ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 9882-9887

Secure Geographic Routing Hybrid Approach For Void Resolution In Wireless Sensor Network

Shishir Patra[1] Jajati Mallick[2]
Department of Computer Science and Engineering
Purushottam Institute of Engineering and Technology
Rourkela, Mandiakudar, Odisha, India
shishirpatra9@gmail.com[1]
mallick.jajati@gmail.com[2]

Abstract- In this paper, we propose a new hybrid approach between the geographic greedy mode and the recovery mode in order to improve routing efficiency in number of hops, without network overhead. It exploits the optimal topological route to base stations, obtained by beacon messages, as a resource to find better routes than the ones created by greedy mode and recovery mode. We show by simulations that the proposed hybrid approach leads to a significant improvement of routing performance when applied to combined greedy and recovery routing algorithms.

Keywords- Geographic routing, CDF, GPSR SGR, CTR

I. INTRODUCTION

The geographic greedy mode and the recovery mode in order to improve routing efficient in number of hops, without overhead; it exploits the optimal topological route to base station, obtained by beacon message, as a resource to find better routes than the ones created by face routing[1]. "Yi-hua Zhu*, wan-deng wu, jian pan, Yi-ping Tang"[2] have proposed which is able to dramatically prolong network lifetime while efficient expending energy. In the ERAPL, a data gathering sequence (DGS), used to avoid mutual transmission and loop transmission among nodes, is constructed, and each node proportionally transmit traffic to the links confined in the DGS. In addition, a mathematical programming model, in which minimal remaining energy of nodes and total energy consumption are included, is presented to optimize network lifetime. Moreover, genetic algorithms are used to find the optimal solution of the propose programming problems. Further. Simulation experiments are conducted to compared the ERAPL, with some well-known routing algorithms and simulation result show the ERAPL, outperforms then in term of network lifetime.

"Gyanendra Prasad joshi and sung won kim"[3] have proposed a void avoidance algorithm(VAA), a novel idea based on upgrading virtual distance. VAA allow wireless sensore nodes to remove all the tacks by transforming routing graph and forwarding packet using on it greedy routing. In VAA, the stack node upgrades distance unless find a next hop node that close to destination than it is. VAA guarantees packet delivery if there is a topology valid path. "Ivan strojmenovic, mark russel and bosko vukojevic" [4] have proposed the first localized QoS routing algoritms for wireless network. It perform network. It perform DFS routing algorithms after adages with insufficient bandwidths or insufficient connection time are deleted from graph, and attempts to minimize hop count . This is also the first paper to apply GPS in QoS routing decision, and to consider the connection time (estimated lifetime of a link) as a QoS criterion. The average length of measured QoS path our experiments, obtained by DFS method, was between 1 and 1.34 times longer than the length of QoS path obtained by shortest path algorithms . The overhead is considerably reduced by applying the concept of internal nodes. "Sudar subamanian, sanjay shakkottai and piyush gupta"[5] have proposed a randomized geographic routing scheme that can achieve a throughput capacity of (within a poly-logarithmic factor) even in network with in routing holes. "Aissani, M., Mellouk, A., Badache, N., Djebbar, M.," [6] have proposed novel routing mechanism to makes data packet avoid meeting voids in advance. After discovering boundary nodes of a void, . A sender node inside announce area. At n-hops far from the boundary nodes, uses this information to obtain the appropriate forwarding region and starts counting the void in advance. For that, the sender node selects its forwarding candidate neighbor according to its obtained forwarding region. The proposed mechanism is fairly simple to implement and saves sensor network resources. "Abidalrahuman moh'da, Hosein Marzib, Nauman Aslama, William Phillipsa, William Robertsona, a*" [7] have proposed the security holes in current WSNs platform, and compare the main approaches to implemented the cryptographic primitives used to provide security service for these platform, in term of security, energy, and time efficiency. The choice of cryptographic primitives for suggest platform is based on their compatibility with the constrained nature of WSNs and there secure status. "William R.claycomb, DongwanShin" [8] have proposed to protect wireless sensor network based on security policy, enforced at the node level. This policy is based on new approach to key establishment, which combines a group-based distribution model and identity-based cryptography. Using the solution enable node to authenticate each other, and provide them with structure to build secure communication between one another, and between various

groups. Using the key establishment protocol and security policy, how to reduce or prevent significant attack on wireless sensor network. "Necla Bandirmali a, Ismail Erturk b" [9] have proposed on increase security for the WSNs employed in especially military and health areas recently receives a remarkable attention as primary focused on in this presented work. The WSN sec smoothly combines the advantageous Aspect of the scalable encryption algorithms (SEA) with the counter mode (CTR) and cipher block chaining-message authentication code (CBC-MAC) approach. It provides not only high data confidentiality but also message authentication and integrity functions. The WSN sec security level can be boosted dynamically if required. It has been shown that using the proposed WSN sec with the 192-bit data block/key has a trivial increase on the memory usage and energy consumption while providing an extremely high level of security compared to the traditional tiny SEC. in addition, modeling and simulation of a WSN employing the proposed WSN sec have been realized using the OPNET modeler software. The simulation result reveal that the ratio of the delay resulted from the particular of both WSN sec and tiny SEC to the total end to end delay converge at 13% for increase the network load. Therefore the WSN sec provides a better delay performance in highly scalable application.

II. SYSTEM ARCHITECTURE

Geographic routing algorithms use node position information to forward a message to its destination. Such algorithm use small (constant-size) per-node state and scale very well for point-to-point communication in wireless networks .Geographic routing algorithm use greedy routing where possible. In greedy routing, each message is stamped with the coordinates of its destination, all nodes know their own coordinates, and a node forwards the message to the neighbor that is geographically closest to the destination. Local minima may exist where no neighbor is closer to the destination. In such cases, greedy forwarding fails and another backup strategy must be used to continue making progress toward the destination.

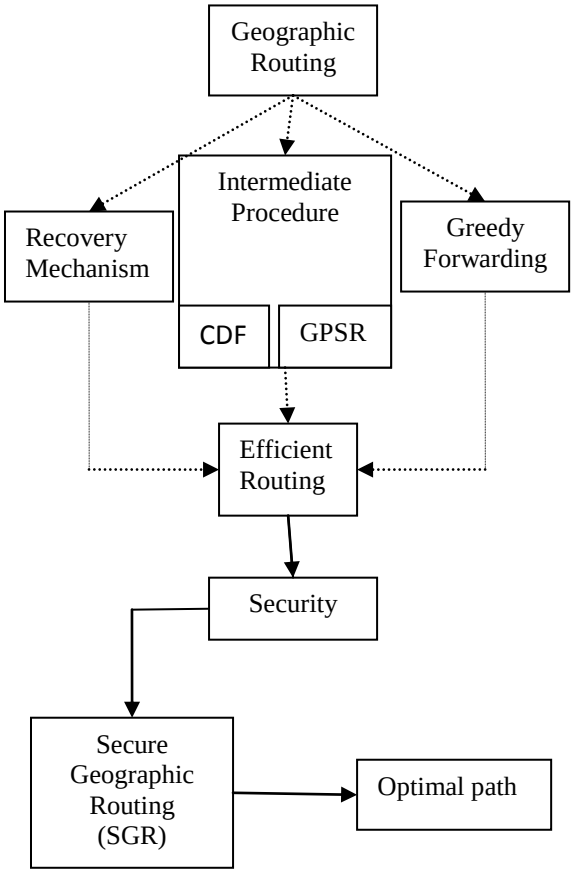

Figure -1 System Architecture

The early proposals for geographic routing did not have any such backup strategy, and therefore could not guarantee message delivery. The first geographic routing algorithm to provide guaranteed delivery in any connected network was face routing. It uses geometric rules to route around voids near local minima. Face routing and its variants require that the network graph is first converted to a planar graph by using a suitable planarization algorithm or that problematic cross links are removed from the network as needed. Recently proposed hull routing does not require the network graph to be planar; it uses predefined spanning trees to route messages when they end up at local minima. Opportunistic routing protocols extend geographic routing by dynamically choosing the forwarding node based on the best node that heard the transmitted message. These protocols typically consider link uncertainty, and adapt routing accordingly. Hence geographic routing points these two issues: Routing packet successfully given any topology and acquiring location information of nodes reflecting the given topology. Geographic routing based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. The idea of using position information for routing was first proposed in the 1980s in the area of packet radio networks and interconnection networks. Geographic routing requires that each node can determine its own location and that the source is aware of the location of the destination. Advantages of greedy forwarding: Greedy forwarding's great advantage is its reliance only on knowledge of the forwarding node's immediate neighbors. The state required is negligible and dependent on the density of nodes in the wireless network not the total number of destinations in the network. On networks where multi hop routing is useful, the number of neighbors with in a node's radio range must be substantially

less than the total number of nodes in the network. As the density in space of the nodes deployed on a wireless network increases, greedy forwarding approximates shortest paths progressively more closely; the shortest path between two nodes tends toward the Euclidean straight line between them, as the minimum possible number of hopes is bounded below by the number of radio ranges between source and destination, laid end to end. Traditional shortest path routing algorithm cannot exploit structure in IP addresses to make forwarding decisions; they must treat IP addresses as flat identifiers, and resort to a table lookup among all destinations in the routing domain. It is the self describing nature of geographies coordinates that allows forwarding routers to interpret the destination location in a packet to make a purely local forwarding decision. The scalability and data concentric attributes of geographic routing make it a feasible routing alternative in WSNs. Its capability assumes, however, that the geographic locations of all neighboring nodes, or at least a subset thereof, are known to the message holder. Accurate information about the geographic location of nodes is typically available from a global positioning system (GPS) device. It is possible that in certain settings, sensing node may be equipped with GPS device. In most cases, however, the resource and energy limitation of sensor nodes prohibits the use of GPS device. Nodes without GPS devices can use a variety of triangularization algorithms to determine their location and the location of their neighboring nodes.

A. GREEDY FORWARDING

Greedy forwarding tries to bring the message closer to the destination in is step using only local information. Thus, each node forwards the message to the neighbor that is most suitable from a local point of view. The most suitable neighbor can be the one who minimizes the distance to the destination in each step. A greedy algorithm is an algorithm that follows the problem solving heuristics of making the locally optimal choice at each stage with the hope of finding a global optimum. On some problems, a greedy strategy need not produce an optimal solution, but nonetheless greedy heuristic may yield locally optimal solutions that approximate a global optimal solution.

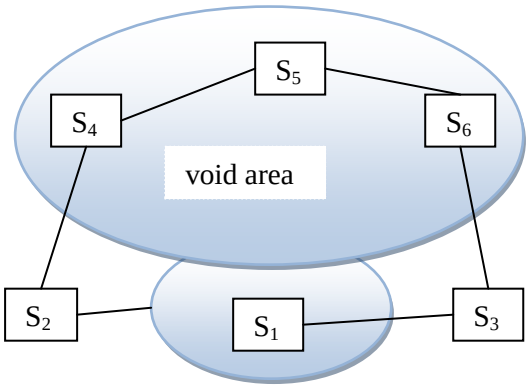

Figure-2 Greedy algorithm forward progress failure

For example, a greedy strategy for the travel salesman problem is the following heuristic:" At each stage visit an unvisited city nearest to the current city". This heuristic need not find a best solution but terminates in a reasonable number of steps, finding an optimal solution typically requires unreasonably many steps. In mathematical optimization, greedy algorithms solve combinational problems having the properties of closed sets. For many other problems, greedy algorithms fail to the optimal solution, and may even produce the unique worst possible solution. One example is the travelling salesmen problem, for each number of cities there is an assignment of distances between the cities for which the nearest neighbor heuristic produces the unique worst possible tour. The Greedy approach to geographical routine may either fail to find a path, even when one exists, or produce insufficient routes. For this problem consider the figure-2, where node S1 needs to forward a packet to the destination D. based on the Greedy approach, S1 must select the closet neighbor to the destination as the next hop to forward the packet. However, node S2 & S3, are both farther away from the destination than is node S1. The Greedy approach trapped in a local minimum and fails to make forward progress. Geometric techniques exploit the geometric properties of voids by considering its topological structures. It is mainly applied to improve both nodes in geographic routing. In this technique the boundary through which the packets are to be routed are mentioned by considering their topological structure. Lemon ET.AI proposed a geographic routing called boundary state routing [BSR] which improves greedy forwarding mode through a strategy called greedy bounded compass. In this strategy, the packets to be forwarded dare routed around concave boundaries by using the boundary state information proposed from boundary mapping protocol [BMP]. Here the path completion rate improvement becomes negligible in denser networks, with connectivity equal or greater than 5.0. practically, it has been demonstrate that an improved path completion rate of up to 45.7% in sparse network is commonly used in greedy forwarding strategy. However, bound whole approach is used in geometric approach to traverse a void through boundary similar to that of perimeter routing in planar graph. Bound hole present an algorithm to discover the hole-surrounding path of voids. However, bound hole cannot deliver the packet when the destination is within the hole.

B. SECURITY

There are three security goals and they are Confidentially, Integrity, & Availability. Any organization needs to protect the confidential information and process is known as confidentially. The industries confidential data should be protected from the rivals. The confidentiality does not mean that not only store the data in secure manner but also at the time of transmission it should be protected from a middleman. Consider an example of bank, in such case when a customer deposits or withdraw the money into or from his or her account, the information should be updated by the authorized person. From this it is conclude that the integrity should be maintained with the data by authorized user in authorized manner**.** Whatever the confidential information stored should available to the authorized user as authorized entity.

C. CHECKING INTEGRITY

To check the integrity of a message or document we run the cryptographic hash function again and compare the new message digest with the previous one. If both are same we are sure that the original message has not been changed. The whole process is shown in Figure- 3. The message digest guaranteed the integrity of a message; however it does not

authenticate the sender of the message. To provide the message authentication, sender needs to provide a proof that it has send the message not by imposter. The digest created by a cryptographic hash function is normally known as modification detection code (MDC) .This code can detect any modification in the message. The message authentication means data origin authentication is the message authentication code (MAC).

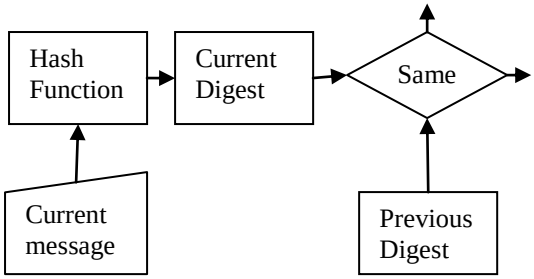

Figure-3 Checking Integrity

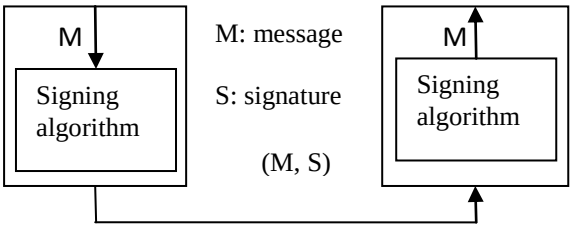

Figure-4 Digital Signature Process

Consider an example of check facility in the banking system. At the time of submitting the check in the counter, the bank employee with check the signature which is already with the bank, if it match with the current signature which is on the check then it is authenticate else false. That means the signature which stored in the bank is in the form of electronic format. So the electronic signature is known as digital signature. A Digital Signature needs a public key system. The signer signs with her private key. The verifier verifies with the signer's public key.

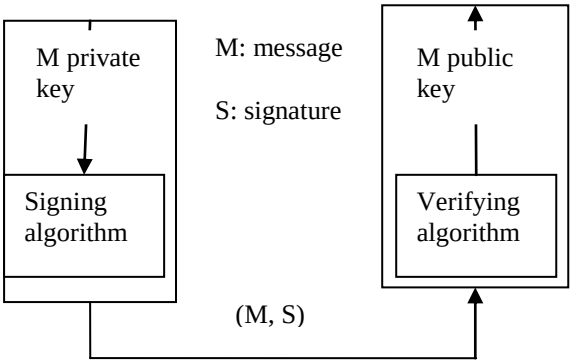

Figure- 5 Adding Key to the Digital Signature Process

III. ENERGY CONSUMPTION STATES

The network interface has four possible energy consumption states: transmit and receive are for transmitting and receiving data. In the idle mode, the interface can transmit or receive. This is the default mode for ad hoc environment. The sleep mode has extremely low power consumption. The interface can neither transmit nor receive until it is woken up. A base station moderates communication among mobile nodes, scheduling and buffering traffic so that the mobiles can spend most of their time in the sleep state. In an ad hoc environment, there are no base stations and nodes cannot predict when they will receive traffic. Therefore, the default state in an ad hoc network is the idle state, rather than the sleep state. The model computes energy relative to the idle state. As there is currently little work in the area of energy management for ad hoc networks, the model does not provide for arbitrary transition to the sleep state. The model assumes that the same link-layer operation always has the same energy: an assumption that may not be true if, for example, signal strength affects the energy required to receive the data. The energy for a node to send or receive a network-layer packet is modeled linearly as in equation (1). There is a fixed of the packet:

$$Energy = m \times size + b \qquad (1)$$

The total energy of a packet is the sum of the energy incurred by the sending node as in equation (2) and all receivers as in equation (3). The incremental payload energy msend and mrecv are the same for broadcast and point-to-point traffic. For point-to-point traffic, the fixed energy includes both the channel access energy and the MAC negotiation. The channel access energy is assumed to be the same as in the broadcast case. In the IEEE 802.11 MAC protocol, the source sends an RTS (request-to-send) control message, identifying the destination. The destination responds with a CTS (clear-to-send) message. Upon receiving the CTS, the source sends the data and awaits an ACK from the destination. For simplicity, these small control messages are assumed to have the same fixed send (bsendctl) and receive (brecvctl) energy. At the sender:

$$Energy = bsendctl + brecvctl + msend \times size + bsend + brecvctl \qquad (2)$$

At the destination:

$$Energy = brecvctl + bsendctl + mrecv \times size + brecv + bsendctl \qquad (3)$$

In practice, messages may be lost due to collision or other failures and the protocol provides for various MAC layer retransmissions.

IV. RESULTS

The network simulator OMNET 4.1 is used to implement the proposed secure geographic routing.

Parameter	**Value**
Simulation time	10 min
Dimension	1,200m×1,200m
No. of routing element	60
RTE placement	Random
Mobility model	Random waypoint
Min. speed	O m/s
Max. speed	3m/s
Pause time	2m/s

Input/output queue	250 kbyte
N flow	59
CBR data size	512 byte
Communication period	2-7 min
Sending rate	10 packet/s

Table-1 Simulation Parameter

Different types of experiments is conducted to evaluate the performance of a secure geographic routing and to check whether the proposed node selection performance the expected routing operations. Table-1 describes the common settings throughout the entire experiment. Simulated scenarios were designed with various voids and dead ends to verify the efficiency of the routing algorithm on handling the local minima problem. Furthermore, we generated several networks on square fields of side equal to 1000 m by distributing nodes randomly and uniformly according to a Poisson point process. Therefore, we were able to investigate how the proposed algorithm performs on different network topologies. Figure-7 scenario show that there are 2 base station , like rte[1], rte[3] and 5 node are there, to the base station rte[1] packet are transmit from rte[4]-rte[2]-rte[1]. In this transmission packet is generated by rte[4]. Then it transmitted to rte[2] and reaches to the rte[3]; so one base station can also transmit to another base station if it is overloaded.

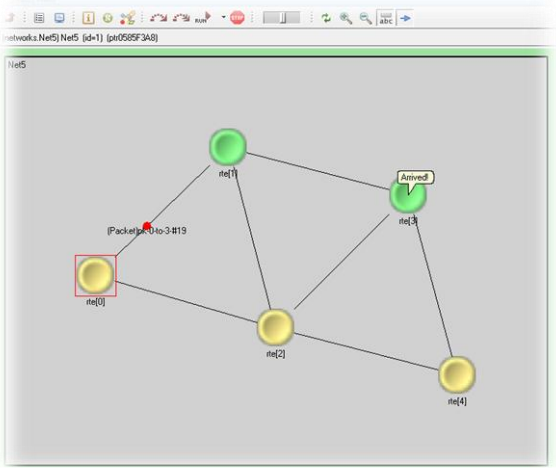

Figure- 7 NAM output during packet transmission with Two Base Stations and 3 Transmitting Stations

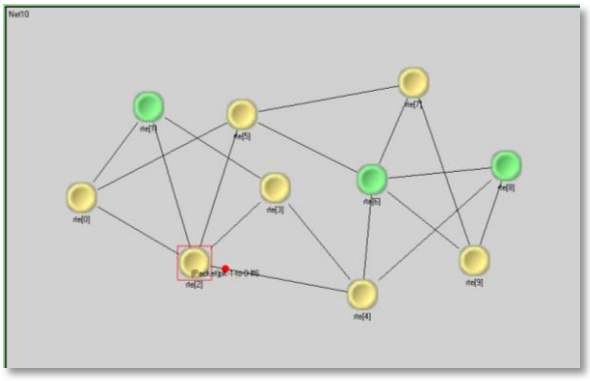

Figure- 8 NAM output during packet transmission with Three Base Stations and 7 no's of Transmitting Stations

Figure- 8 scenario show that there are 3 base station like rte[1], rte[6],[8] and 10 are there. To the base station [1] packet are transmitted from rte[5]-rte[0]-rte[1]. Packet are transmitted from rte[5]-rte[0]-rte[1].in this transmission packet is generated by rte[0] to the base station rte[8], Packet are transmitted from rte[2]-rte[4]-rte[8].in this transmission packet is generated by rte[5]. Similarly to the base station rte[6] Packet are transmitted from rte[2]-rte[4]-rte[6].in this transmission packet is generated by rte[3]. In this case one base station can also transmit to another base station if it is overloaded. Figure- 9 scenario shows that there are three 3 base station like rte[1], rte[28], rte[50]. To the base station rte[1], packet are transmitted from rte[55]-rte[0]-rte[1]. In this transmission packet is generated by rte[55] then it transmitted to rte[55]. Then it transmitted to rte[0], which buffer the packet till it reaches to the neighbor node similarly it start from rte[27]-rte[29]-rte[28] and packet is generated by rte[31]. Similarly to the base station rte[50] Packet are transmitted from rte[52]-rte[53]-rte[50]. In this transmission packet is generated by rte[52]; so one base station is not transmitting its packet to another base station because each node is having enough quantity capacity.

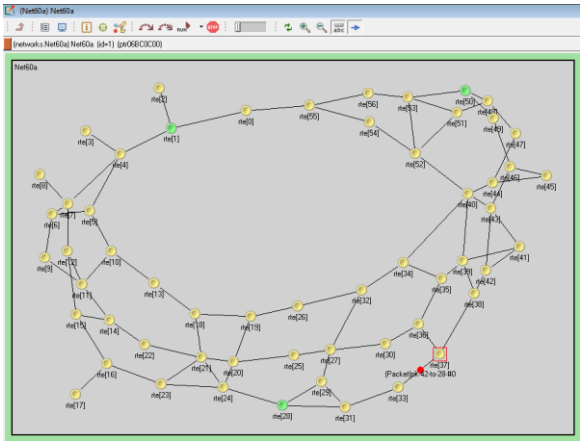

Figure- 9 NAM output during packet transmission with Three Base Stations and 52 no's of Transmitting Stations

From that we can conclude if a node is having enough quantity capacity then it can handled any traffic of finite capacity. Figure- 10 shows that the average packet transmission delay of date packet increases linearly. When the number of node increases, which indicates when network load increases due to congestion delay time of increases, in case of light load delay time is less. The Figure- 11 shows that the packet delivery ratio when the number of flow increases, the above parameter also increase correspondingly. That means packet loss is very less. Figure- 12 shows that the energy depletion rate; which shows that the network exist for a long time because the energy depletion rate is falling smoothly.

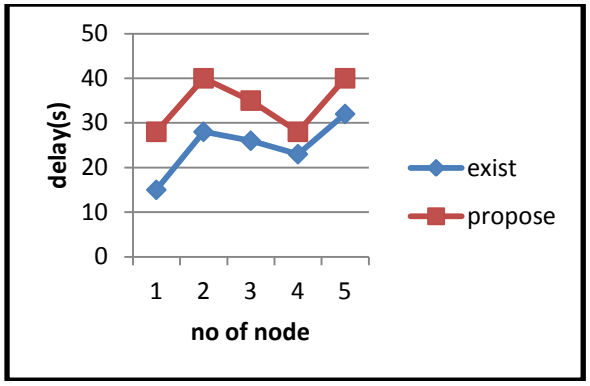

Figure- 10 Packet Transmission Delay

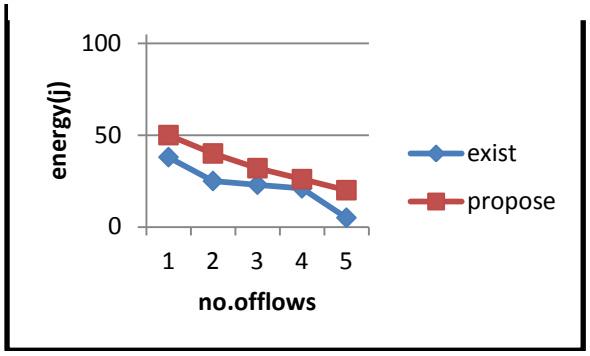

Figure- 11 Packet Delivery Ratio

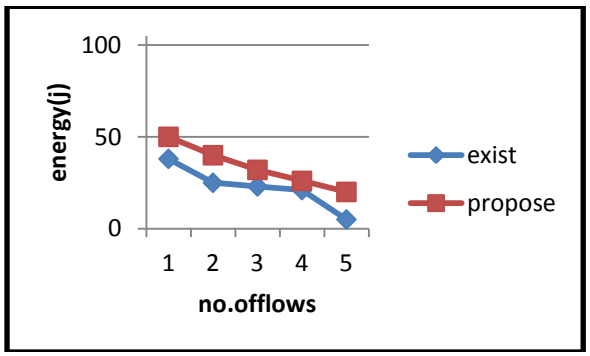

Figure- 12 Energy Depletion Rate

CONCLUSIONS AND FUTURE WORK

In this paper, we have proposed a secure hybrid geographic routing scheme, which employs an intermediate procedure between the geographic greedy mode and the recovery mode. We called this procedure Coordinate Depth Forwarding (CDF). Its main goal is to put the security during the transmission & improve routing efficiency in number of hops, without network overhead. Based on the distance in hops from the set of base stations in the network, we provided a virtual coordinate system, which contains topological information, in order to efficiency detour Void Simulation show that, in average, greedy-face routing algorithms presented a route 1.48 times longer than the optimal path. On the other hand, the hybrid GPSR+CDF Presented shorter routes, around 1.1 times longer than the optimal path when considering the scenario with four base stations. The RSA Digital Signature Scheme also provides a good security during the transmission of data packets. Finally the proposed algorithm provides 50% of performance improvement at the peak of the critical density range and good security during the transmission.

REFERENCES

[1] Gustavo Weber Denardin*, carols Henrique Barriquello, Alexander campos, Ricardo Nederson do prado, "A geographic routing hybrid approach for void resolution in wireless sensor network", The journal of system and software 84(2011) 1577-1590.

[2] Yi-hua Zhu a*, wan-deng wua,jian pan a Yi-ping Tang b, "An energy efficient data gathering algorithm to prolong lifetime of wireless sensor network", computer communication 33(2010)639-647.

[3] Gyanendra Prasad joshi and sung won Kim, "A Distributed Geo-Routing Algorithm for wireless sensor network", sensors 2009, 9, 4083-4103; doi: 10.3390/s90604083.

[4] lvan stojmenovic, Mark Russell and Bosko Vukojevic, "Depth First Search and Location Based Localized Routing and QoS Routing in wireless network", University of Ottawa Ciudad Universitaria, University of waterloo.

[5] Sundar Subramanian, Sanjay Shakkottai and piyush Gupta, "on optimal Geographic Routing in wireless network with Holes and Non-uniform Traffic".

[6] Aissani, M., Mellouk, a., Badache, N., Djebbar, M., "A new approach of announcement and avoiding routing voids in wireless sensor networks." In Global Telecommunications Conference. IEEE GLOBECOM 2008. IEEE, pp. 1-5.

[7] Abidalrahman moh' da, Hosein Marzib, Nauman Aslama, William phillipsa, William Robertsona, a*, "A secure platform of wireless sensor Network", procedia computer science 5(2011) 115-122.

[8] William R.claycomb, DongwanShin, "A novel node level security policy framework for wireless sensor network", jornal of network and computer application 34(2011)418-428.

[9] Necla Bandirmali a, Ismail Erturk b, "WSNsec: A scalable data link layer security protocol for WSNs", ad Hoc Network 10(2012)37-45.