INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue2)

LOAD BALANCING AND PROVIDING SECURITY USING RSA IN WIRELESS SENSOR NETWORKS

Megha I Mathapati
meghamathapati@gmail.com
M.Tech; CSE department
S.I.E.T., Vijayapur, India

Mr.Shrikant Salotagi
Shreekant2486@gmail.com
Assistant Professor, CSE department
S.I.E.T., Vijayapur, India

Abstract--This paper presents load balancing and provides security using RSA algorithm. This is brief introduction to handle the traffic on node. This represents the converge-casting protocol in wireless sensor networks. The protocol is localized and distributed, and adapts efficiently to vary traffic. Graphs are analyzed using NS-2 simulator, here end-to-end packet latency, packet delivery ratio, throughput are analyzed. This is done for 30 nodes in NS-2 simulation.

Key words: ***Load balancing algorithm, RSA algorithm, QPI, GPI, Encryption, Decryption***

I.INTRODUCTION

Sensors are distributed in the geographic area where these are sensing and gathering data. These are implemented through the deployment of wireless sensor networks (WSNs)[1] .A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability. These sensors work with each other to sense some physical phenomenon. That information is gathered and processed to get the relevant results. Wireless sensor networks consist of protocols and algorithms with self-organizing capabilities.

Dead ends are unable to forward the packets they generate or receive. These packets will never reach their destination and will be dropped shown in Fig 1.

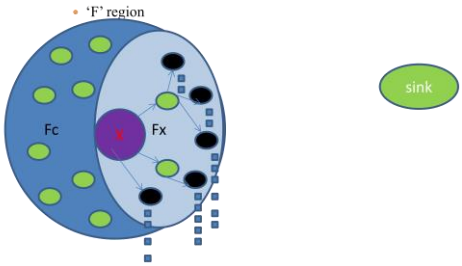


Fig 1: Dead ends

Designing challenges of geographic routing [1] are as follows:

i) Routing around dead ends,

ii) Resilience to localization errors, and

iii) Correct relay selection.

The main motto is to provide load balancing among the nodes and to overcome the packet loss and to provide security. So, ALBA mechanism performs load balancing based on splitting of packets, key generation and signature on data. The splitting of packets is based on number of inputs and transferring file /data will be encrypted using RSA algorithm.

II. LITERATURE SURVEY

A. *Research issues in load balancing geographic routing techniques [2]*

An ad hoc network is a network consisting of mobile hosts that is established as needed, not necessarily with any assistance from the existing internet architecture. The mobile hosts can communicate with each other using wireless broadcasts. However, allow the possibility that not all hosts are within the transmission range of each other. Thus communication between two hosts is achieved by multi-hop routing, where intermediate nodes cooperate by forwarding packets. Host mobility means that the topology of the network can change with time. Furthermore, no assumption can be made about the initial topology of the network. Several papers showed how to perform routing in ad hoc wireless networks based on the positions of the mobile hosts. However, all these protocols are likely to fall if the transmission ranges of the mobile hosts vary due to natural or man-made obstacles or weather conditions. These protocols may fall because in routing either some connections are not considered which effectively results in disconnecting the network, or the use of some connections causes lovelocks. These algorithms include Greedy mode and Recovery mode. The path strategies are shortest path, flooding-based, hop count. It provides low delivery rates for sparse graphs and high communication overhead for sparse graphs. It can perform up to 200 nodes geographic routing combined with GLS. Robust has the ability to deliver a message when the communication model deviates from the unit graph, due to obstacles or noise. It also involves greedy schemes for the performance of optimal shortest path algorithm for dense graphs

B. A location-based routing method for mobile ad hoc networks [3]

Using location information to help routing is often proposed as a means to achieve scalability in large mobile ad hoc networks. However, location-based routing is difficult when there are holes in the network topology and nodes are mobile or frequently disconnected to save battery. Terminode routing, presented here, addresses these issues. It uses a combination of location-based routing (Terminode Remote Routing, TRR), used when the destination is far, and link state routing (Terminode Local Routing, TLR), used when the destination is close. TRR uses anchored paths, a list of geographic points (not nodes) used as loose source routing information. Anchored paths are discovered and managed by sources, using one of two low overhead protocols: Friend Assisted Path Discovery and Geographical Map-based Path Discovery. In smaller networks, the performance is comparable to MANET routing protocols. In larger networks that are not uniformly populated with nodes, terminode routing outperforms existing location-based or MANET routing protocols. LAR is an on-demand routing protocol where location information is used to reduce the search space for a desired route, but it uses a DSR-like source routes for packet forwarding. The source uses the last known destination location in order to estimate the zone in which the destination is expected to be found. This zone is used to determine a request zone, as a set of nodes that should forward route requests. DREAM proactively maintains location information at each node in routing tables and data packets are partially flooded to nodes in the direction of the destination. It able to handle node failures and provides guaranteed delivery. It does not require additional storage.

C. A scalable logical coordinate's framework for routing in wireless sensor networks [5]

Recent technology has made exciting progress in large scale sensor networks, which opens the door for myriads of civil, meteorological and military applications. Large scale sensor networks can be deployed to carry out various tasks without the need for human intervention. Efficient data dissemination among different parts of the network is crucial for overall application performance. Such dissemination hinges on the design and implementation of efficient routing protocols. The latter implicitly defines a set of destinations by their attributes and delivers the data to all matching destinations. It is likely that future sensor networks need both types of routing protocols. Content-based routing may be used as an efficient multicast mechanism that discovers a set of destinations matching given criteria (and returns their addresses to the sender if needed). Address-based routing can then be used to unicast data individually to particular destinations in the content-

based groups as dictated by application logic. In this paper, focus on the latter type and assume that when the address-based routing is needed, the addresses of the destinations have been obtained in advance, presumably through some content based mechanism. Unicast defines transmitting same data to all the destinations. Unicast messaging is used for all network processes in which a private or unique resource is requested. All LANs (e.g. Ethernet) and IP networks support the unicast transfer mode, and most users are familiar with the standard unicast applications (e.g. http, smtp, ftp and telnet) which employ the TCP transport protocol.

D. Survey of localization techniques in wireless sensor networks [6]

The localization methods algorithms are centralized, Distributed, Range-free, absolute and Relative.

In Centralized localization method requires base station to gather network wide environment information & with plenty of computational power. Examples are SDP-semi definite programming. It performs longer-delay, lower energy. In Distributed localization method each node is independent. It performs up to limited communication and poor localization. Example is diffusion and approximate point of triangular test. In Range-free localization method is based on distance between nodes to obtain unknown node's location. Therefore, it requires additional energy consumption. Examples are centroid localization, APIT.

In absolute localization method is based on GPS. It requires sensor equipped with GPS receiver. It is easily understood and used by users. In relative localization method is used to obtain the relationship of distance (or) angle between nodes. It is performed by manual configuration or reference nodes.

E. Geometric spanners for routing in mobile networks [7]

It is based on the restricted Delaunay graph (RDG), for mobile ad hoc networks. Each node only needs constant time to make routing decisions. Obtaining the location information is difficult (or) expensive. Location is performed by means of GPS and it is costly to perform. In this, source node first acquires the location of the destination node it wants to communicate and then forwards the packet to a neighbor closer to the destination .It does not require hash tables or make global broadcasts. It suffers from local minimum in which a packet stuck at a node does not have a closer neighbor to the destination. Therefore, it provided a way to maintain a planar sub graph of the underlying connectivity. When a packet is stuck at a node, the protocol will route the packet around a face of the graph to get out of the local minimum. This process is repeated until it reaches the destination. It consists of sub graphs such as relative neighborhood graph and Gabrial graph to solve the local minima problem.

III. LOAD BALANCING ALGORITHM

This is the cross layer solution for the converge casting. This protocol is represented by geographic routing scheme. This integrates awake/asleep schedules, traffic load balancing. Nodes alternate between the awake and asleep modes. Relay is greedily chosen based on the advancement it provides towards the sink. Geographic routing requires little computation and storage resources at the nodes.

ALGORITHM

STEP 1: Source node broadcasts RTS to neighbor awake agents.

STEP 2: Available nodes respond to CTS.

STEP 3: Source Node chooses the best relay based on the QPI AND GPI.

Where, QPI: Queue priority index.

GPI: Geographic priority index.

STEP 4: GPI=Average number of packets which can transmit without error.

STEP 5: QPI=min $\{Q+NB, Nq\}$…….(I)

M

Where, Q =No of packets in queue,
M=Average no of moving packets

NB=Requested no of packets transmitted in burst.

Nq = max allowed QPI

Here, Low QPI decrease the latency and balances the network load

IV. RSA ALGORITHM

The most important public-key cryptosystem is the RSA cryptosystem on which one can also illustrate a variety of important ideas of modern public-key cryptography [8]. Invented in 1978 by Rivest, Shamir, Adleman .Basic idea: prime multiplication is very easy, integer factorization seems to be unfeasible.

STEP 1: A user wishing to set up an RSA cryptosystem will:

a. Choose a pair of public/private keys: (PU, PR).
b. Publish the public (encryption) key.
c. Keep secret the private (decryption) key.

STEP 2: Design of RSA cryptosystems

a. Each user generates a public/private key pair by: (PU, PR).
b. Selecting two large primes at random - p, q
c. Computing their system modulus N=p.q , note ø(N)=(p-1)(q-1)
d. Selecting at random the encryption key e
Where, $1<e<ø(N)$, $gcd(e,ø(N))=1$
e. solve following equation to find decryption key d
f. $e.d=1 \bmod ø(N)$ and $0 \leq d \leq N$

STEP 3: publish their public encryption key: KU={e,N}

STEP 4: keep secret private decryption key: KR={d,p,q}

V.PROPOSED SYSTEM

This is the combination of Load balancing, RAINBOW protocol and RSA algorithms which enhances greedy geographic forwarding and security. The new relay selection scheme implements a routing function in a cross-layer fashion. For data transfer security is given.

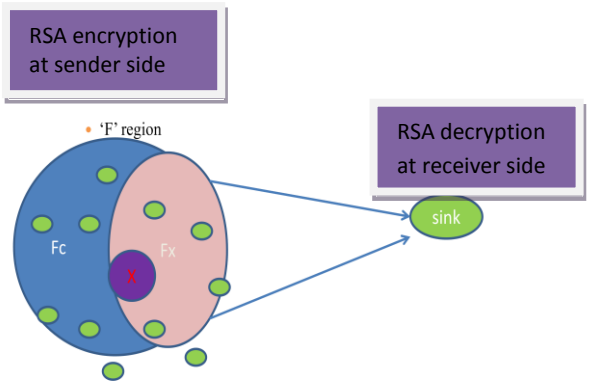


Fig 2: Proposed system

The figure Fig2 shows the proposed system. Here x be a node that is engaged in packet transferring. Transmission area is divided into Fc region and Fx region. Fx region provide positive advancement and Fc region provides negative advancement. Before transferring packets X node does the RSA encryption to the packets and packets are moved in accordance with the load balancing algorithm. At the sink side RSA decryption is done. Flowchart of the system is drawn in figure Fig 3.

Flow chart:

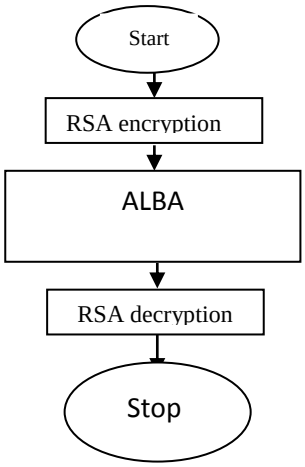
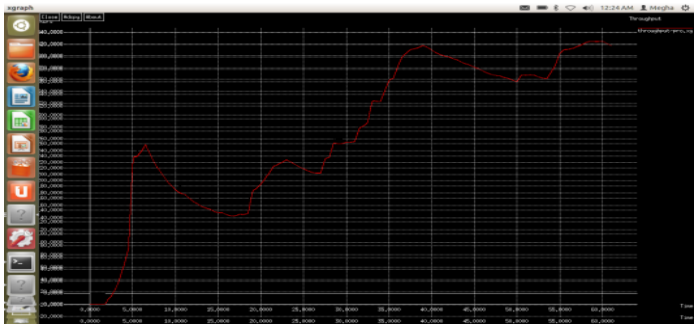


Fig 3: flow chart of the system

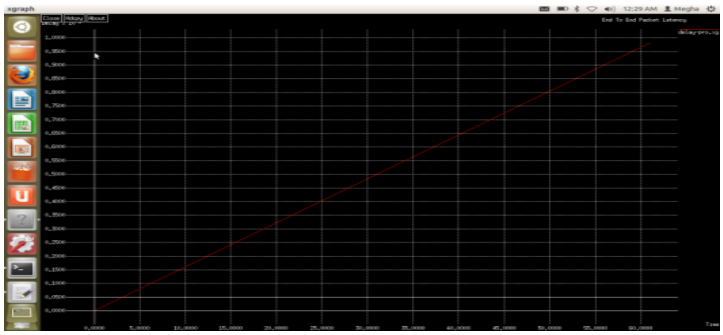
ALGORITHM

STEP 1: Initially all the nodes are in zeroth position.
STEP 2: Encryption of the sending data with RSA algorithm.
STEP 3: Nodes will move to their particular position.
STEP 4: Find GPI.
STEP 5: Find QPI,
QPI= [Q+NB/M],
STEP 6: Initially all the nodes are colored as C0,
STEP 7: Transmission of the data starts according to the ALBA mechanism using RSA key for encryption to provide security.
STEP 8: step7 repeats till the end of the transmission.
STEP 9: Finally Load balancing and solving problem .
STEP 10: Decryption is done using RSA while receiving the data.
STEP 11: Finally Xgraphs are taken as output.

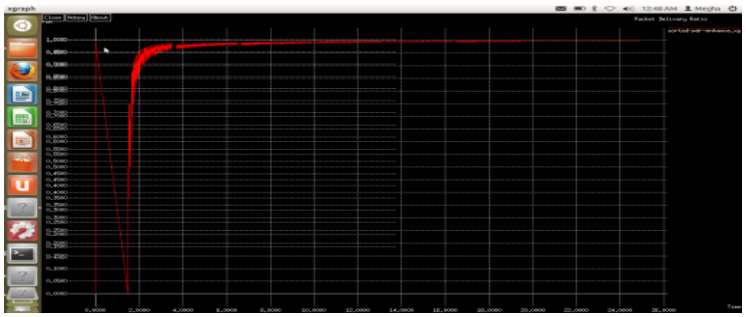
VI.PERFORMANCE ANALYSIS



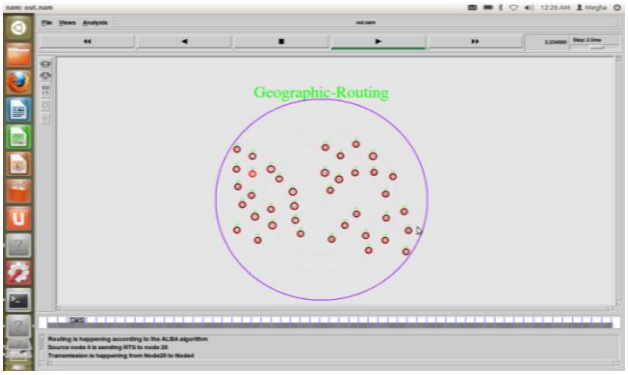
(a) Throughput of the system



(b) End-to-end packet latency



(c) Packet delivery ratio



(d) Geographic routing.

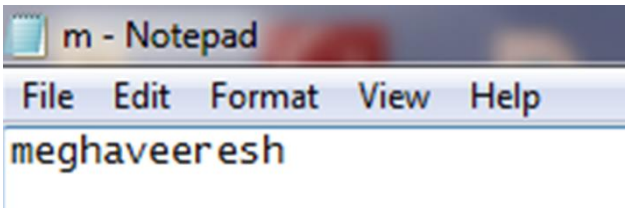
Fig 4: X –graph simulations

The X-graph shown in fig4 (a) describes the throughput of the system. Here X axis represents time and Y axis represents kb/s. If throughput is more, proposed system is efficient.

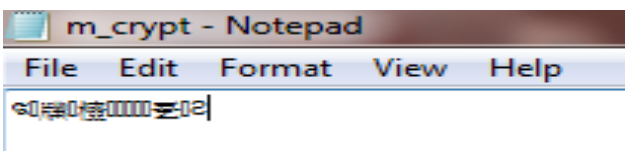
The X-graph shown in fig4 (b) describes the end to end packet latency of the system. Here X axis represents time and Y axis represents delay. If end to end packet latency is less, proposed system is efficient.

The X-graph shown in fig4 (c) describes the packet delivery ratio of the system. Here X axis represents time and Y axis represents packet delivered. If end to end packet delivery ratio is less, proposed system is efficient.

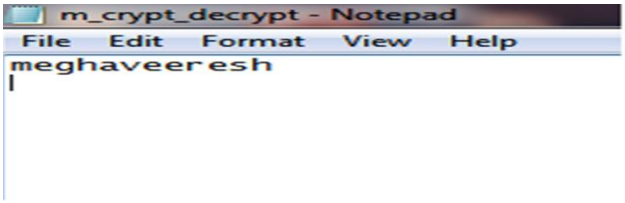
The graph shown in fig4 (d) describes the simulation of geographic routing of the system.



5. (a) Original 'm' file



5. (b) Encrypted 'm' file



5. (c) Decrypted 'm' file

Fig 5: RSA process

The RSA process is shown in the Fig 5. Original file is shown in Fig5 (a) and encrypted and decrypted file is shown in Fig 5(b) and 5.(c) respectively.

VII .CONCLUSION

The problem of routing around connectivity holes is solved. The combination of the two protocols results in load balancing. This achieves the performance superior to the existing protocols in terms of energy efficiency, packet delivery ratio. And RSA algorithm provides the security for transferring the data in the network.

REFERENCES

[1]. Chiara Petrioli, Michele Nati,Paolo Casari,Michele Zorzi, and Stefano Basagni, **"ALBA-R: Load-Balancing Geographic Routing Around Connectivity Holes in Wireless Sensor Networks",** IEEE TRANSACTIONS, VOL. 25, NO. 3, MARCH 2014.

[2].A LBA-R: Load balancing geographic routing in wireless sensor networks, S.Sujeet, Mr. P.Karunakaran and Mr.C.Venkatesh International Journal of Scientific & Engineering Research,Volume 5, Issue 1, January -2014 1908 ISSN 2229 -5518

[3]. An Efficient Location Based Routing for Mobile Adhoc Networks , ISSN(Online): 2320 - 9801ISSN (Print): 2320 -9798 International Journal of Innovative Research in Computer and C ommunication E ngineering S.Saranya , D.Gokilapriya , M.Maheswari

[4]. Locating and bypassing holes in sensor networks INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies (Volume:4) Date of Conference: 7-11 March 2004

[5].Ad-hoc, Mobile, and Wireless Networks: 11th International Conference, ADHOC ...edited by Xiang-Yang Li, Symeon Papavassiliou, Stefan Ruehrup Xiang-Yang Li, Symeon Papavassiliou, Stefan Ruehrup - 2012

[6]. A Survey of Localization in Wireless Sensor Network Long Cheng,1 Chengdong Wu,1 Yunzhou Zhang,1 Hao Wu,2 Mengxin Li,3 and Carsten Maple4International Journal of Distributed Sensor Networks Volume 2012 (2012), Article ID 962523, 12 pages

[7].Geometric spanners for routing in mobile networks, jie gao , member, ieee, leonidas j. guibas, john hershberger, li zhang, and an zhu selected areas in communications, vol. 23, no. 1, january 2005

[8]. RSA Cryptosystem using Object -Oriented Model ing Technique N. C. Ashioba , R. E. Yoro, Volume 4No. 2, February 2014ISSN 2223-4985 International Journal of Information and Communication Technology Research ©2014 ICT Journal.