animals, human beings. Due to this random mobility it is difficult to bound the data transfer latency and the data delivery ratio. An analytical model based on queuing theory is presented for random path which incorporates many detailed aspects such as different mule mobility models, radio characteristics etc.

B.Path constrained sink mobility:

Architecture of wireless sensor networks with mobile sinks (MSSN) is proposed for traffic surveillance application.It is also assumed that all sensor nodes in MSSN are located within the direct communication range of the mobile sink. A communication protocol and a speed control algorithm of the mobile sink are suggested to improve the energy performance and the amount of data collected by the sink. A routing protocol called Mobiroute [11] [12] is suggested for WSNs with a path predictable mobile sink to prolong the network life time and improve the packet delivery ratio, where the sink is moved at some anchor points and the halt time is much longer than the movement time. Accordingly, the mobile sink has enough amount time to collect data, which is different from the designed scenario. Moreover, in Mobiroute[11] all sensor nodes need to know the topological changes caused by the sink mobility.

C.Path controllable sink mobility:

Mobile element scheduling problem is studied, where the path of the mobile sink is optimized to visit each node and collect data before buffer overflow occurs. A partioning based algorithm is presented to schedule the movements of the mobile element to avoid buffer overflow. The mobile sinks will visit all sensor nodes to collect data accordingly and the path optimization is based on the constraint of buffer and data generation rate of each node. The path selection problem of a mobile device is focused to achieve the smallest data delivery latency in the case of minimum energy consumption at each sensor. It is however assumed that each sensor node will sends its data directly to the mobile device. Single hop communication is not feasible due to the limitation of road infrastructure and requirement on delivery latency. A rendezvous based data collection approach is proposed to select the optimal path due to the delay limitation in WSNs with a mobile base station [11] [12].

Black hole attack

It is also called as packet drop attack and it is similar to denial of service of attack. An internal node or external node can begin this attack [4]. At the beginning of a route discovery process the attacker node is present in the network, on receiving RREQ message, attacker will send a false RREP message to the node. This RREP message will reach the source node before the messages sent by other nodes because attacker will send this RREP without checking its route table. This RREP claims to have shortest route to the desired destination; where value of hop count is minimum and has maximum value of sequence number which indicates that fresh enough route to the destination is available. The source node will be tricked by this fake RREP and choose this path to transmit data packets. After the data packets are received, the attacker node will simply drop these packets.

D.Problem Formulation

Let n sensor nodes be deployed randomly and let 11s nodes close to the trajectory of the mobile sink be chosen as subsinks. The other 11m nodes away from the mobile sink choose different subsinks as their destinations. The mobile sink moves along a fixed dedicated path periodically with constant speed to collect data. It is assumed that the mobile sink has unlimited energy, memory computing resources and has enough storage to buffer data. Each sensor node is continuously collecting the data and transmits it either directly to the mobile sinks or to one of the subsinks which finally delivers the data to the mobile sink. The members within the multihop communication range need to choose one and only one subs ink as its destination. A highly dense sensor network is considered, in which all members can reach the subsinks through single-hop or multihop communication. Here the predictable mobile sink path is considered. The main objective is to improve the energy efficiency for gathering data, which minimizes the energy consumption of entire network under the condition of maximizing the total amount of data collected by the mobile sink. Network life time can be improved by optimal subsink selection which depends on the residual energy of the nodes. The problem is solved as follows.

E. Proposed System

A data collection scheme is proposed based on the multi-hop communication is designed to improve the amount of data and reduce energy consumption. Proposed protocol is a shortest path tree (SPT) is used to choose the cluster heads and route data, which may cause imbalance in traffic and energy dissipation. To address the imbalance problem, the Maximum Amount Shortest Path (MASP) scheme proposed is designed to enhance data collection from the viewpoint of choosing cluster heads more efficiently.If a mobile sink is mounted on public transportation, its speed cannot often be changed freely to the purpose of data collection. The mobile element visits exact decided locations, called rendezvous points, according to the pre computed schedule to collect data. The rendezvous points buffer and aggregate data originated from the source nodes through multihop relay and transfer to the mobile element when it arrives.

With respect to the proposed method, a validity value is attached with the RREP message and is stored in routing table at each node of active path. Whenever a node receives route request and if it is the intended destination or possess a legitimate route, then route reply message will be generated by setting the

value for validity bit in RREP . This RREP then will be sent back to its neighboring hop from which it obtained RREQ. The proposed route reply message is different from the validity value with the fundamental Advanced on demand distance vector routing route reply message. The validity value mechanism protocol is implemented in the RREP message. RREP of AODV will contain an extra header format bit in as validity bit. In the fundamental AODV protocol, route table contains following nine fields:

Destination IP address
• Destination Sequence Number
• Valid Destination Sequence Number Flag
• Other state and routing flags
• Network Interface
• Hop Count
• Next Hop
• Precursor List
• Lifetime

In addition to the above points the paper proposes an additional field for validity value. The validity of the route will be checked by this new method. Every time a node receives a route reply, it will be processed if and only if validity bit in that RREP is set. If the validity bit is set an entry for that route will be made.. The entry in the route table will consist of above mentioned nine fields plus one proposed in this paper i.e. validity value. Since the attacker will be unaware about this mechanism; he will reply without having a look in its route table. So validity bit will have null or zero value in the RREP sent by attacker node. A node which receives such a reply where validity value is not set will simple drop that RREP without making entry in the route table. Hence routing table will be free from the fake routes developed by the malicious nodes .

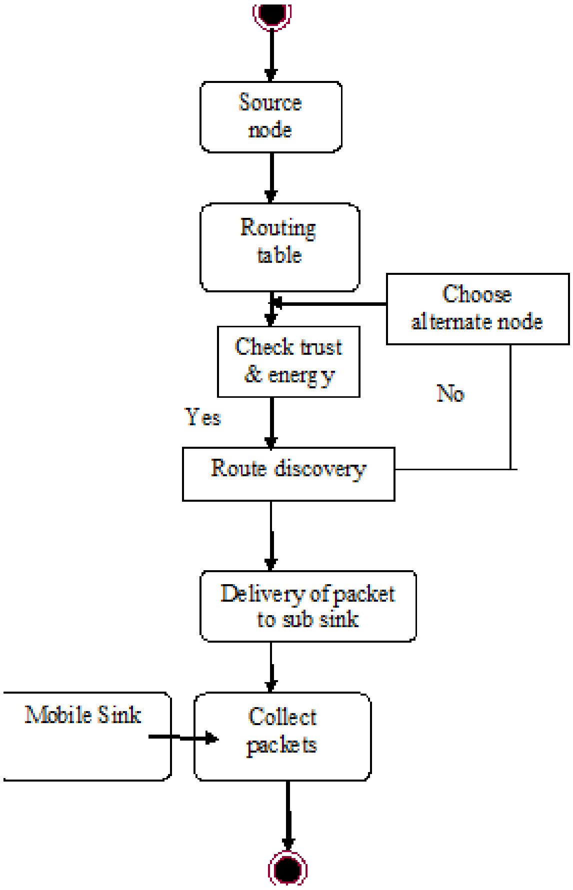

Figure:1 Flowchart of the proposed system

F. Problem solution

The proposed solution focuses efficient data collection using improved ant colony optimization. Ant Colony Optimization, a swarm intelligence based optimization technique, which is widely used in network routing. A novel routing approach using Improved Ant Colony Optimization algorithm is proposed for Wireless Sensor Networks consisting path constrained mobile sink. Ant colony optimization (ACO)[1] algorithms simulating the behavior of ant colony have been successfully applied in the proposed problem. Least cost path protocol is proposed to establish the shortest route that can satisfy the source node's requirements including energy, trust, and route length.

G. Proposed Algorithm:

(1)A wireless sensor network with N nodes is considered, where N nodes denote all the nodes in the network.
(2)The communication among the nodes is based on a tree topology with sink as the root.
(3)The sink first broadcasts a message with a hop counter
(4) The nodes receiving the message will set the message sender as the parent node, increase the hop count by one and broadcast it to their neighbor.
(5) Least cost path protocol is proposed to establish the shortest route that can satisfy the source nodes requirements, including energy, trust and route length.
(6) To establish the route to destination node D, the source node S broadcast a RREQ packet and waits for RREP packet.
(7) The source node embeds its requirements in RREQ packet and the nodes that can satisfy these requirements broadcasts the packet.
(8)The destination node establishes the shortest route that can satisfy the source nodes requirements.
(9) The rationale of this protocol is that the node that satisfies the source nodes requirements is trusted enough to act as a relay.
(10) The energy values of node are declared as numerical values such as 1,2,3,4 etc. and threshold of energy is assigned as 2, thus route is taken in such a way that node should have energy value of less than or equal to one.

III. Calculation of Parameters

In order to calculate the throughput in the scenario several bw variables are created in the record procedure and set them equal to bytes. The sample time is set to 0.9 so that the so that all the values will be updated every 0.9 seconds. Also holdrate variables are created and set equal to bytes_. The bw is the current number of bytes received and holdrate is the previous number of bytes received. Thus the throughput is calculated by adding them together and multiplying by 8 to convert from bytes to bits and dividing by 2 for the two intervals and then again multiplying by 1000000 to convert from bits to mega bits. And lastly dividing by the current time to obtain bits/s.

The number of lost packets are placed in a variable and then divided by the current runtime to get the number of packets lost per second. This calculation will be performed each time that record runs and the calculated value will be output to the trace file along with the current runtime.

If the current number of packets received is greater than the last number of packets received then subtract the most current last packet arrival time with the previous iterations of records most current last packet arrival time). Then divide this value by the current number of packets received minus the previous number of packets received

IV. Results and Discussion

Simulation setup:

Sr. No	Parameters	Values
1.	Radio Model	Two ray round
2	MAC type	802_11
3.	Antenna	Omni Antenna
4.	Max packet in ifq	50
5.	Number of nodes	5,10,15,20,28
6.	Routing protocol	AODV
7.	Dimension of topography	1000x1000 2000x2000
8.	Time of simulation	900 seconds
9.	Packet size	512
10.	Traffic type	CBR
11.	Max Speed	100

The performance parameters of the proposed data collection scheme using shortest reliable routing using ant colony optimization is implemented in NS2. Initial energy of each node including the sink, subsink and sensor nodes are set and the mobile sink moves with a constant speed. Three zones are created each having 9 nodes where 1,2 and 3 are subsinks and 0 is the sink. From the energy file generated low value energy nodes are selected for routing path and one hop neighbours are identified. Source node 10 routing path is created i.e. 10-7-6-1-0 where 0 is the sink node and 1 is the subsink. For another flow the the path is 14-15-2-0.The sink moves towards the subsink to collect the data packets. Multiple sinks can gather more data efficiently.

Here, the mapping between sensor nodes and subs inks is optimized to maximize the amount of data collected by mobile sinks and also balance the energy consumption. . The algorithm finds the shortest route which speeds up the packet delivery and provides energy efficient routing. The main objective of the paper is to improve the energy efficiency for data gathering, which minimizes the energy consumption of entire network under the condition of maximizing the amount of data collected by the mobile sink.

A, Figures and Tables

Least cost results for the delay, packet loss and throughput are shown below.

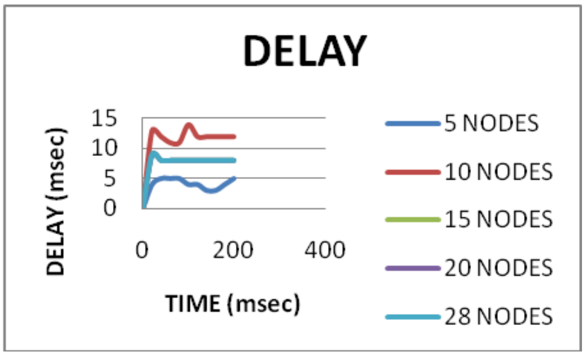

Figure 1. Graph for evaluation of delay

Figure 1 shows when the number of nodes sharing the network resources, the delay significantly consistent at 5msec high for 10 nodes increases.

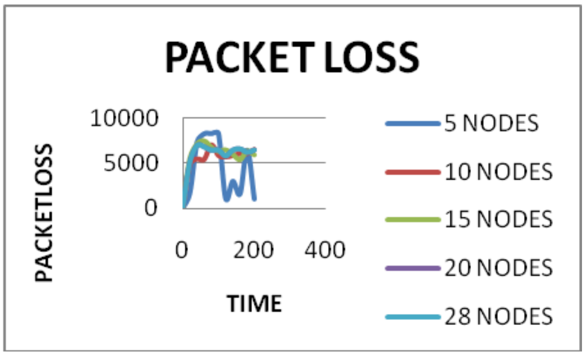

Figure.2. Graph for evaluation of packet loss

The figure 2 shows a high packet drop rate whenever the number of nodes sharing a network increases. It can be seen that the packet loss rate is fluctuating. This can be easily justified since we are making use of a mobile sink. However this high quality performance is deteriorated as the number of nodes sharing the network increases.

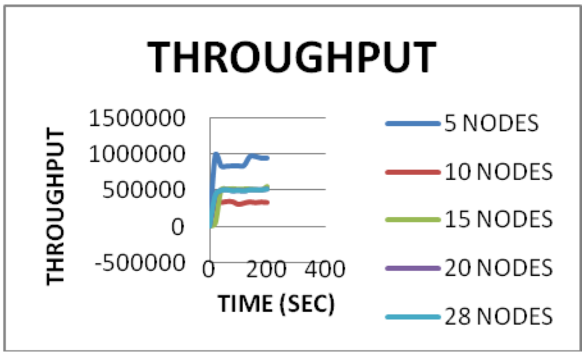

Figure.3. Graph for evaluation of throughput

It is been observed from the graph that least cost route has a better throughput than AODV routing which shows a maximum throughput of around 200.

Results for least cost path Protocol

	NUMBER OF NODES				
	5	10	15	20	28
Packet loss	0	328	294	342	342
Delay	14	7	15	16	16
Throughput	578	449	348	345	345
Energy	80	50	70	80	80

Table 1 Results of least cost path Protocol

Results for AODV protocol

	NUMBER OF NODES				
	5	10	15	20	28
Packet loss	0	250	140	250	250
Delay	33	140	120	120	120
Throughput	350	350	350	350	350
Energy	70	50	60	70	70

Table 2 Results of AODV Protocol

From the above results we can say that Shortest reliable routing protocol gives a better performance than AODV routing by finding the shortest route to the destination and thus by consuming less energy and increasing the network lifetime of the network.

V. Conclusion

This paper proposes an efficient data collection scheme using least cost path and ACO [1] for wireless sensor networks with path-constrained mobile sinks. Here, the mapping between sensor nodes and subs inks is optimized to maximize the amount of data collected by mobile sinks and also balance the energy consumption. An improved least cost algorithm, based on the basic ant colony algorithm is implemented where the subsinks receive the packets and deliver to the sink node.. The previous search probability of the path is introduced in every search to speed up the search. The algorithm finds the shortest route which speeds up the packet delivery and provides energy efficient routing. The main objective of the paper is to improve the energy efficiency for data gathering, which minimizes the energy consumption of entire network under the condition of maximizing the amount of data collected by the mobile sink. For future work we can validate the proposed scheme on different scenarios with various movement trajectories of mobile sinks and study the subsink selection problem.

Acknowledgement

I would like to express my deep and sincere gratitude towards institute and my college, his wide knowledge and logical way of thinking have been of great value for me. His understanding, encouraging and personal guidance have provided a good basis for the present thesis. I would like to thank him for his invaluable guidance, patience and constructive feedback.

References

[1]. Anil Kumar, Anil Thomas "Energy Efficiency and network lifetime maximization in wireless sensor networks using improved Ant colony optimization" IEEE 20180.

[2]. RC. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling a Three-Tier Architecture for Sparse Sensor Networks," Proc. Fir& IEEE Int'I Workshop Sensor Network Protocols and Applications, pp. 30 -41, 2003

[3]. S. Jain, RC. Shah, W. Brmette, G. Borriello, and S. Roy, "Exploiting Mobility for Energy Efficient Data Collection in Sensor Networks," Mobile Networks and Applications, voL I I, no. 3, pp. 32 7-339, 2006.

[4]. A Chakrabarti, A Sabharwal, and B. Aazhang, "Communication Power Optimization in a Sensor Network with a Path- Con& rained Mobile Observer," ACM Trans. Sensor Networks, vol. 2, no. 3, pp. 297-324 , Aug. 2 006.

[5]. L. Song and D. Hatzinakos, "Architecture of Wireless Sensor Network s with Mobile Sinks: Sparsely Deployed Sensors," IEEE Trans. Vehicular Technology, vol. 56, no. 4, pp. 1 826-1 836, July 2 007.

[6]. D.Jea, A. Somasundara, and M Srivastava, "Multiple Controlled Mobile Elements (Data Mules) f or Data Collection in Sensor Networks," Proc. Fir& I EE E/ACM Int'l Conf. Distributed Computing in Sensor Systems (DCDSS), pp. 2 44 -257, 2005.

[7]. A. Kansal, A Somasundara, D. Jea, M. Srivastava, and D. Erin, "Intelligent Fluid Infrastructure for Embedded Networks," Proc. ACM Mobi Sys, pp. 111- 124,20 04 .

[8]. J. Lill, J. Panchard, M. Piorkowski, M Grossglauser, and J. Hubau x, "MobiRoute: Routing towards a Mobile Sink f or Improving Lifetime in Sensor Networks," Proc. Second IEEEI ACM Int'I Conf. Distributed Computing in Sensor Systems (DCOSS), pp. 480-497 , 200 6.

[9]. A. Somasundara, A Kansal, D. Jea, D. E:;trin, and M . Srivastava, "Controllably Mobile Infrastructure for Low Energy Embedded Networks," I EEE Trans. Mobile Computing, vol. 5, no. 8, pp. 958- 973, Aug. 2 006.

[10]. M Wang, S.Basagni, E. Melachrinoudis, and C. Petrioli, "Exploiting Sink Mobility f or Maximizing Sensor Networks Lifetime," Proc. 38th Ann. Hawaii Int'l Conf. System Sciences, p. 287a, 2005.

[11]. S. Gao, H. Zhang, and S.K. Das, "Efficient Data Collection in Wireless Sensor Networks with Path-Constrained Mobile Sinks," Proc. 1 0 th IEEE Int'l Sym p. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2009.

[12]. A. Somasundara, A. Ramamoorthy, and M. Srivastava, "Mobile Element Scheduling for Efficient Data Collection in Wireless Sensor Networks with Dynamic Deadlines," Proc. 25t h IEE E In!'1 Real-Time Systems Symp. (RTSS), pp. 296-305, 2004.

[13]. R Sugihara an d R Gupta, "Improving the Data Delivery Latency in Sensor Networks with Controlled Mobility," Proc. Fourth IEEE Int'l Conf . Distributed Computing in Sensor Systems (DCDSS), pp. 386-399,2008.

[14]. M.Shankar, Dr.M.Sridar, Dr.M.Rajani" Performance Evaluation of LEACH Protocol in Wireless Network" International Journal of Scientific & Engineering Research, Volume 3, Issue 1, January-2012 1 ISSN 2229-5518

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Kaveri Sawant. " Improved Network Lifetime And Secured Routing Against Blackhole Attack In Wireless Sensor Networks Using SRR.." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 14.2 (2019): 30-36.