THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Extended Bridge Protection Algorithm :An Technique For Fault Tolerance In Sensor Network

Abhinav Sharma
Departement of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India

Vinay Kumar
Departement of Computer Engineering Technology, Guru Nanak Dev University, Amritsar,India

Namarta Vij
Departement of Computer Science and Engineering , Lovely Professional Univeristy,Punjab,India

Abstract

Sensor network's operating scenario makes them susceptible to various catastrophic events which can then led to simultaneous failure of a plethora of nodes deployed in a particular geography. After recovering from any such event a resultant topology of the network is generally unstable and contains various fragments which are linked by a single or few bridge nodes which have gate nodes on a far side and fan out nodes on a near side of the sink. These significant nodes are prone to failure while bearing high load, because of a significant link position they have in the resultant operative scenario.

This paper describes a series of intelligent decisions in an algorithm named as, extended bridge protection algorithm (EBPA),which is designed to protect these nodes from performing unnecessary computations. These decisions are about distribution and shifting of some unnecessary communication which helps in reduction of number of messages transmitted in a network and hence saving the energy of these topologically significant nodes, and hence, prolonging the network's lifetime.

Keywords: Resilient sensor networks, fault tolerance, extended bridge protection algorithm

Introduction

An approproitae approach is used to select the physical location of the Sensor Nodes so that all the operational and sensing requirements of the customer are satisfied, but unfortunately there are various reasons due to which one or more sensor nodes goes offline. The reason can be battery drain, intruder's unwanted activities, human interference or natural catastrophic events. Nodes from a particular area goes offline (or destroyed) due to these events, it makes sense to design an orthogonal algorithm to protect all the functional motives of the rmaining WirelessSensorNetwork (WSN) nodes,which remains functional even after a major CE, since, it is very difficult to redeploy these SN's after any CE owing to harsh conditions

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

related to environment and sensitive locations of the WSN, our mechanism must be tolerant/resilient enough to survive after the CE, and must remain functional for its maximum possible time.
Generally, after the CE, we recalculate the routing tables and the available routes are figured out by analyzing the properties of remaining available live nodes.

Now, in the worst case scenario: The new network's topology is in such a state that several partitions are connected with each other by only one node and that single node is the sole link between those two partitions and there can be more than one such partition also. So, the failure of that link node converts the partitions into disjoint sets.

The disadvantage of this particular link's failure and creation of two disjoint partitions is that even after having one partition operational and actively sensing the environment, this partition will not be able to transmit its observations to the sink since the link between the two partitions is terminated. So the link node which acts as the bridge between two partitions is very significant as its failure leads to a severe degradation in the sensing quality even after having much of the nodes functioning properly.

Due to the uncertainty of the area, time, and outcome of the CE, This scenario cannot be handled at the design time by providing high energy or high capacity battery to the Bridge node as the Bridge node is not detected until any CE is occurred and without the prior knowledge of CE, we cannot decide which node to give more energy.

To better understand the functionality and principle of Bridge protection and then optimize it to Extended Bridge Protection Algorithm (EBPA), a hypothetical situation is considered where connectivity still exists after the event which are catastrophic, whereas the network is transformed into a fragmented network. The connectivity is through a single bridge node which is the only intersection point between the two partitions.

We will consider the bridge node, as a node, removal of which will lead the network topology into two disjoint sets.

In contrast to the nodes which are constructed to bear high loads at run time, bridge nodes are general purpose nodes which, after some unpredictable CE remains the only link between two partitions of the network and are called as bridge nodes.

These nodes do not have long transmission range or high energy, and with their limited resources they are supposed to transmit the complete observations of one part to the sink side in order to keep the WSN operational.

This document describes a series of reactive measures in the form of EBPA. An early version of which is discussed in [13].

EBPA is a reactive algorithm in response to a CE observed by the network. The goal of EBPA is to prolong the network's life time and keep it operational with a desired level of sensing quality.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

EBPA alters the way the bridge node(s), its neighboring nodes, and some of the other significant nodes which are identified at run time after the CE, behave. It transfers some of the calculation (processing) done at sink to these special nodes in order to reduce the traffic burden of the significant and vulnerable nodes.

Its goal is to delay the failure of bridge and gate nodes to prevent further partitioning of the network by imposing policies which tries to prevent or delay the creation of new bridge nodes.

In the section 2, the considered scenario, some quality metrics and the method using which CE is mentioned. In the section 3, basic principle behind the extended bridge protection method which includes the approaches of particular nodes in the local area of the Bridge node. In the section 4, Simulation criteria considered for creating the results and the comparison between EBPA, BPA. This section further describes how does a sensor network responds to a catastrophic event. In the section 5 and 6 , Related work and conclusion is discussed

SECTION 2: Catastrophic events in an intruder detection sensor network

2.1 The operating scenario and the topology of the network

This is regarding an intruder detection system which providing observations regarding an interest such as surroundings of a strategically crucial military installation or a sensitive environment or ecological system such as on high altitude mountains or in a very remote and sensitive area of ocean. In these types of operational scenarios nodes, which costs hundreds to thousand dollars are deployed at very careful and strategically important locations with the nodes expected to have larger energy consumption (e.g. Nodes close to the sink) which can be identified during the design time by having a prior knowledge of geographical area is provided high capacity batteries. The grid's depth may vary according to the transmission distance of the nodes. The ideal and optimized arrangement suggests that all nodes should be under the transmission range of one hope away neighbors but out of the transmission range of two or more hope away neighbors. This arrangement suggests a hexagonal grid type structure with central node's connectivity with up to 8 nodes including the diagonal ones.

Common sense engineering consideration suggests that the transmission range should be a slightly larger than the connectivity range for better transmission of the signals.

In practice, however environmental strategic conditions such as obstacles, camouflage requirement forces the user to deviate from of a perfect grid arrangement most of the times. The customer will definitely prefer to place its node to a strategically important location rather than at some perfect grid position. In the resultant lattice game plan "with noise" a few nodes probably won't have the option to arrive at all of its close to neighbors however they may potentially arrive at one expectation away neighbors. The principle data stream on the system is coordinated towards sink hub from the sensor hub.

All the nodes detects the intruder in their range and then sends their observation to the sink node by a "hop by hop" approach which then transmits the data directly to the user.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Normally practiced routing algorithms for a permanently deployed sensor network are also worth discussion. Quick response and reporting of each intruder is a fundamental design requirement of these systems. This hard requirement forces the used routing algorithm to deliver the packet to the sink by using minimum number of hopes. It is analyzed that need cannot not refer to a routing approach. Multifarious routing techniques used in wireless sensor networks can qualify for these criteria on prioritize routing protocols such as gradient based techniques, and centralized techniques also falls under this categories. These algorithms are distinguished on the basis of their decision making when significant modifies in the network topology are triggered by node failures and by the mobility of nodes. Also each routing algorithm has its own routing overheads and cost of the signaling required establishing and modifying the routes.

In the remainder of this paper, we will consider any of the above generic algorithms which converge to the shortest path as our baseline algorithm (SP) and we will also compare the performance of EBPA and its previous version BPA.

With the most brief way combination presumption, the sending ways in the sensor system will look like as in fig. 1.

The main motive of sink node is in (a) Intruder tracking (b) Monitoring the health of the sensor network.

2.1.1 Intruder tracking task

The main objective of the sink node is to track the intruder and particularly, it wants the latest location of each intruder present inside the interested area. The sink also desires that the location of the intruder is confirmed by one or more nodes independently. The assumption made in the operating scenario is that each node's own observation will be transmitted after fixed intervals but other node's observations are transmitted immediately.

It may be noted that the proposed algorithm is orthogonal to and can be easily combined with various additional strategies for making the whole system more energy efficient such as aggregation and selective transmission of reports.

2.1.2 Sensor network health monitoring

One of the many important duties of the sink node is to correctly interpret the existing health of the sensor network in order to make it more reliable. On the off chance that a node isn't sending any perception information, it can mean, either that the node isn't having any intruders in its detecting range, or that the node isn't practical .

Heartbeat signal will be automatically replaced by any reported observation.

2.2 Types of catastrophic events

A catastrophic event can be describe as a immediate loss of a major number of sensor nodes by any mean but our main discussion will be on geographically limited catastrophic events, which destroys a very big

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

chunk of the sensor nodes in the overall topology graph. Such events can occur because of floods, forest fires, chemical contamination or the action of opponent forces. Depending on the relative position of the geographic area of the CE and the interest area, there can be several cases based on the impact of the CE, which are considered and distinguished on the basis of the remaining ability of the sensor network.For each case, we have also suggested an appropriate response to a CE by the network and its user in order to restore the operations.So, in order to prolong the network's connectivity, the prolonged life time of the bridge node is of utter importance and our described technique in the remainder of the paper focuses on to reduce the traffic burden from this significant node which becomes crucial for the whole network's sensing ability after an CE.

3. Basic Objectives of Extended bridge protection algorithm

3.1. The topology of a network with bridged fragments

Base of the approach used in the remainder of the paper lies in the topological position and functionality of some important nodes. These nodes are identified after the CE based on their relative position in the resultant network topology and are discussed in this section. It is assumed that before the occurrence of CE shortest path routing is followed by the network to transmit data to the sink node (Fig. 1).

So to restore the operations of the sensor network after CE re computation of the routing tables is done first. This case is illustrated in Fig.3where two fragments are created with a connecting bridge node. For performing the analysis we will assume that there are only two bridged fragments however there can be n number of fragments based on the impact of the CE. For further discussion in the paper, the fragment which contains the sink will be called as the side near and the fragment.

A bridge node is the node whose removal will create disjoint fragment and disconnect a fragment from sink node's connectivity. Number of bridge nodes after CE depends upon the nature of CE and there can be n number of bridge nodes in the resultant network topology. The nodes which are adjacent to the bridge node on the far side are called gate nodes. Since the bridge node is the only link between the near and far segments so bridge node have to transmit all the traffic load of far side to the sink. Similarly, the adjacent nodes on the near side segment are called as fan out nodes. It is intuitive that there will always be more than one fan out and gate node because otherwise that node will also be considered as a part of the bridge. The sensor nodes connected with the gate nodes on the far side are called extended gate nodes (EGN) which are responsible for the convergence of observed data of the far side onto the gate nodes. A gate node can be connected to one or more EGN. Fig. 4 can be referred for an example of the location of the bridge node, gate node, fan-out nodes and EGN.

3.2. The prime objectives of the Extended bridge protection algorithm

The main objectives of introducing the extended bridge protection algorithm are as follows:

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Bridge node protection: The EBPA must be able to diminish the energy of the bridge node and should divert unnecessary computation to other nodes in order to prolong its lifetime when compared using the response of the network.

Protect the creation of new bridge nodes: Since a bridge node is the vulnerable link for the network's lifetime so creation of new bridge nodes should be prevented by conserving fan out and gate node's resources and prevent them from performing unnecessary computation.

Ensures minimal intrusion and report every intrusion: The critical functionality of any intruder detection system is to ensure zero intrusion and detail report of every intrusion attempt so this functionality should be sustained by EBPA algorithm.

3.3 EBPA functionality at EGN

The EBPA algorithm focuses on reducing the traffic reaching at the gate nodes and thus saving the bridge also from that data load (see Algorithm 2). So EBPA suggest to shift some processing done at the sink to the EGN in order to prevent the gate nodes and the bridge node from processing less important data.

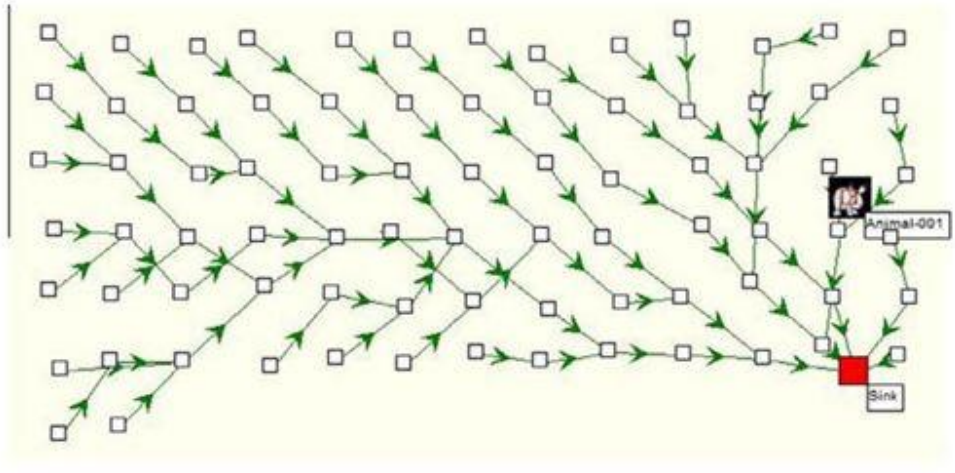


Fig.1. Forwarding paths followed by network packets with default SP routing in normal operational scenario.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

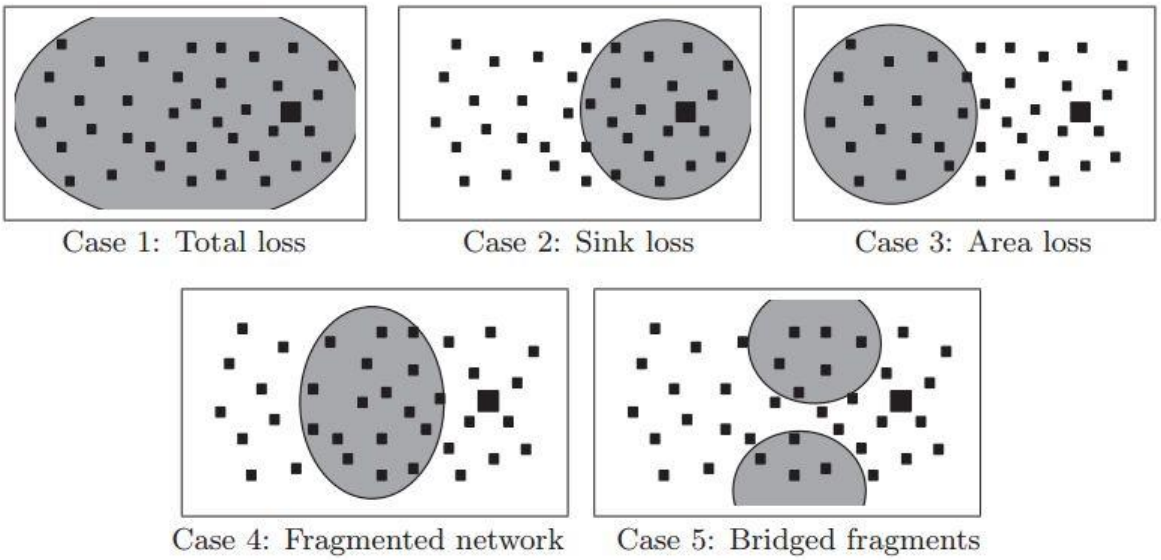


Fig. 2. Possible impacts on the network by a catastrophic event.

The functional responsibility of the sink is shifted to the extended gate nodes and not to the gate nodes or bridge nodes because gate or bridge nodes are nothing but normal working nodes which are trapped in significant and crucial position after the CE these nodes are not designed to handle large traffic loads. So EBPA suggests that rather than putting the complete load on the gate nodes it is wise to distribute in among gate node's neighbors. If there are minimum two gate nodes in the network topology then there must be at least four EGN, so we have reduced the complete load of the gate nodes and by distributing it to the EGNs we are optimizing on two fronts. First, we are reducing the burden of the gate and bridge nodes and second, we are saving on the messages needed to be transmitted between EGN and gate nodes. It is a slight advantage over the previous version of EBPA i.e. Bridge Protection Algorithm (BPA) which forces gate nodes to handle the high load of far side segment. Thus theyare more likely to drain their energy soon if traffic is not handled intelligently.

So an extended gate node will start processing these two types of fundamental messages differently:

1. Heartbeat messages: In normal operation the every node sends a heartbeat message destined to sink which is an indicator to the sink that the node is alive and operational a node which sends neither the heartbeat message nor the observation message after some time quantum is considered to be a dead node and routing tables are updated accordingly.

The time interval between any two successive heartbeat messages is generally kept long but still they can cause a significant load on bridge and gate nodes since they are a part of the traffic needed to be transmitted to the near side by bridge and gate nodes and after any CE it is desired that bridge node should only transmit the critical messages which must reach sink. To implement this reduction of number of messages transmitted, the extended gate nodes will take on the charge from sink and start performing the reasoning about the operational status of the far side nodes. Extended gate nodes only allow the node failure messages

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

to transmit through the gate and bridge node that too if necessary. Since it is taking the responsibility of performing the reasoning about the live status of the nodes of far side segments the extended gate nodes are required to send their own heartbeat messages through the gate and bridge nodes.

2. Occlusion reasoning (see Algorithm 2 lines 3–13): From any intruder detection system it is desired that it should provide the most recent observation which should possess the most recent location of the intruder the historical observations are discarded by the sink but due to the nature of routing algorithms and availability of multiple paths often obsolete messages reaches at the sink which then are discarded by the sink node. These messages are of no use to the sink but in the process of reaching at the sink they consumeprecious energy resources of the gate and bridge node which may later cause them to die sooner. The occlusion reasoning technique (similar to that deployed in [2]) suggested in the EBPA shifts this processing at the extended gate nodes. It suggests introducing a delay of ΔT in the forwarding time of messages about every intruder after getting the last report about the same intruder. Due to this delay the node gets additional time to collect any obsolete or new information about the intruder.

The node will only transmit the most recent observation about the intruder after the delay time has passed. Occlusion reasoning might seems a very good alternative to decreases the number of messages passing through the node but the delay introduced in the transmission can cost us in hard real time scenarios and thus it is not suggested to deploy this strategy at every node if our goal is to report every intruder's location in minimum possible time. However this strategy can be implemented on extended gate nodes because these nodes are located just before the vulnerable gate and bridge nodes and efforts must be done here only to decrease the traffic by eliminating the obsolete messages and in long term running scenarios the cost of delays is justified by the prolonged lifetime of the network.

3.4 EBPA functionality at gate nodes

After any CE gate nodes are the middle and significant link between the EGNs and the bridge so their conservation is a very important task as their failure may lead to create more bridge nodes. If after the CE the remaining energy left in the gate nodes is less than that of the bridge node then these gate nodes becomes the critical nodes rather than the bridge node. So in order to reduce the transmission and processing burden from these nodes and prevent them from failure, only the utmost important messages such as failure messages of the nodes and the observation messages will be passed to them for transmission to the near side. The processing overhead saved will be more if there are large number of sensor nodes which sends the Heartbeat signal and have multiple and obsolete observations. Since the extended gate nodes will take care of these processing tasks.

3.5 EBPA functionality at bridge nodes

The bridge node functionality will be the same as suggested in [13] since it is the only link between the far and near side of the network all the filtered messages sent from EGNs and gate nodes will pass through bridge in order to reach at sink. After passing through sink their first encountered node in the near segment is the fan out node and if all the traffic from bridge node is diverted to a single fan out node then this node may

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

be in danger of exhausting the resources and this fan out node may have another duties like to pass other node's and its own observations to the sink which may results in further overloading of tasks to a single fan out node so EBPA suggests to distribute the load between all of the fan out nodes in a round robin fashion (see Algorithm 3). The gate, bridge, EGNs and fan-out nodes after a catastrophic event can be figured out in Fig. 4.

3.6 EBPA functionality at fan-out nodes

The fan out nodes will also behave in the same way as suggested by [13].The suggested technique will prevent fan out nodes from exposing to heavy traffic as the load will be distributed equally among all fan out nodes in round robin fashion. There is a special case generally in large sensor networks in which the traffic will converge to a single node This condition can occur if two or more fan out nodes are forwarding traffic with a common successor so in this case that successor can be in danger of exhausting its resources which may not be good for a network which already had suffered a CE. These cases can be handled by providing high capacity batteries to the nodes which are closer to sink since there is quite a possibility of these kinds of circumstances (see Algorithm 4)**.** This solution is already practiced very commonly by the sensor network designers.

4. Simulation Study

4.1 Simulation scenario

We have designed the simulation scenario to analyze the performance of BPA-SP, EBPA-SP and the baseline shortest path routing approaches after an occurrence of CE. We have tried to simulate the CE and the counter response of the network in the form of above three algorithms.The simulation is done in the NS2 simulator **[6]**. All simulation parameters are described in **Table 1**. The simulation scenario consists of 40 sensor nodes deployed in an area of 500×250 m. The simulation scenario includes the presence of **5–10** intruders. It is assumed that intruders are movable objects with a variable speed between **5–20 m/s**. All the sensor nodes send their observation of intruder's location and if there is not any intruder present inside their sensing range they will send a heartbeat message after 10 seconds. Energy dissipation method details are given in the table itself and are adopted from **Rappaport [3]**.

4.2 Catastrophic events, recovery and bridge protection

Our aim is to demonstrate the behavior of a network which survives from a CE and the resultant topology is of the form of fragmented segments connected by a bridge node.

In our simulation scenario our network starts with normal operation and after the simulation time of 5 sec (at $t_k = 5$ s) the network becomes a bridged segmented network because of two CE occurred in the network and we will analyze the performance of the network by simulating three different types of responses to the same event by the network in the form of following routing algorithms:

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

SP: This strategy does not involve any bridge protection technique and re calculate the shortest paths to transmit the data to the sink it is the baseline response to a CE by the network.

BPA-SP: This is bridge protection algorithm working orthogonally to shortest path algorithm. In this response topologically significant nodes are identified after the CE and functionalities of some nodes are altered as suggested by **[13]**.

EBPA-SP: This is the suggested strategy in this paper. This technique suggests shifting some of the reasoning done at the sink to the EGNs which are identified after a CE and the strategy is discussed in the section 3 onwards.

4.3 Total transmitted messages

We have considered the total number of messages transmitted as performance criteria and in this simulation we have compared the number of messages sent in each scenario with constant number of intruders in all the three scenarios. The total number of messages sent by SP were largest followed by BPA and then EBPA. All the three algorithms are followingthe same routing paths but the differential in the numbers arise due to the shifting of processing From

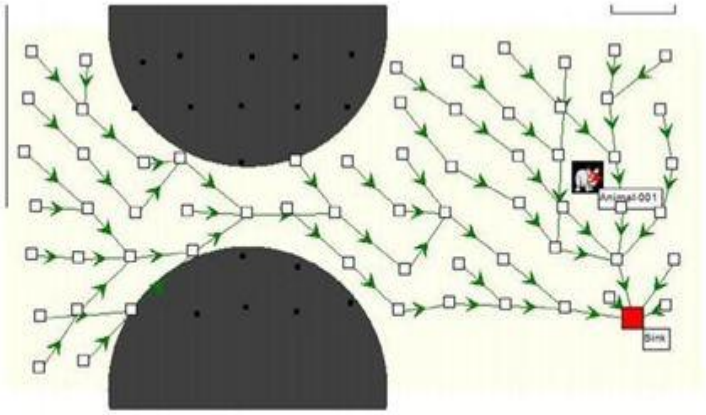


Fig. 3. Forwarding paths recalculated by the baseline shortest path response after the CE

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

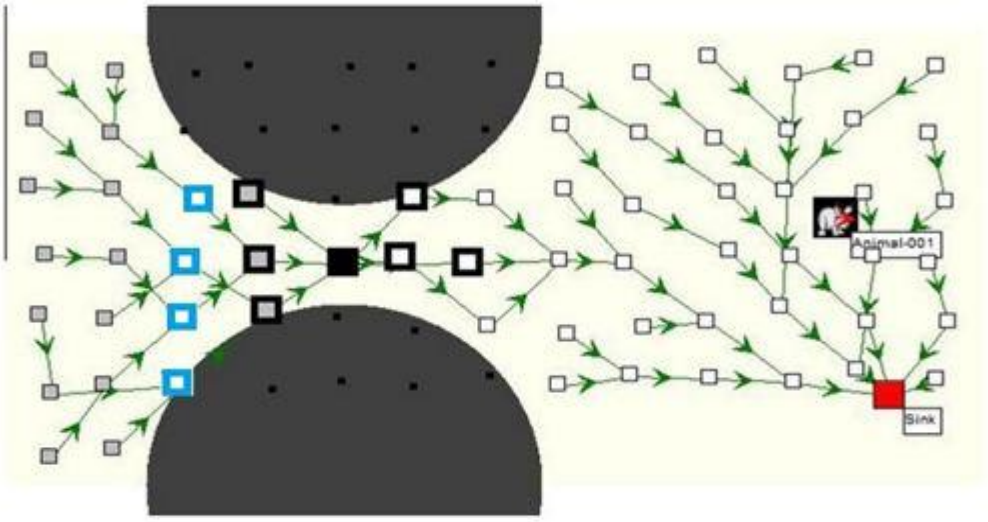


Fig. 4. Forwarding paths using the extended bridge protection algorithm after the CE. The special nodes are marked as follows: extended gate nodes: blue border, gate nodes: black border surrounding gray square, bridge node: solid black, fan out nodes: black border surrounding white square.

Algorithm 1: Default behavior of sensor nodes[13]

```
1: When received intruder report m do
2:     forwardMessage(m)
3:     reset heartbeat timer
4: End When
5: When received heartbeat message m do
6:     forwardMessage(m)
7:     reset heartbeat timer
8: End When
9: When intruder i sighted do
10:    m' = new message
11:    m' = intruder identifier, location, time of sighting
12:    forwardMessage(m')
13:    reset heartbeat timer
14: End When
15: When heartbeat timer expired do
16:    m' = new heartbeat message
17:    forwardMessage(m')
18: End When
```

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Algorithm 2. Behavior of an extended gate node in EBPA[13]

1: When received intruder report m about intruder i from node x originating in y **do**
2: reset heartbeat timer for x and y
3: p= most recent report about intruder i
4: if p== null **then**
5: set a delayed transmission timer for i
6: end if
7: if m.sightingTime > p.sightingTime **then**
8: set m as the most recent report about intruder i
9: discard p
10: else
11: discard m
12: end if
13: End When
14: When timer for intruder i expired do
15: m= most recent report about intruder i
16: forward Message(m)
17: End When
18: When received heartbeat message m **from** node x originating in y **do**
19: reset heartbeat timer for x and y
20: End When
21: When heartbeat timer expired for x
22: m= heartbeat failed for x
23: forwardMessage(m)
24: End When
25: // other events handled as default

Algorithm 3. Behavior of a bridge node in EBPA[13]

1: When received intruder report m about intruder i **do**
2: choose next hop f from the fan-out nodes using round-robin
3: forward m to f
4: reset heartbeat timer
5: End When
6: // other events handled as default

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Algorithm 4. Behavior of a fan-out node in EBPA[13]

1: When received intruder report m about intruder i
do
2: choose next hop f using the load splitting routes
3: forward m to f
4: reset heartbeat timer
5: End When
6: // other events handled as default

sink to the gate and extended gate nodes in BPA and EBPA algorithms respectively. Number of messages depends upon the number of hopes required to reach packet's destination and sometimes number of hopesare increased because the closest individual neighbor on the sink side is selected by the routing algorithm.

4.4 Bridge node energy consumption

The bridge node's energy consumption will remain optimized as it was in the previous version of EBPA as we are only allowing critically important messages to pass through the bridge node but it will be significantly reduced when compared with the default baseline response of the network.

4.5. Maximum energy consumption of a fan-out node

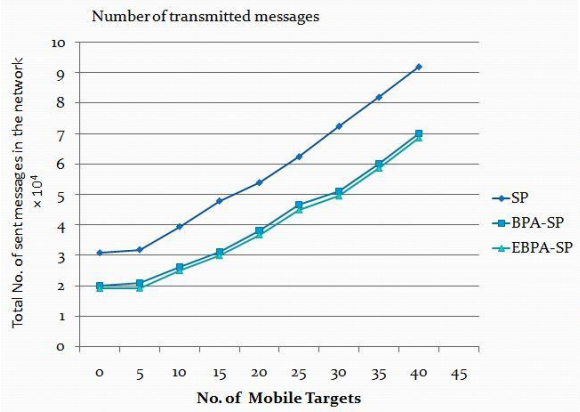
The fan out nodes can also be under danger of draining their energy resources rapidly if significant amount of traffic is converged to a single fan out node and since demise of a fan out node can also cause performance degradation of the whole network for long time, its energy consumption analysis is necessary. However the load on the fan out node depends on the physical position of the intruders. It is been observed in the simulationthat the energy consumption of the fan out node is increased with increase in number of intruders for all of the three simulated strategies. It is found that the energyconsumption of fan out nodes is reduced by same amount in BPA and EBPA strategies when compared with the baseline SP algorithm.

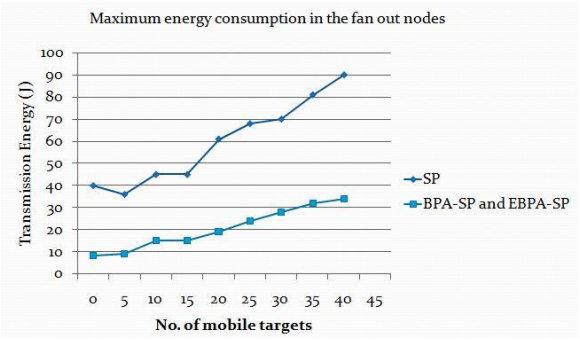
4.6 Network life extension ratio

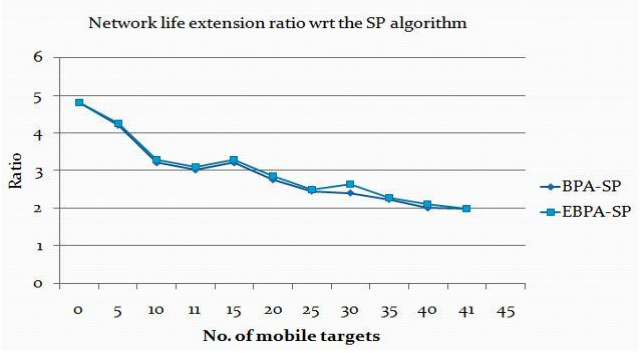
The objectives of the suggested EBPA strategy is to prolong the network lifetime and considering the partitioning of the network as the end of network functionality which can be because of the extension of the bridge or gate node this algorithm has shown significant improvement over the default response of the network. This algorithm conserves the bridge node with the same set of rules suggested by its previous base version BPA and it additionally deploys strategies to protect the gate nodes also. The best case in which EBPA can show its benefit is when the gate nodes are left with very little energy (even less than bridge node) so that the gate nodes become the critical link for the network's life time.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

In most of the simulating scenarios it has increased the network's life time nearly 1.5 times and sometimes even 2 times when compared with the default baseline SP algorithm for 30 intruders and if the number of intruders are less then there are very little energy dissipation of bridge nodes resulting to prolonged network's life time by 4-5 times. To compare this algorithm with BPA-SP we have to consider the scenarios where gate nodes possess very little energy and then EBPA showed slightly better statistics and the network's life time was increased about 1.1 to 1.2 times. This is also a significant improvement since every second's increase in the network's life time enables us to collect more amount of precious data from the environment.







ISSN: 0971-1260
Vol-22-Issue-3-July-2019

General settings		Heartbeat message	10 s
Number of nodes	40	Interval	
Distribution area	500×250 m	Simulation time	50 s
Interest area	500×250 m	**Transmission power model**	
Sensing range	150 m	Path loss index n	4
Transmitting range	140 m	α_{11}	45 nj/bit
Sink node location	(475,125)	α_2	0.001 pj/bit/m^4
Intruder specifications		**Catastrophic events**	
Intruder speed	5-15 m/s	Event 1: at t = 5, circular area, range 200, center (250, 50)	
Number of intruders	5-30	Event 2: at t = 5, circular area, range 200, center (250,240)	

Table1: Simulation parameters for results generation

5. Related work

It was believed in earlier sensor network literature that introduction of fragmentation in sensor network makes it dysfunctional because the main objective of sensing is not fulfilled after the partition [7]. In sensor networks literature prime focus was on to delay the fragmentation (for example energy aware routing) but a little was on the scenarios when fragmentation is already done (or is about to happen). But now since the fault tolerance of sensor networks is become a primary concern so a lot of investigation and development is done for the scenarios where the network topology is converted in to loosely link fragmented networks. The current techniques to counter these circumstances are divided in two sections. The first section suggests recovery of the fragmented network by using mobile nodes as a new link between fragments of the networks. One of the technique is the Data mule architecture [8] is one of the initial approaches of this kind. A more recent work proposed[9,10] suggests the use of linear optimization techniques and heuristics to enhance the remaining lifetime of the resultant fragmented network after a CE.[11,12] proposed the use of mobile relay nodes (MRs) as a link between fragmented sensor network partitions. Closed queueing network was used in the calculation of the Mathematical model of the expected movement of the [14,15] has suggested shifting some of the existing mobile nodes to the critical link positions to perform the recovery process after a CE the new position of nodes will provide single or double node connectivity in order to make the SN functional again. One can classify these techniques as a hybrid between the relay node-based and mobile node-based approaches. The same scenario is studied by[16]and Imran et al.[17–19].

Some suggested[20] a solution which introduces the concept of using some special nodes called message ferries are used for the communication services between the mobile network nodes. There were two approaches discussed in the paper which depends upon the initiation of movement that is whether the nodes are moving close to the ferries or ferries are moving towards nodes in order to communicate. There is another approach In contrast to the approaches which suggests mobility of existing nodes should be used as a solution for the connectivity, opportunistic networking[21] uses protocols which take advantage of

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

movements of nodes to bring the data closer to their respective destination. Cascaded node movement was proposed [22] to prevent the fragmentation of the network. This idea works has two phases of working. In the first phase a nearby sensor node of a failure node is located for replacement. Low movement is the preferred criteria for the selection. Then in the second phase second phase cascaded movements between sensor nodes is used in order to rearrange the network. Its basic principle is to move the nearby node instead of bringing a new node to improve and maintain the connectivity of the overall network. The optimized number of relay nodes required is also very difficult to calculate as shown [23] in their study. They proved that getting the minimum possible number of relay nodes to maintain the connectivity is of the complexity order equivalent to the NP-hard problems.[24] uses the in the fragmented state of the network, and suggested a solution by using a combination of deploying new relay nodes and upgrading the existing resources. This solutions converts the problem of finding optimum number of relay nodes into a mixed-integer nonlinear programming problem where each solution has two components. Since the problem was a part of NP hard set so to solve this non deterministic heuristic approach was suggested by the author, which performs the transformation of the problem into a linear programming problem, without wasting too much energy resources for the computation. [25] investigate and suggested a solution which addresses the relay node placement problem. Their solution solves both the issues of maintenance of connectivity and also fulfills the quality of service requirements. The EBPA algorithm tries to postpone the event of gate and bridge node's failure and hence it delays the further partitioning of the network.

6. Conclusions

Therefore, we have taken an intruder tracking sensor network which after the occurrence of a CE is transformed into bridged segments. Such networks have vulnerable failure points in the form of bridge node and gate nodes which are exposed to high traffic load for which they are not designed to encounter. An EBPA strategy is suggested to protect such nodes in order to continue the network's lifetime by distributing their load to their significant neighbors in the network topology. Using a simulation study It has proved that by applying this protocol we can boost the lifetime of the network after CE about 2 to 5 times over the default SP response of the network and almost 1.2 times over the previous version of EBPA algorithm.

7. References

[1] L. Bölöni, D. Turgut, Protecting bridges: reorganizing sensor networks after catastrophic events, in: Proc. of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC-2011), 2011, pp. 2028–2033.

[2] D. Turgut, B. Turgut, L. Bölöni, Stealthy dissemination in intruder tracking sensor networks, in: Proc. of IEEE Local Computer Networks(LCN 2009), 2009, pp. 22–29.

[3] T. Rappaport, Wireless Communications: Principles & Practice, Prentice-Hall, 1996.

[4] D.-T. Lee, A.K. Lin, Generalized Delaunay triangulation for planar graphs, Discr. Comput. Geomet. 1 (1) (1986) 201–217.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[5] K.J. Supowit, The relative neighborhood graph, with an application to minimum spanning trees, J. ACM (JACM) 30 (3) (1983) 428–448.

[6] L. Bölöni, D. Turgut, YAES – a modular simulator for mobile networks, in: Proc. of the 8-th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2005), 2005, pp. 169–173.

[7] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Networks 52 (12) (2008) 2292–2330.

[8] R. Shah, S. Roy, S. Jain, W. Brunette, Data mules: modeling and analysis of a three-tier architecture for sparse sensor networks, Ad Hoc Networks 1 (2–3) (2003) 215–233.

[9] S. Basagni, A. Carosi, C. Petrioli, Heuristics for lifetime maximization in wireless sensor networks with multiple mobile sinks, in: Proc. of the IEEE ICC'09, 2009, pp. 1–6.

[10] S. Basagni, A. Carosi, C. Petrioli, C.A. Phillips, Coordinated and controlled mobility of multiple sinks for maximizing the lifetime of wireless sensor networks, Wireless Networks 17 (3) (2011) 759–778.

[11] H. Almasaeid, A. Kamal, Data delivery in fragmented wireless sensor networks using mobile agents, in: Proc. of the ACM Int'l Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2007), 2007, pp. 86–94.

[12] H. Almasaeid, A. Kamal, Modeling mobility-assisted data collection in wireless sensor networks, in: Proc. of the IEEE Global Communications Conference (GLOBECOM-2008), 2008, pp. 1–5.

[13] P. Levis, N. Lee, M. Welsh, D. Culler, TOSSIM: accurate and scalable simulation of entire TinyOS applications, in: Proc. of the 1st International Conference on Embedded Networked Sensor Systems, 2003, pp. 126–137.

[14] A.A. Abbasi, K. Akkaya, M. Younis, A distributed connectivity restoration algorithm in wireless sensor and actor networks, in: Proc. of 32nd IEEE Conference on Local Computer Networks (LCN 2007), 2007, pp. 496–503.

[15] A.A. Abbasi, M. Younis, K. Akkaya, Movement-assisted connectivity restoration in wireless sensor and actor networks, IEEE Trans. Parallel Distrib. Syst. 20 (9) (2009) 1366–1379.

[16] K. Akkaya, F. Senel, A. Thimmapuram, S. Uludag, Distributed recovery from network partitioning in movable sensor/actor networks via controlled mobility, IEEE Trans. Comput. 59 (2) (2010) 258–271.

[17] M. Imran, M. Younis, A. Md Said, H. Hasbullah, Volunteer-instigated connectivity restoration algorithm for wireless sensor and actor networks, in: Proc. of IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS 2010), 2010, pp. 679–683.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[18] M. Imran, M. Younis, A.M. Said, H. Hasbullah, Partitioning detection and connectivity restoration algorithm for wireless sensor and actor networks, in: Proc. of the 8th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC 2010), 2010, pp. 200–207.

[19] M. Imran, M. Younis, A. Md Said, H. Hasbullah, Localized motionbased connectivity restoration algorithms for wireless sensor and actor networks, J. Network Comput. Appl. 35 (2) (2012) 844–856.

[20] W. Zhao, M. Ammar, E. Zegura, A message ferrying approach for data delivery in sparse mobile ad hoc networks, in: Proc. of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2004), 2004, pp. 187–198.

[21] L. Pelusi, A. Passarella, M. Conti, Opportunistic networking: data forwarding in disconnected mobile ad hoc networks, IEEE Commun. Mag. 44 (11) (2006) 134–141.

[22] G. Wang, G. Cao, T. La Porta, W. Zhang, Sensor relocation in mobile sensor networks, in: Proc. of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM-2005), vol. 4, 2005, pp. 2302–2312.

[23] X. Cheng, D. Du, L. Wang, B. Xu, Relay sensor placement in wireless sensor networks, Wireless Networks 14 (3) (2008) 347–355.

[24] Y. Hou, Y. Shi, H. Sherali, S. Midkiff, On energy provisioning and relay node placement for wireless sensor networks, IEEE Trans. Wireless Commun. 4 (5) (2005) 2579–2590.

[25] S. Lee, M. Younis, QoS-aware relay node placement in a segmented wireless sensor network, in: Proc. of the IEEE Int'l Conference on Communications (ICC 2009), 2009, pp. 1–5.