ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

An Efficient Wireless Communication through Geography Based Routing (GBR) Protocol in Wireless Sensor Networks

Ashfaq Ahmed[1], Abdul Wasay Mudasser[2]

M.Tech Student (Wireless Mobile Communications), Dept. of E.C.E, Lords Institute of Engineering and Technology Hyderabad, Telangana, India.[1]

Associate Professor, Dept. of E.C.E., Lords Institute of Engineering and Technology Hyderabad, Telangana, India.[2]

ABSTRACT: Unlimited Activation process and vulnerability are the two combating scenarios for several leap wireless sensor networks (WSNs) with non-charging power assets [5]. In this paper, we first propose an innovative geography based routing (GBR) protocol to address these two combating scenarios through two adaptable criterion: symmetric power regulation (SPR) and presumptive-based casual routing [1][2]. We then unearth that the power utilization is intensely unsymmetrical to the homogeneous power distribution strategy to activate unlimited communication path for information transmission rate under the similar power assets and protection requirement [15][9]. To solve this problem, we propose an efficient un-symmetric power distribution strategy to activate unlimited communication path for information transfer rate under the similar power assets and protection requirement [4][5]. Our idealised analysis and Network Simulator (NS2) simulation results demonstrate that the designed GBR protocol can provide an excellent deal between power symmetry and routing efficiency, and can significantly activate the life of the sensor networks for a longer period of time in all scenarios[6][7]. For an unsymmetrical power distribution,our study demonstrates that we can increment the life of sensor networks and the total sum of information bits that can be transmitted by more than the times under the similar hypothesis[25]. We also established that the suggested geography based routing (GBR) can also acquire more information transmission bit rate while prohibiting routing vestiginal assaults [18][19].

KEYWORDS: protection, power symmetry, power, transmission rate, implement, routing, simulation.

I. INTRODUCTION

The modern hi-tech methods forge wireless sensor networks (WSNs) technically and efficiently profitable to be generally benefited for the purpose in both combatant and non-combatant employment, such as tracking of surrounded circumstances akin to the relevant context, prized collection and crucial frameworks[10]. A decisive character of such a structure is that every chain will have a large number of unreleased and neglected sensor nodes[8][14]. These nodes often have very finite and non-chargeable power assets, which makes power a very significant architectural concern for these convolutions [6][7]. Routing is another very challenging design issue for WSNs[11][13]. A properly designed routing protocol should not only ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime[1][5]. In addition to the aforementioned issues, WSNs rely on wire-less communications, which is by nature a broadcast medium [2].

It is highly unsecure to adversial assaults than its cabled supplement due to the deprivation of solid frames[1]. In general, there is a maximum probability in wireless sensor realm, to have an adapted wireless receiver that can track and cut-off the sensor topological transmissions [10][19]. The rival may use sky-high transceivers, dominant modules and intervene with the network from a far-off place since they are not regulated to using sensor network hardware [10][9]. It is possible for the foes to implement obstructions and routing vestiginal assaults [10]. Encouraged by the evidence that WSNs routing is often geography-based, we propose a geography-based secure and efficient (GBR) protocol for WSNs without depending on inundations [8][10]. GBR protocol provides transmissions using two routing techniques, probabilistic walking and shortest path routing, in the same network. The distribution of these two

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

strategies is determined by the specific security requirements [1][12]. This scenario is analogous to delivering US Mail through USPS: express mails cost more than regular mails; however, mails can be delivered faster [1][2]. The protocol also provides a protective transmission rate to choice to increase the transmission bit rate under adversial attacks [9]. In addition, we also give quantitative secure analysis on the proposed routing protocol based on the criteria proposed in [1]. GBR protocol has two major advantages: (i) It certifies balanced power utilization of the total topology of sensors so that the unlimited activation of the WSNs can be increased. (ii) GBR protocol ensures varying routing techniques based on the routing necessities, in conjunction with rapid/sluggish transmission rate. And protected transmission rate to prohibit routing vestigial assaults and environs influx obstruction assaults in WSNs[15][20]. Our contributions of this paper can be summarized as follows:

1) We propose geography based routing (GBR) protocol for WSNs. In this protocol, geographic based routing strategies can be applied to address the message delivery requirements.

2) We devise a quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are maximized under the same energy deployment.
3) We develop theoretical formulas to estimate the number of routing hops in GBR under varying routing energy balance control and security requirements.
4) We quantitatively analyse security of the proposed routing algorithm.
5) We provide a non-uniform energy deployment strategy for the given sensor networks based on energy consumption ratio our theoretical and simulation results both show that under the same total energy deployment, we can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario.

II. RELATED WORK

Routing is a challenging task in WSNs due to the limited resources. Geographic routing has been widely viewed as one of the most promising approaches for WSNs. Geographic routing protocols utilize the geographic location information to route data packets hop-by-hop from the source to the destination [2]. The source chooses the immediate neighbouring node to forward the message based on either the direction or the distance [3]–[5]. The distance between the neighbouring nodes can be estimated or acquired by signal strengths or using GPS equipments [6], [7]. The relative location information of neighbour nodes can be exchanged between neighbouring nodes for this we used average residual battery level of the entire network and it was calculated by adding two fields to the RREQ packet header of a on-demand routing algorithm i) average residual battery energy of the nodes on the path ii) number of hops that the RREQ packet has passed through.According to their equation retransmission time is proportional to residual battery energy[11]. Those nodes having more battery energy than the average energy will be selected because its retransmission time will be less. Small hop count is selected at the stage when most of the nodes have same retransmission time. Individual battery power of a node is considered as a metric to prolong the network lifetime[9]. We have improved the protocol by implementing a balanced energy consumption idea into route discovery process. RREQ message will be forwarded when the nodes have sufficient amount of energy to transmit the message otherwise message will be dropped.

This condition will be checked with threshold value which is dynamically changing. It allows a node with over used battery to refuse to route the traffic in order to prolong the network life. Inthis we havemodified the route table of sensor node adding power factor field[13][20]. Only active nodes can take part in rout selection and remaining nodes can be idle. The lifetime of a node is calculated and transmitted along with Hello packets. Route discovery has been done in the same way as being done in on-demand routing algorithms. After packet has been reached to the destination, destination will wait for time and collects all the packets [14][15]. After time it calls the random number to select the path and send RREP. Random number uses the individual node's battery energy; if node is having low energy level then random number will not use that node.In [4], a geographic adaptive fidelity (GAF) routing scheme was proposed for sensor networks equipped with low power GPS receivers. In GAF, the network area is divided into fixed size virtual grids. In each grid, only one node is selected as the active node, while the others will sleep for a period to save energy. The sensor forwards the messages based on greedy geographic routing strategy. A query based geographic and energy aware routing (GEAR) was proposed in [6]. In GEAR, the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighbouring nodes based on

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

estimated cost and learning cost. The estimated cost considers both the distance to the destination and the remaining energy of the sensor nodes. While the learning cost provides the updating information to deal with the local minimum problem [12][19].

III. MODELS AND ASSUMPTIONS

A. *THE SYSTEM MODEL*

We assume that the WSNs are composed of a large number of sensor nodes and a sink node [1]. The sensor nodes arerandomly deployed throughout the sensor domain[13][14]. Each sensor node has a very limited and non-replenishable energy resource [15]. The sink node is the only destination for all sensor nodes to send messages to through a multi-hop routing strategy [23][25]. The information of the sink node is made public [1][2]. For security purposes, each message may also be assigned a node ID corresponding to the location where this message is initiated [5]. To prevent adversaries from recovering the source location from the node ID, a dynamic ID can be used [20]. The content of each message can also be encrypted using the secret key shared between the node/grid and the sink node [10][11].

B. *DESIGN GOALS*

Our design goal can be summarized as follows:

- To maximize the sensor network lifetime, 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 when an alternative routing path exists.
- The adversaries should not be able to get the source location information by analysing the traffic pattern.
- The adversaries should not be able to get the source location information if he is only able to monitor a certain area of the WSN and compromise a few sensor nodes.
- Only the sink node is able to identify the source location through the message received. The recovery of the source location from the received message should be very efficient.
- The routing protocol should maximize the probability that the message is being delivered to the sink node when adversaries are only able to jam a few sensor nodes.

C. *OVERVIEW OF THE PROPOSED SCHEME*

In our scheme, the network is evenly divided into small grids[12]. Each grid has a relative location based on the grid information [10][11]. The node in each grid with the highest energy level is selected as the head node for message forwarding [20]. In addition, each node in the grid will maintain its own attributes [7][8], including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighbouring grids. The information maintained by each sensor node will be updated periodically.

IV. THE PROPOSED GBR ROUTING PROTOCOL

.We now describe the proposed GBR protocol. Under the GBR protocol, routing decisions can vary to emphasize different routing strategies. In this paper, we will focus on two routing strategies for message forwarding[1][11]: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention. As described before, we are interested in routing schemes that can balance energy consumption [1][2].

A. *ASSUMPTIONS AND ENERGY BALANCE ROUTING*

In the GBR protocol, we assume that each node maintains its relative location and the remaining energy levels of its immediate adjacent neighbouringgrids [1][2]. For node A , denote the set of its immediate adjacent neighbouring grids as N_A and the remaining energy of grid i as εri, $i \in N_A$. With this information, the node A can compute the average remaining energy of the grids in N_A :

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

$$\mathcal{E}_a(A) = \frac{1}{|N_A|} \sum_{i \in N_A} \mathcal{E}r_i.$$

In the multi-hop routing protocol, node A selects its next hop grid only from the set N_A according to the predetermined routing strategy [12][17]. To achieve energy balance among all the grids in the sensor network, we carefully monitor and control the energy consumption for the nodes with relatively low energy levels by configuring A to only select the grids with relatively higher remaining energy levels for message forwarding[5][6].

For this purpose, we introduce a parameter 2 [0, 1] to enforce the degree of the energy balance control (EBC). We define the candidate set for the next hop node as $N_A^\alpha = \{i \in N_A \mid \varepsilon ri. \geq \alpha\ \varepsilon\alpha(A)|\}$ based on the EBC α. It can be easily seen that a larger α corresponds to a better EBC. It is also clear that increasing of α may also increase the routing length [1][12]. However, it can effectively control energy consumption from the nodes with energy levels lower than εα(*A*)[7][8].We summarize the GBR routing protocol in Algorithm [1][2]. It should be pointed out that the EBC parameter α can be configured in the message level, or in the node level based on the application scenario and the preference [19][23]. When α increases from 0 to 1, more and more sensor nodes with relatively low energy levels will be excluded from the active routing selection. Therefore, the N_A^α shrinks as αincrease. In other words, as increases, the routing flexibility may reduce[1][2]. As a result, the overall routing hops may increase. But since εα (*A*) is defined as the average energy level of the nodes in N_A, this subset is dynamic and will never be empty [20]. Therefore, the next hop grid can always be selected from N_A.

B. SECURE ROUTING STRATEGY

In the previous section, we only described the shortest path routing grid selection strategy. However, in GBR protocol, we can support other routing strategies.

In this section, we propose a routing strategy that can provide routing path un-predictability and security [12][17]. The routing protocol contains two options for message forwarding: one is a deterministic shortest path routing grid selection algorithm, and the other is a secure routing grid selection algorithm through random walking.

V. SECURITY ANALYSIS

In GBR, the next hop grid is selected based on one of the two routing strategies: shortest path routing or random walking [1][14]. The selection of these two routing strategies is probabilistically controlled by the security level β[17][18]. The security level of each message can be determined by the message source according to the message priority or delivery preference [5]. As β increases, the routing path becomes more random, unpredictable, robust to hostile detection, interception and interference attacks [6][7].While random walking can provide good routing path un-predictability, it has poor routing performance [1][5]. GBR provides an excellent balance between routing security and efficiency [10].

A. QUANTITATIVE SECURITY ANALYSIS OF GBR

In [1], we introduced criteria to quantitatively measure source-location privacy for WSNs.

Definition 1([1] Source-location Disclosure Index (SDI)).SDI measures, from an information entropy point of view, the amount of source-location information that one message can leak to the adversaries.For a routing scheme, to achieve good source- location privacy, SDI value for the scheme should be as closeto zero possible.

B. DYNAMIC ROUTING AND JAMMING ATTACKS

For security level β , the distribution between random walking and the shortest path routing for the next routing hop is β and $1 - \beta$. β can vary for each message from the same source. In this way, the routing path becomes dynamic and unpredictable [21][24]. In addition, when an adversary receives a message, he is, at most based on our assumption, able to trace back to the immediate source node that the message was transmitted [20][21]. Since the message can be sent to the previous node by either of the routing strategies, it is infeasible for the adversary to determine the routing strategy and find out the previous nodes in the routing path [22]. Fig. 1 gives the routing path distribution for four

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

different security levels using NS2. The messages are transmitted from a single source located at (332, 259) to the fixed sink node located at (1250, 1250)[12][17]. The source node and the destination node are 10 hops away in direct distance. In the figures, each line represents a routing path used by at least one message [25]. This figure demonstrates that the routing path distribution width increases with the energy balance control α and the security parameter β [5]. In fact, if we assume that the minimum number of hops between the source node and the sink node is h for β = 0, then for β > 0, the total number of random walking is about $\frac{h\beta}{1-\beta}$hops [6]. The routing path can be spread largely in the area of width $\frac{h\beta}{1-\beta}$ centered around the path for security level β = 0[9][10]. Therefore, for a larger security level, more effort is required to intercept a message since it triggers more random walking, which will create a wider routing path distribution and a higher routing robustness under hostile attacks[1][12]. As a result, the adversary has to monitor a larger area in order to intercept/jam a message [23]. As an example, when β = 0.5, the width of the routing path is about the same as the length of the routing path, as shown in Fig. 1(d).

C. ENERGY LEVEL AND COMPROMISED NODE DETECTION

Since we assume that each node has knowledge of energy levels of its adjacent neighbouring grids, each sensor node can update the energy levels based on the detected energy usage[13][14]. The actual energy is updated periodically. For WSNs with non-replenishable energy resources, the energy level is a monotonically decreasing function [12][17]. The updated energy level should never be higher than the predicated energy level since the predicted energy level is calculated based on only the actually detected usage. If the updated energy level is higher than the predicted level, the node must have been compromised and should be excluded from its list of the adjacent neighbouringgrids [1][2]. We also compared the GBR algorithm with the RSIN algorithm in on path distribution under the similar energy consumption [15][17]. The results show that the GBR can achieve better and more uniform path distribution, as shown in Fig. 2.

VI. PROPOSED ALGORITHMS

Algorithm 1 : Node A finds the next hop routing grid based on the EBC α∈ [0, 1].
1: Compute the average remaining energy of the adjacent neighbouring grids :

$$\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|} \sum_{i \in \mathcal{N}_A} \mathcal{E}r_i.$$

2: Determine the candidate grids for the next routing hop :

$$\mathcal{N}_A^{\alpha} = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha \bar{\mathcal{E}}_a(A)\}.$$

3:Send the message to the grid in the N_A that is closest to the sink node based on its relative location.

Algorithm 2 Node A finds the next hop routing grid based on the given parameters α ,β ∈ [0, 1].
1: Compute the average remaining energy of the adjacent neighbouring grids :

$$\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|} \sum_{i \in \mathcal{N}_A} \mathcal{E}r_i.$$

2: Determine the candidate grids for the next routing hop :

$$\mathcal{N}_A^{\alpha} = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha \bar{\mathcal{E}}_a(A)\}.$$

3: Select a random number γ ∈ [0, 1].
4: if γ > β then
5: Send the message to the grid in the $\mathcal{N}_A^{\alpha}$ that is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Closest to the sink node based on its relative location.
6: else
7:Route the message to a randomly selected grid in the set
$\mathcal{N}_A^{\alpha}$

8: end if

Algorithm 3 Node A finds the next hop routing grid based on the given parameters α,β ∈ [0, 1]
1: Compute the average remaining energy of the adjacent neighbouring grids :

2: Determine the candidate grids for the next routing hop :

$$\mathcal{N}_A^{\alpha} = \{i \in \mathcal{N}_A \mid \mathcal{E}r_i \geq \alpha \bar{\mathcal{E}}_a(A)\}.$$

3: Select a random number γ ∈ [0, 1].

4: if γ > β then

5: Send the message to the grid in the $\mathcal{N}_A^{\alpha}$ that is closest to the sink node based on its relative location.

6: else

7:Route the message to a randomly selected grid in the set
$\mathcal{N}_A^{\alpha}$

8: end if.

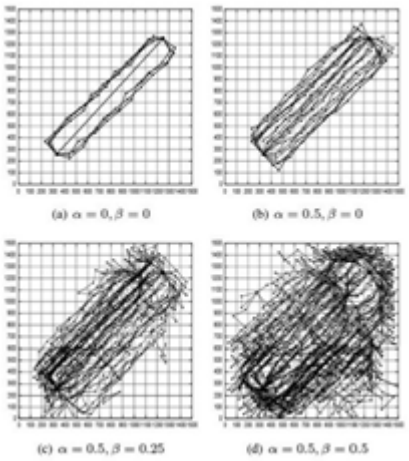

Fig.1. Routing path distribution statistics for various balance energy Controland security parameters β. In all simulations, the target area is 1500x1500.The source node is located at (332,259) and sink is located at (1250,1250).

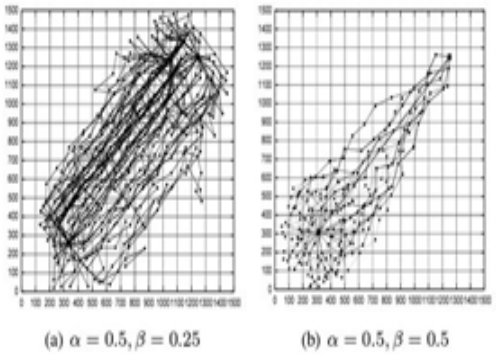

Fig. 2. Routing path distribution statistics for energy balance control α = 0.5 and security parameters β = 0.25 and RSIN in[20] with Parameters $d_{min = 100,}$ α = 3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

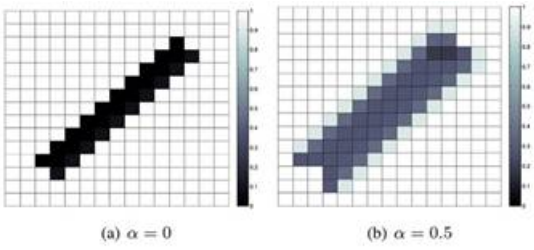

Fig. 3. Remaining energy distribution statistics after the source transmitted about 600 messages.

VII. PERFORMANCE EVALUATION AND SIMULATION RESULTS

In this section, we will analyse the routing performance of the proposed GBR protocol from four different areas: routing path length, energy balance, the number of messages that can be delivered and the delivery ratio under the same energy consumption. Our simulations were conducted in a targeted sensor area of size 1500 × 1500 meters divided into grids Of 15 × 15.

A. ROUTING EFFICIENCY AND DELAY

For routing efficiency, we conduct simulations of the pro-posed GBR protocol using NS2 to measure the average number of routing hops for four different security levels. We randomly deployed 1000 sensor nodes in the entire sensor domain. We also assume that the source node and destination node are 10 hops away in direct distance. The routing hops increase as the number of transmitted messages increase. The routing hops also increase with the security levels.

B. ENERGY BALANCE

The GBR algorithm is designed to balance the overall sensor network energy consumption in all grids by controlling energy spending from sensor nodes with low energy levels. In this way, we can extend the lifetime of the sensor networks. Through the EBC α, energy consumption from the sensor nodes with relatively lower energy levels can be regulated and controlled. Therefore, we can effectively prevent any major sections of the sensor domain from completely running out of energy and becoming unavailable.In our simulations, shown in fig .3, the message source is located at (332, 259) and the message destination is located at (1250, 1250). The source node and the destination node are 10 hops away in direct distance. There are three nodes in each grid, and each node is deployed with energy to transmit 70 messages. We show the remaining energy levels of the sensor nodes under two different α levels. The darker gray-scale level corresponds to a lower remaining level. Fig. 3(a), we set $\alpha = 0$ and there is only one source node. The energy consumption is concentrated around the shortest routing path and moves away only until energy runs out in that area. In Fig. 3(b), we set$\alpha = 0.5$, then the energy consumption is spread over a large area between this node and the sink. While maximizing the availability of the sensor nodes, or lifetime, this design can also guarantee a high message delivery ratio until the energy runs out for all of the available sensor nodes in the area.

C. TRANSMISSION RATE

One of the major differences between our proposed GBR routing protocol and the existing routing schemes is that we try to avoid having any sensor nodes run out of energy while the energy levels of other sensor nodes in that area are still high.We implement this by enforcing balanced energy consumption for all sensor nodes so that all sensor nodes will run out of energy at about the same time. This design guarantees a high message delivery ratio until energy runs out from all available sensor nodes at about the same time. Then the delivery ratio drops sharply.

VIII. GBR OPTIMAL NON-UNIFORM ENERGYDEPLOYMENT

GBR is designed to balance the energy consumption of sensor nodes and thereby extends the lifetime of the sensor networks. However, the energy consumption is uneven in sensor networks. The energy consumption for the sensor nodes closer to the sink node is much higher than the nodes that are away from the sink node. In fact, the average

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

energy consumption for the node with distance *i* to the sink node can be calculated according to equation. Therefore, the best that we can do is to balance the energy of the grids with the same radius to the sink node.

A. NODE ENERGY DEPLOYMENT

For the optimal energy deployment, the energy allocation of the grids should be proportional to the energy usage. We still assume that the sink node is in the centre of the sensor domain. All sensor nodes transmit messages at the same frequency.

B. ROUTING IN NON-UNIFORM ENERGY DEPLOYMENT

Under the new energy deployment, we have to redefine the way we calculate the average remaining energy of the adjacent neighbouring grids since otherwise, the messages will always be routed to the nodes that are closer to the sink node, at least initially. In this way, the number of possible nodes for the next hop can be greatly limited and security routing may become trivial.

C. SIMULATION RESULTS

We conducted simulations using Network Simulator Ver2 (NS2) to compare the the existing, proposed and enhanced system for Geographic Routing Protocol (GBR) for different values of parameters α,β,γ. In existing system we overcome the problem of source attack, but we don't know about the energy based attack. As the time we send the data in low energy path, so data loss occurs.

Data not send properly to the destination. In a proposed system, we use proactive technique. We can know the status of the nodes at particular interval of time. Here, first of all we identified the energy attack and we remove the energy attack. In Enhancement mode, we mainly overcome the problem of fake energy nodes and focus on saving the energy. Because, we already overcome the problem of energy attack and source attack. For that purpose we use reactive technique, by this single RREQ and RREP messages are sent to choose the best path and send the data in that way. Finally, using comparison mode we analyse the total number of messages that can be delivered in those scenarios using Network Animation Window (NAM).

Our statistics are based on the message delivery ratio that is 95% or above. In uniform energy deployment, when α = 0, the number of messages that can be delivered is 1510. When α = 0.25, the number of messages that can be delivered increases to 1624. The increase is 7.55%. We found that when we further increase α, the number of messages that can be transmitted increases slightly. At this point, all the nodes around the sink have run out of energy and no more messages can be transmitted. And also the graphical analysis using X-Graph for node failure and as well as packets delivery ratio. We also observed that node failure is less when compared to existing system and Packet delivery ratio is more in enhanced system when compared to existing system.

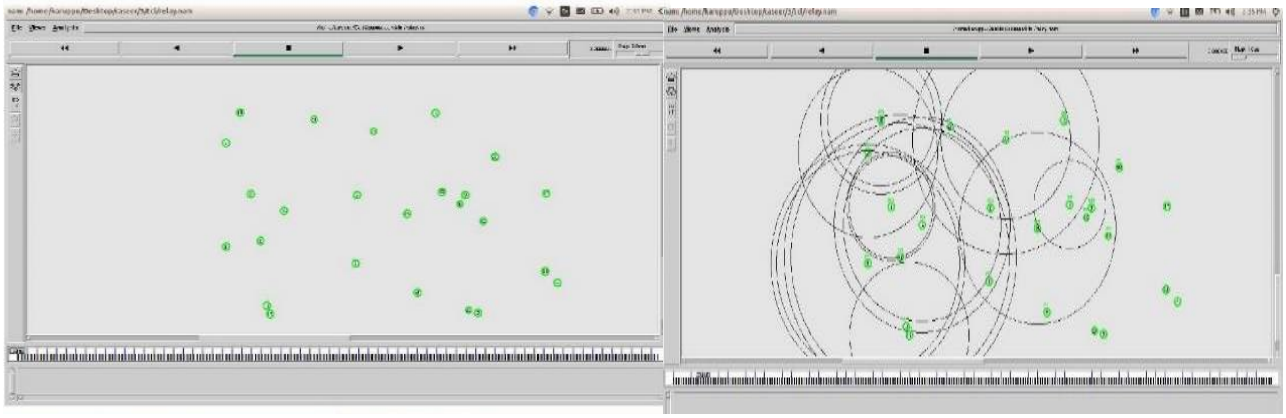

Fig. 4. Sensor Nodes in a Wireless Sensor Network.

Fig. 5. Data Communication using RREQ and RREP through Sensor Nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

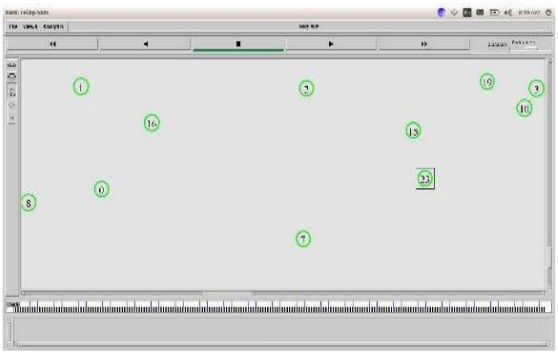

Fig. 6. Adverbial Attack on a Sensor Node.

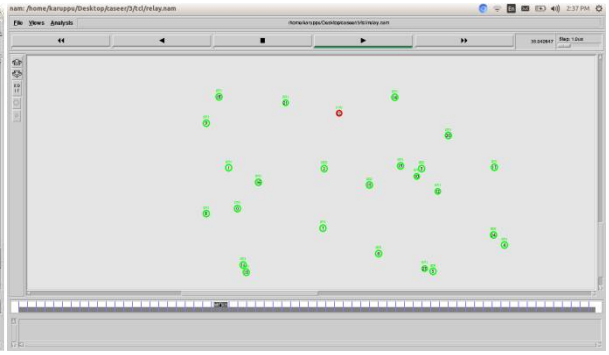

Fig. 7. Knock-Out Node which loses its energy in red colour.

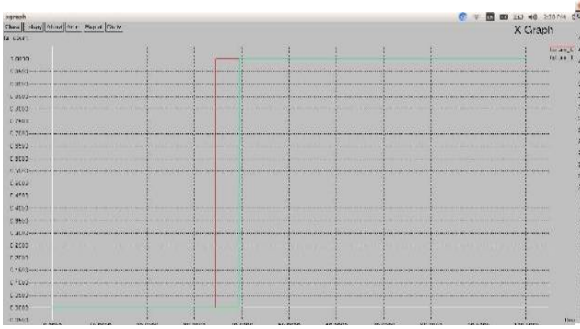

Fig. 8. Node Failure Graph.

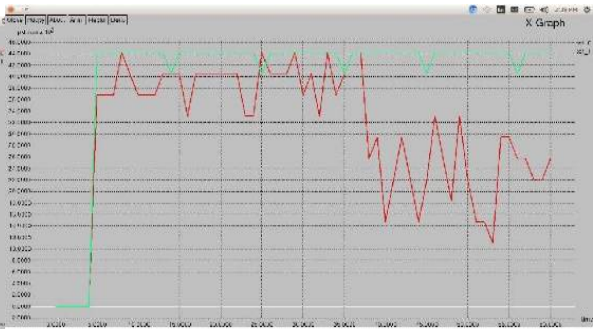

Fig. 9. Packet delivery ratio graph.

IX. CONCLUSION

In this paper, we presented a geography based routing (GBR) protocol for WSNs to balance the power utilization and increases the life of network. GBR 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 GBR has an excellent routing performance in terms of balanced power efficiency and routing path distribution for routing path security. We also proposed a varied power deployment scheme to maximize the life of the sensor network. Our analysis and simulation results show that we can increase the life and the number of data bits that can be transmitted under the varied power distribution by having the probability of more than quad number times.

REFERENCES

1. Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, accepted, to appearVol. 23, No.. 7, July 2012.
2. Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks," in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30, 2012.
3. B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in MobiCom'2000, New York, NY, USA, 2000, pp. 243 – 254.
4. Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001, pp. 70–84.
5. Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor net-works," UCLA Computer Science Department Technical Report, UCLA-CSD, May 2001.
6. N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor local-ization for very small devices," Computer science department, University of Southern California, Tech. Rep. Technical report00-729, April 2000.
7. A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in Proceedings of the Seventh ACM Annual International Conference on Mobile Computing and Networking (MobiCom), July 2001, pp. 166–179.
8. P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaran-teed delivery in adhoc wireless networks," in 3rd Int. Workshopon Dis-crete Algorithms and methods for mobile computing and communications, 1999, pp. 48–55.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

9. "Routing with guaranteed delivery in ad hoc wireless networks," in the 3rd ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL M 99), Seattle, WA, August 1999, pp. 48–55.
10. T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowl-edge for energy efficient geographical routing in sensor networks," in Proc. IEEE INFOCOM, vol. 3, March 2004, pp. 1705 –1716 vol.3.
11. Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," Mobile Computing, IEEE Transactions on, vol. 9, no. 4, pp. 582–595, April 2010.
12. R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE, vol. 1, 17-21 March 2002, pp. 350– 355 vol.1.
13. J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," Networking, IEEE/ACM Transactions on, vol. 12, no. 4, pp. 609–619, August 2004.
14. H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.
15. F. Liu, C.-Y. Tsui, and Y. J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 9, no. 7, pp. 2258–2267, July 2010.
16. C.-C. Hung, K.-J. Lin, C.-C. Hsu, C.-F. Chou, and C.-J. Tu, "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, Aug. 2010, pp. 1–6.
17. C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in SASN. ACM, 2004, pp. 88–93.
18. Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in Proceedings of IEEE SECON 2009, Rome, Italy., June 22-26, 2009.
19. "Source-location privacy through dynamic routing in wireless sensor networks," in Proceedings of IEEE INFOCOM 2010, San Diego, USA., March 15-19, 2010.
20. M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, April 2008, pp. 51 – 55.
21. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," ICDCS, pp. 599–608, June 2005.
22. AlGabri Malek, Chunlin LI, Z. Yang, Naji Hasan.A.H and X.Zhang ,' Improved the Energy of Ad hoc On- Demand Distance Vector Routing Protocol', International Conference on Future Computer Supported Education, Published by Elsevier, IERI, pp. 355-361, 2012.
23. W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," IEEE Network, vol. 20, no. 3, pp. 41–47, 2006.
24. A. Pathan, H.-W. Lee, and C. seon Hong, "Security in wireless sensor networks: issues and challenges," in The 8th International Conference on Advanced Communication Technology (ICACT), vol. 2, 2006, pp. 6 pp.–1048.
25. Shilpa jain and Sourabh jain,'Energy Efficient Maximum Lifetime Ad-Hoc Routing (EEMLAR)', international Journal of Computer Networks and Wireless Communications, Vol.2, Issue 4, pp. 450-455, 2012.

BIOGRAPHY

Ashfaq Ahmed recievedthe B.Tech degree from Shadan College of Engineering and Technology in 2014, and currently pursuing the M.Tech degree in Wireless and Mobile Communications from Lords Institute of Engineering and Technology. His current research interests include wireless sensor net-works and network security.

Abdul Wasay Mudasser Completed B.tech in 2007 & M.tech in 2010 from JNTUH. Having 5years of Teaching and 3years of Industrial Experience. Field of interest is wireless communication, Telecommunication, Computer Networking and Image Processing. Published 7 papers in International Journal, 2 papers in International Conference and 1 paper in National Conference. Presently working asAssociate Professor in Department of Electronics & Communication Engineering at **Lords Institute of Engineering & Technology, Hyderabad, Telangana State, India.**