International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep-2016 www.irjet.net p-ISSN: 2395-0072

REVIEW PAPER ON LIFETIME OPTIMIZATION AND SECURITY IN WIRELESS SENSOR NETWORK USING COST-AWARE SECURE ROUTING PROTOCOL

Tambe Vijayshree C.[1], Jadhav Chandrakant M.[2]

[1] *Student of ME,Dept of Computer Science and Engg,Solapur University,Maharashtra,India*
[2] *Assistant Professor,Dept of Computer Science and Engg,Solapur University,Maharashtra,India*

Abstract – *Now a days, wireless networks are facing number of drawback to transfer the data from source to destination through the various routings. In that two major issues are extremely effect on networks those are network lifetime and security. Therefore, lifetime improvement and security are the main challenging design issues in this paper. To realize these two challenges for the primary time we tend to projected (CASER) Cost Aware Secure Routing protocol during this paper. According this paper, in existing we tend to used uniform energy preparation within the networks. Through this uniform energy deployment strategy, network lifetime reduced extremely. For that in our protocol we provide non-uniform energy deployment strategy.*

Key Words **- Wireless Sensor Networks, Energy Balance control, Random Walking, Deterministic Routing, Security in CASER;**

1.INTRODUCTION

Wireless sensor networks (WSNs) are a main used for monitoring allotted far off environments. As some of the key technologies concerned in WSNs, nodes fault detection is crucial in most WSN applications. It is well known that the distributed fault detection scheme checks out the failed nodes via commutation data and mutually checking out among neighbor nodes on this network. However, the fault detection accuracy of a scheme would reduce quickly once the amount of neighbor nodes to be diagnosed is low and therefore the node's failure ratio is excessive. A multiplied scheme is projected through process novel detection criterion. Simulation results demonstrate that the accelerated scheme performs well within the higher than crisis and might develop the fault detection accuracy typically. Wireless sensor-actor networks, sensors probe their surroundings and ahead their data to actor nodes. Actors collaboratively reply to achieve predefined software mission. In view that actors ought to coordinate their operation, it's example to maintain a powerfully connected configuration systematically. Additionally, the dimensions of the inter-actor communication methods can be restricted to fulfill latency demand. Wireless sensor community are designed to look at movements or setting alterations sensors are unfold around a factory to watch distance, forming a multi-hop self-prepared network technique by means that of wireless communication. The sensors wireless data acquisition instruments for the additional robust actor nodes that route the sensor readings and advance a right response. Failure of Nodes could foundation the community to partition into reinstate blocks and would so violate this sort of property demand. The readying of any resources to exchange failing nodes impractical and position of nodes becomes the superb restoration possibility. Once a node fails its neighbors nodes can separately request advice their probably partial routing desk to decide on the suitable manner of actions and description operates among the healing if any. If the unsuccessful nodes are principal to the community property, i.e. a node whose failure causes the community to partition into reinstate blocks, the neighbor nodes that belongs to the smallest block reacts. The goal is to with consideration feel, accumulate and procedure the data concerning objects among the nodes failure further as then send it to the observer for process and examining. Sensors self readying offers with unbiased insurance policy formation in sensor community actors are additional ready nodes with somewhat involved additional energy deliver and richer computation and dispatch assets. The transmission sort of actors is considerably a lot of less. It is integral for actors to believe most likely on existing radio links for coordinative themselves. Distributed Actor Recovery algorithm further as Partition Detection and Recovery algorithm need every node to take care of a record of their multi-hop neighbors and check the scope of the healing through checking whether or not or not the failing nodes. Cost-Aware Secure Routing protocol for WSNs to steadiness the energy consumption and develop network lifetime. CASER has the pliability to assist multiple routing techniques in message forwarding to lengthen the lifetime as increasing routing safety. Each theoretical analysis and simulation can

exhibit that, CASER has a satisfactory routing performance in terms of energy balance control and routing direction distribution for routing course security. We tend to additionally projected a non-uniform energy readying scheme to extend the sensor network lifetime. Our analysis can showing that we tend to are able to develop the life and therefore the variety of messages which will be delivered below the non-uniform energy deployment by means of greater than four occasions. CASER supports secure delivery, to hinder routing trackback attack and malicious website visitor's congestion attack in wireless sensor communication.

2. EXISTING SYSTEM

The current methodological progresses create sensor networks possible to be wide utilized in both military and civilian applications. The nature of such networks makes communication delay, energy consumption and security the foremost essential problems for wireless sensor networks. However, these problems are also conflicting with each other. The present works typically try and optimize one in every of these key problems while not providing sufficient diversity and adaptability of varied alternative needs in protocol design. During this dissertation, we tend to investigate the connection and design trade-offs among these conflicting problems. By using ancient system we tend to face some issues like: a lot of energy consumption, Increase the network collision, scale back the packet delivery ratio, Cannot provide complete security for packets, more cost, Time consuming.

3. RELATED WORK

Routing is also a difficult task in WSNs because of the restricted resources. Geographic routing has been wide viewed together of the foremost promising approaches for WSNs. Geographic routing protocols utilize the geographic location data to route data packets hop-by-hop from the source to the destination. The provision chooses the immediate neighboring node to send the message supported either the direction or the gap. The gap between the neighboring nodes is estimated or no inheritable by signal strengths or mistreatment GPS equipments. The relative location data of neighbor nodes are modified between neighboring nodes. A Geographic adaptive Fidelity (GAF) routing scheme was planned for detector networks ready with low energy GPS receivers. In GAF, the network area is split into mounted size virtual grids. In each grid, only one node is chosen as a result of the active node, whereas the others can sleep for a quantity to avoid wasting lots of energy. The detector forwards the messages supported greedy geographic routing strategy. An issue based Geographic and Energy Aware Routing (GEAR) was planned. In GEAR, the sink node disseminates requests with geographic attributes to the target region instead of pattern flooding. Each node forwards messages to its neighboring nodes supported estimated value and learning price. The estimated price considers every the gap to the destination and additionally the remaining energy of the detector nodes. Whereas, the tutorial value provides the change data to touch upon the native minimum drawback; whereas geographic routing algorithms have the advantages that every node exclusively should maintain its neighboring data, and provides a stronger an improved efficiency and a more robust scalability for large scale WSNs, these algorithms might reach their native minimum, which can end in dead end or loops. To resolve the native minimum disadvantage, some variations of those basic routing algorithms were planned, as well as GEDIR, MFR and compass routing rule. The delivery quantitative relation is improved if each node is alert to its two-hop neighbors. Time period is another area that has been extensively studied in WSNs.

4. FRAME WORK

In our theme, the network is equally divided into little grids. Each grid incorporates a relative location supported the grid data. The node in each grid with the best energy level is chosen as a result of the head node for message forwarding. To enhance, each node inside the grid will maintain its own attributes, as well as location data, remaining energy level of its grid, additional as a result of the attributes of its adjacent neighboring grids. The data maintained by each sensor node are updated intermittently.

System Design: during this paper, we tend to design a protocol i.e., CASER protocol. To use this protocol within the wireless sensor network at first we need to design the network. In figure1, we tend to consider that in our network we have additional range of sensors and one sink node. During this network are going to be partitioned as grids. In every grid equivalent sensor nodes are deployed. From the figure, we have four grids and in each grid have five sensor nodes. For complete network we have only single sink node.

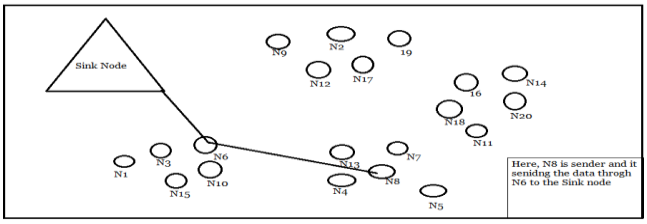

Fig- 1: CASER Protocol Network Design

It suggests that the sink node is simply destination for all sensor nodes. The data of the sink node is made public. For

security functions, each message will be assigned a node identity equivalent to the situation the place this message is initiated. To prevent adversaries from raising the source location from the node identity, a dynamic id will be used. The content of every message also can be encrypted creating use of the key shared between the node/grid and therefore the sink node. We tend to additionally anticipate that each sensor node is attentive to its relative neighborhood among the sensor area and has competencies of its instant contiguous neighboring grids and their vigor levels of the grid. The understanding concerning the relative space of the sensor domain may even be broadcasted inside the network for routing data replace. Routing methods in CASER in this protocol, two types of methods are there: 1) Deterministic Routing Strategy and 2) Random Walk Routing Strategy.

Deterministic Routing: actually, the CASER protocol works supported two adjustable routing parameters such as follows: 1) Energy Balance control (EBC) and 2) random walk. In deterministic routing, we tend to use the EBC parameter. During this strategy we tend to implement the non-uniform energy readying strategy. During this strategy, initially all sensor nodes have constant energy and when some time they lose few quantity of energy. Remaining energies are we need to calculate initial. After that we tend to should choose the user grids.

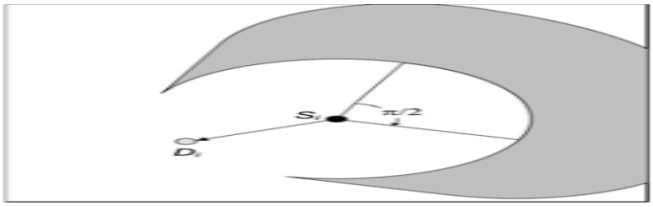

Fig-2: Deterministic Routing

User grids suggest that based on calculated energy levels of sensor nodes; in each grid we have one high energy level node. We tend to choose that node to routing which node grid is referred to as a candidate grid. Supported elite candidate grids we tend to formulate a shortest path. Through that shortest path we tend to are causing the data. Finally, we are able to maintain the energy levels of the sensor nodes within the network. Like this, we are able to optimize the network lifetime with efficiency within the wireless sensor networks.

Security in CASER Protocol: In random walking parameter, CASER protocol sends the messages with secure. Once sender node sends the info to sink node, throughout transmission range of attacks are might occurred. So, during this protocol we tend to implemented Random walking strategy. To supply the safety we tend to choose the random walk routing strategy. It not only provides the safety to the node however additionally it managed the energy levels.

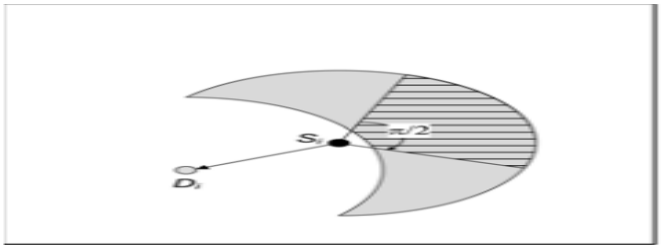

Fig-3: Random Walking

In random walk routing strategy, after we send the data through the shortest path it will not shows the sender node to protect the node details and corresponding data from the hackers. It simply hides the particular sender node details and it displays the closest node of the sender node as a sender node. By implementing likewise, there is no possibility to the aggressor to get the sender node details. If we tend to observe in figure3, the particular sender node is going to be set in shaded space and nearest node displayed as sender node. Here, supported node distance we are able to estimate that node is nearest to the sender node. Like this we are able to forward the messages from sender node to the sink node. During this paper, initial we tend to management the energy levels of the sensor nodes. After we are managed the sensor nodes energy levels within the network, then automatically, we tend to optimize the network lifespan. If network lifetime is increased, then we are able to increase the high message delivery ratio within the wireless sensor networks. Through the random walk strategy we can achieve the security side additionally at a time within the routing.

5. CONCLUSION

We conclude that in this paper, we tend to present a secure and efficient Cost-Aware Secure Routing (CASER) protocol for wireless sensor networks. By using this protocol we will balance the energy consumption and reduce network lifetime improvement. Cost-Aware Secure Routing protocol has the flexibility to support multiple routing schemes in message forwarding to support network lifetime whereas improving routing security.

REFERENCES

[1] Di Tang, Tongtong Li, Jian Ren, "Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.

[2] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Trans. Parallel

Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul. 2012.

[3] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

[4] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY, USA, 2000, pp. 243–254.

[5] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 120–130.

[6] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., 2001, pp. 70–84.

[7] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energyaware routing: A recursive data dissemination protocol for wireless sensor networks," Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech. Rep., May 2001.

[8] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," Comput. Sci. Dept., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00- 729, Apr. 2000.

[9] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic finegrained localization in ad-hoc networks of sensors," in Proc. 7th ACM Annu. Int. Conf. Mobile Comput. Netw., Jul. 2001, pp. 166–179.

[10] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., 1999, pp. 48–55.

[11] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," in Proc. 3rd ACM Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., Seattle, WA, USA, Aug. 1999, pp. 48–55.

[12] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2004, vol. 3, pp. 1705–1716.

[13] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582–595, Apr. 2010.

[14] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf., Mar. 17–21, 2002, vol. 1, pp. 350–355.