ISSN No: - 2456 - 2165

Multi-hop Cost Aware Secure Routing in Wireless Networks

Priyanka Shelare
M.E. (IV-Sem) Dept. of W.C.C.,
AGPCE, R.T.M.N.U., Nagpur, India
piu.shelare@gmail.com

Yogesh Bhute
Assistant Professor, Dept. of C.S.E.
AGPCE, R.T.M.N.U., Nagpur, India
yog.bhute@gmail.com

***Abstract* — Wireless sensor networks are an important for monitoring distributed remote environments. As one of the key technologies involved in WSNs, nodes fault detection is indispensable in most WSN applications. It is well known that the distributed fault detection scheme checks out the failed nodes by exchanging data and mutually testing among neighbor nodes in this network, but the fault detection accuracy of a scheme would decrease rapidly when the number of neighbor nodes to be diagnosed is small and the node's failure ratio is high. Cost Aware Secure Routing protocol to address these two conflicting issues through two adjustable parameters: energy balance control and probabilistic based random walking. CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. The main objective to have a network which gives assurance of packet delivery and give the node time to regain its so that it will be able to carry further load Packets on the network. This can be done by using shortest path. Prior work relies on maintaining multi hop neighbor lists and predetermines some criteria for the node's involvement in the recovery. Multi hop based schemes often impose high node repositioning overhead and the repaired inter actor topology using two hop schemes may differ significantly from its pre-failure status.**

Keywords *— Cost Aware Secure Routing, Electronic Book Code, multi hop, Security, topology, Wireless Sensor Network.*

I. INTRODUCTION

Wireless sensor networks are composed of massive, small and low-cost sensor nodes deployed in a monitoring region; forming a multi hop self organized network system through wireless communication. The target is to cooperatively sense, collect and process the information about objects in the node failure, and then sends it to the observer for processing and analyzing. The sensors serve as wireless data acquisition devices for the more powerful actor nodes that process the sensor readings and put forward an appropriate response a failure of an actor may cause the network to partition into disjoint blocks and would thus violate such a connectivity requirement. The remote setup in which WSANs often serve makes the deployment of additional resources to replace failed actors impractical, and repositioning of nodes becomes the best recovery option when a node fails, its neighbors will individually consult their possibly incomplete routing table to decide on the appropriate course of actions and define their role in the recovery if any. If the failed node is critical to the network connectivity, i.e., a node whose failure causes the network to partition into disjoint blocks, the neighbor that belongs to the smallest block reacts. Require every node to maintain a list of their multi-hop neighbors and determine the scope of the recovery by checking whether the failed node. Cost Aware Secure Routing protocol for WSNs to balance the energy consumption and increase network lifetime. CASER has the flexibility to support multiple routing strategies in message forwarding to extend the lifetime while increasing routing security. Both theoretical analysis and simulation results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. Our analysis and simulation results show that we can increase the lifetime and the number of messages that can be delivered under the non-uniform energy deployment by more than four time.The main aim is to detect the failure node using shortest path to send the data and recover the failure node and also maximize the sensor network lifetime, due to this the traffic load is on the single node which cause the bottleneck in the network traffic .we ensure that the energy consumption of all sensor grids are balanced. To achieve a high message delivery ratio, our routing protocol should try to avoid message dropping by multiple node path when an alternative routing path exists and recover.

- It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized.
- CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing
- Trace back attacks and malicious traffic jamming attacks in WSNs.
- We assume that the WSNs are composed of a large number of sensor nodes and a sink node.
- The sensor nodes are randomly deployed throughout the sensor domain. Each sensor node has a very limited and non-replenish able energy resource.
- The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy.

Considering such a problem with collocated node failure is more complex and challenging in nature to investigate this issue. Also includes factoring in coverage and ongoing application tasks in the recovery process and developing a for evaluating the various failure recovery schemes. Sensing and

ISSN No: - 2456 - 2165

data processing are essential WSNs have many more nodes and are more densely deployed Hardware must be cheap; nodes are more prone to failures WSNs operate under very strict energy constraints. Node failures are very improbable unless a part of the deployment area includes factoring in coverage and ongoing application tasks in the recovery process and developing a test bed for evaluating the various failure recovery schemes. Probability for multiple nodes to fail at the same time is very small and would not be a concern the smallest block inward toward the failed node; it may negatively affect the node coverage. The connectivity restoration problems are subjected to path length constraints. Basically, in some applications, such as combat robotic networks and search-and-rescue operation, timely coordination among the actors is required, and extending the shortest path between two actors as a side effect of the recovery process would not be acceptable. For example, interaction among actors during a combat operation would require timeliness to accurately track and attack a fast moving target. A novel approach is proposed. It relies on the local view of a node about the network to relocate the least number of nodes and ensure that no path between any pair of affected nodes is extended relative to its pre failure status. A novel protocol should try to avoid message dropping and create alternate path for massage forwarding and repair the faulty nodes.

II. PROPOSED WORK

To avoid the excessive state-update overhead and to expedite the connectivity restoration process, prior work relies on maintaining multi-hop neighbor lists and predetermines some criteria for the node's involvement in the recovery. Multi-hop-based schemes often impose high node repositioning overhead, and the repaired inter-actor topology using two-hop schemes may differ significantly from its pre failure status.

- ***Number of deployed actors (N):*** This parameter affects the node density and the WSAN connectivity. Increasing N makes the WSAN topology highly connected.
- ***Communication range:*** All actors are assumed to have the same communication range.
- The value of affects the initial WSAN topology. While a small creates a sparse topology, a large boosts the overall connectivity
- ***Total travelled distance:*** reports the distance that the involved nodes collectively travel during the recovery. This can be envisioned as a network-wide assessment of the efficiency of the applied recovery scheme.
- ***Number of relocated nodes:*** reports the number of nodes that moved during the recovery. This metric assesses the scope of the connectivity restoration within the network.
- ***Number of exchanged messages:*** tracks the total number of messages that have been exchanged among nodes. This metric captures the communication overhead.
- ***Number of extended shortest paths:*** reports the total number of shortest paths between pairs of nodes that get extended as a result of the movement-assisted network recovery. Shortest paths are calculated.
- ***Shortest paths not extended:*** reports average number of shortest paths that are not extended per topology: This metric assesses how serious the potential path extension.
- The messaging overhead dramatically grows as the node count increases. On the other hand, requires maintaining one-hop neighbor information for performing the recovery. Thus, an extra N message overhead is considered for to exchange information initially at the network startup.

III. METHODOLOGY

Cost-Aware Secure Routing protocol for WSNs to balance the energy consumption and increase network lifetime. CASER has the flexibility to support multiple routing strategies in message forwarding to extend the lifetime while increasing routing security. Both theoretical analysis and simulation will showing that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. CASER support secure delivery to prevent routing trackback attack and malicious traffic jamming attack in Wireless Sensor Network. This combinational technology helps to improve the recovery scheme.

Step 1: Network creates and forwards the data

Step 2: Check the node is active or not
If $Ea > N_A$
Send the data from the path
Else if $Ea < N_A$
Then node is fail & applies the recovery scheme send the data
Else if faulty nodes repair
Then Active the previous path
Else nodes fail

Step 3: Update the routing table and select the shortest path for data transfer.

Step 4: Stop.

Since Ea (A) is defined as the average energy level of the nodes in N_A. N_A is the selected hop grid from the network node.
This can happen due to changes in the topology caused by node mobility or due to the fact that subsets of actors do not need to interact and that a route has yet to be discovered. In general, a partially populated SRT can raise the following three issues or a distributed implementation.

1) A potential BC actor does not realize that its failed neighbor is a critical node.
2) Every neighbor of the faulty node assumes that it is not part of the smallest block leaving the network topology unrepaired.

ISSN No: - 2456 - 2165

3) More than one neighbor in different blocks step forward.

If the process starts it maintain the routing table and generate the routing list. As per the implementation of caser it analyzes the failure nodes and using shortest routing path send the data and balance the load. It also recover the failed node send the another data from the node.

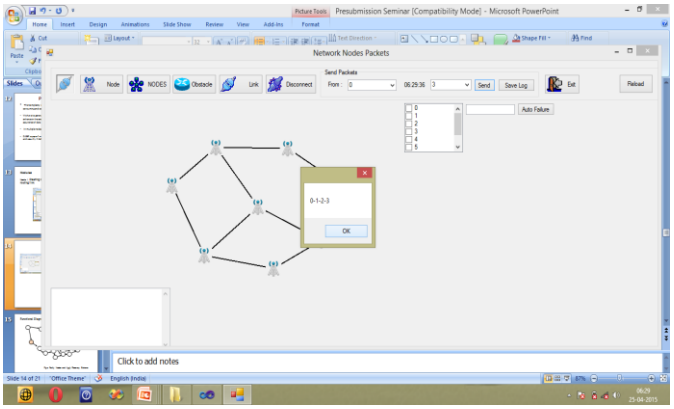

Figure 1: Routing Generation

This scenario select the nodes for transmission i.e. node 0, node 1, node 2 and node3 using shortest path. The select the node for transmission the node 0 then transfer to the node 1 forward the packet to node 2 then transfer to node 3. The routing path are generate from node 0 to node 1 to node2 and node 3. So data transfer from this routing path. For the data transmission generate the routing path for the routing path generation need to add the selected nodes from the routing table. To select the node from the routing table and add to the routing path generation.

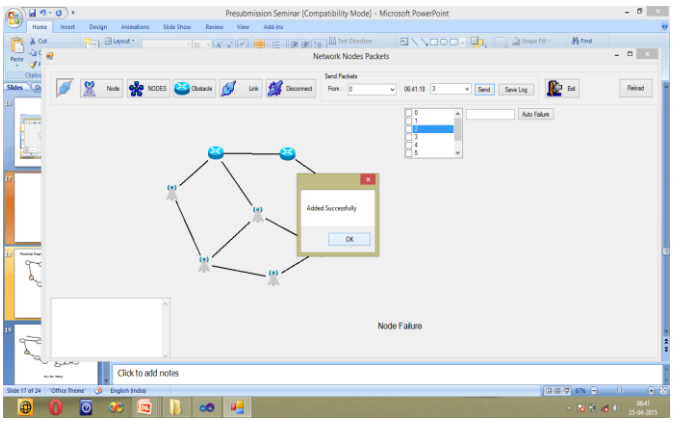

Figure 2: Packet Routing

The flow of the project firstly starts the process, maintain the routing table and send the data using shortest path. CASER calculate the energy level of the nodes if the energy level of the nodes is less for forwarding of the data packet. CASER determine the failure nodes. It applies the recovery scheme. So send the data from another shortest path. CASER giving time to regain the faulty nodes, so they are in repair state. So data packet is send from the previous path. First start the process maintains the routing table and sends the data from shortest path. Check the state of the network if it is ok then sends the data packet. If the state of network is not ok determine the failure nodes and apply the recovery scheme. The CASER giving a time to failure nodes for repairing. So that the data send from the previous path then stop the process.

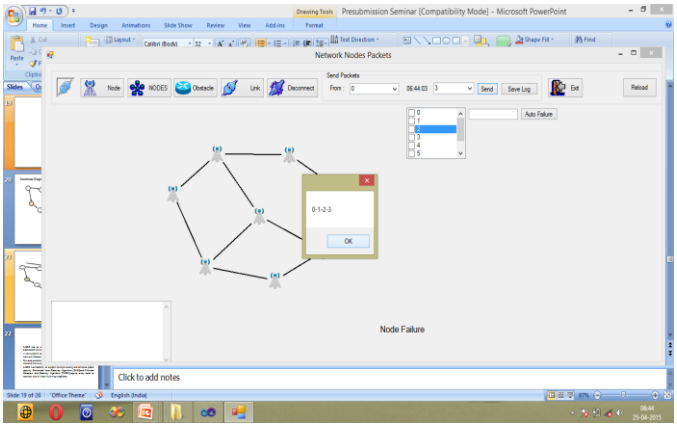

Figure 3 : The repair of failure nodes

This scenario shows the repair the failure nodes. Due to applying the recovery scheme the failure nodes giving the time for regain, so that they are able to transmit the data. The figure shows the repairing of the failure nodes. It has a time for regain the failure nodes so that it is in repair state so that the data is transfer from the previous routing path. The failure nodes are node1 and node2 have a time to regain, So that the data send from the previous routing path. The repair of node by the combinational methodology.

The proposed algorithm has been carried out using the network simulator *.net.* To improved the version of recovery Scheme.

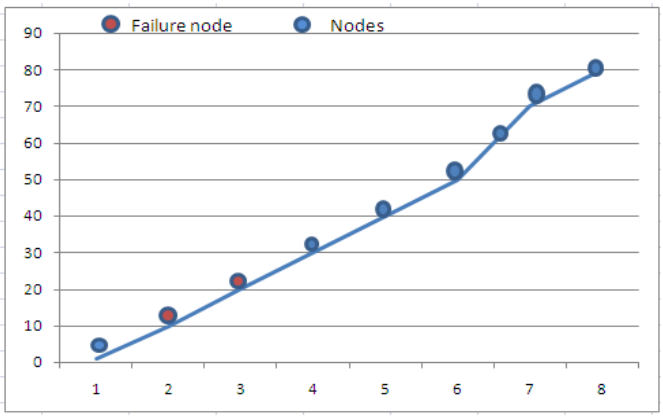

Figure 4: Multiple Nodes failure detection

IV. CONCLUSION

In this project, to propose a secure and efficient Cost-Aware Secure Routing Protocol for WSNs to balance the energy consumption and increase network lifetime. Our analysis and simulation to showing that we can increase the lifetime of wireless sensor network and to maintain a list of their multi-hop neighbors and determine the scope of the recovery by checking whether the failed nodes. It also provides the assurances to packet delivery. CASER has flexibility to support multiple routing. The main objective to have a network which gives assurance of packet delivery and give the time to the

ISSN No: - 2456 - 2165

nodes for regain, so that it will be able to carry further load Packets on the network. This can be done by using shortest path. Prior work relies on maintaining multi-hop neighbor lists and predetermines some criteria for the node's involvement in the recovery. Multi-hop-based schemes often impose high node repositioning overhead and the repaired inter-actor topology using two-hop schemes may differ significantly from its pre-failure status.

REFERENCES

[1] Hong Guo, Gangxiang Shen, *Senior Member, IEEE*, Sanjay K. Bose, *Senior Member, IEEE et al* **"**Routing and Spectrum Assignment for Dual Failure Path Protected Elastic Optical Networks**",** 2169-3536 (c) 2016 IEEE. Translations

[2] K. Akkaya. A. Thimmapuram, F. Senel, amd S.Uludag, *in Proc Workshop FedSenS, Istanbul, Turkey*, "Distributed recovering of actor failuresin wirelesssensor and actor networks", July 2011.

[3] O. Gerstel, M. Jinno, A. Lord, and S. B. Yoo, *IEEE Communications Magazine, vol. 50, no. 2, pp. s12-s20*, "Elastic optical networking: A new dawn for the optical layer?" Feb. 2012.

[4] Y. Wei, G. Shen, and S. K. Bose, *in Proc. ACP pp. AF1I-4*, "Applying ring cover technique to elastic optical networks," 2013.

[5] Y. Wei, G. Shen, and S. K. Bose, *IEEE Transactions on Reliability no. 63, vol. 2, pp. 401-411*, "Span-restorable elastic optical networks under different spectrum conversion capabilities," Jun. 2014.

[6] J. Wu, Y. Liu, C. Yu, and Y. Wu, *Optic-International Journal for Light and Electron Optics, vol. 125, no. 16, pp. 4446-4451*, "Survivable routing and spectrum allocation algorithm based on *p*-cycle protection in elastic optical networks," August 2014.

[7] F. Ji, X. Chen, W. Lu, J. J. Rodrigues, and Z. Zhu, *in Proc. GLOBECOM pp. 2170-2175*, "Dynamic *p*-cycle configuration in spectrum-sliced elastic optical networks," 2013.

[8] X. Chen, F. Ji, and Z. Zhu, *IEEE/OSA Journal of Optical Communications and Networking, vol. 6, no. 10, pp. 901-910*, "Service availability oriented p-cycle protection design in elastic optical networks," Oct. 2014.

[9] X. Chen, S. Zhu, L. Jiang, and Z. Zhu, *IEEE/OSA Journal of Light wave Technology vol. 33, no. 17, pp. 3719-3729, "*On spectrum efficient failure-independent path protection p-cycle design in elastic optical networks," Sep. 2015.

[10] H. M. N. S. Oliveira and N. L. S. da Fonseca, *in Proc. GLOBECOM pp. 1278-1283*, "Algorithm for FIPP p-cycle path protection in flex grid networks," 2014.

[11] M. Klinkowski and K. Walkowiak, *in Proc. ICUMT pp. 670-676*, "Offline RSA algorithms for elastic optical networks with dedicated path protection consideration," 2012.

[12] M. Klinkowski, *in Proc. CISIS pp. 167-176*, "A genetic algorithm for solving RSA problem in elastic optical networks with dedicated path protection," 2013.

[13] M. Klinkowski, *Cybernetics and Systems vol. 44, no.6-7, pp. 589-605*, "An evolutionary algorithm approach for dedicated path protection problem in elastic optical networks", August 2013.