An Efficient Location Privacy Using GSP and Flow Deviation methods In Wireless Sensor Networks

[1]Soumya.S.M
PG Scholar
Department of Information technology
SNS College of Technology, Coimbatore-641035,
TamilNadu, India
soumyamadhavan4@gmail.com

[2]G.Selvavinyagam
Assistant Professor
Department of Information Technology
SNS College of Technology, Coimbatore-641035,
TamilNadu, India
ohmselva@gmail.com

***Abstract*- Location privacy measures need to be developed to prevent the adversary from determining the physical locations of source sensors and sinks. An adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. On the other hand, sensors usually have limited processing speed and energy supplies. So find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes as well as provide privacy preserving protocols for source and sink location in such sensor networks. Thus in the proposed system the sinks should be located as optimally as possible to reduce traffic flow and energy consumption for sensor nodes. Hence Sink placement problem is resolved for minimizing the delay as well as maximizing the lifetime of a WSN. Thus proposed system is efficient in terms of overhead and functionality when compared to existing system.**

Keywords*—*LocationPrivacy,adversary,sink,overhead,routing packet

I.INTRODUCTION

Location privacy is very important in hostile environments. Failure to protect such information can completely destroy the intended purposes of sensor network applications. Location privacy measures need to be developed to prevent the adversary from determining the physical locations of source sensors and sinks. Due to the limited energy lifetime of battery-powered sensor nodes, these methods have to be energy efficient.

Content of messages is protected but contextual information can be exploited by attacker to derive sensitive information such as the locations of monitored objects (source) and data sinks (destination) in the field. To protect such information, researchers in sensor network security have focused considerable effort on finding ways to provide classic security services such as confidentiality, authentication, integrity, and availability. Though these are critical security requirements, they are insufficient in many applications.

An adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets and exploit the information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. On the other hand, sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. So find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes as well as provide privacy preserving protocols for source and sink location in such sensor networks.

In location-based services, a user may want to retrieve location-based data without revealing her location. Techniques such as k-anonymity and private information retrieval have been developed for this purpose. The adversary monitors the wireless transmissions to infer locations of critical infrastructure. However, there are some challenges unique to sensor networks. First, sensor nodes are usually battery powered, which limits their functional lifetime. Second, a sensor network is often significantly larger than the network in smart home or assisted living applications

A. Applications Of The Location Privacy

1). Environmental Applications

Nowadays sensor networks are also widely applied in habitat monitoring, agriculture research, fire detection and traffic control. Because there is no interruption to the environment, sensor networks in environmental area is not that strict as in battlefield.

Bush Fire Response: A low cost distributed sensor network for environmental monitor [1] and disaster response. An integrated network of sensors combining on the ground sensors monitoring local moisture levels, humidity, wind speed and direction, together with satellite imagery and longer term meteorological forecasting will enable the determination of fire risk levels in targeted regions as well as valuable information on probable fire direction.Such a network will provide valuable understanding of bushfire development and most importantly assist authorities in organizing a coordinated disaster response that will save

lives and property by providing early warning for high risk areas.

2). Health Applications

Sensor networks are also widely used in health care area [16]. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital.

Long-term nursing home: This application [16] is focus on nursing of old people. In the town farm cameras, pressure sensors, orientation sensors and sensors for detection of muscle activity construct a complex network. They support fall detection, unconsciousness detection, vital sign monitoring and dietary/exercise monitoring. These applications reduce personnel cost and rapid the reaction of emergence situation.

II.EXISTING SYSTEM

The communications between sensor nodes in the network are encrypted so that the contents of packets appear random to the global eavesdropper. Many key pre distribution protocols are used.

- Location Privacy to Monitored Objects (Source-Location Privacy):
  a. Periodic Collection
  b. Source Simulation.
- Location Privacy to Data Sinks (Sink-Location Privacy):
  a. Sink Simulation
  b. Backbone Flooding.

Prior techniques assume a local eavesdropper which is capable of eavesdropping on a small region. The existing technique assumes global eavesdropper needs to identify the region exhibiting a high number of transmissions to locate the sink.

A. Source-Location Privacy Techniques

The two techniques provide location privacy to monitor objects in sensor networks. Periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. Source simulation method provides practical trade-offs between privacy, communication overhead, and latency.

1). Periodic Collection

The traffic pattern must be independent of the presence of real objects. Hence every sensor node independently and periodically sends packets [9] at a reasonable frequency regardless of whether there are real data to send or not. Each sensor node has a timer that triggers an event every second, as well as a first-in-first-out (FIFO) queue of size q for buffering received packets that carry real data reports. When the timer fires, the node checks if it has any packets in its queue. If so, it dequeues the first packet, encrypts it with the pairwise key it shares with the next hop, and forwards it to that node. Otherwise, it sends a dummy packet with a random payload that will not correctly authenticate at the next hop. Since every sensor node only accepts the packets that correctly authenticate, dummy packets do not enter the receiver's queue. When the queue at a sensor node is full, it will stop accepting new packets.

2). Source Simulation

Create multiple candidate traces in the network to hide the traffic generated by real objects and determine how many number of candidate traces is application dependent.

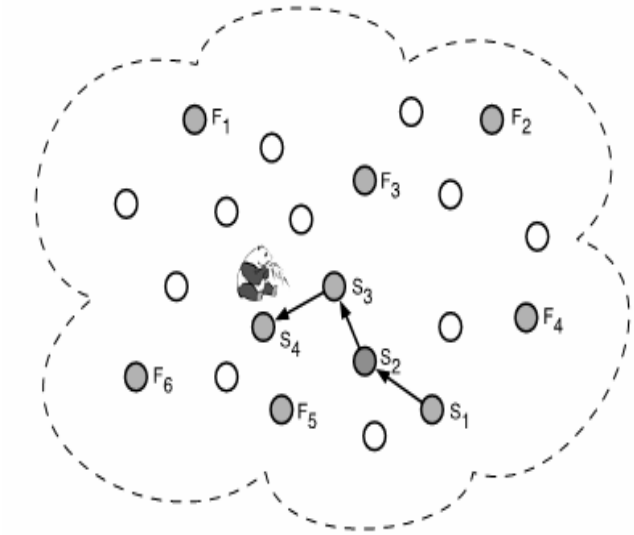

Fig 2.1 Movement Pattern Leaks Location Information

The behaviour of fake objects is modelled inaccurately in one location all the time. Based on this model, the candidate traces are created at locations {F1; F2; ...; F6}. Sensors at each of these locations will send fake traffic to the sink, simulating a real object. However, the adversary can sense the object moves around in the field along the path {S1; S2; S3; S4}. This is used to distinguish real objects from fake ones.

In general, the attacker may be able to distinguish the movement patterns of real objects from fake ones, even if we have the fake ones move. Even if the attacker learns about the object behavior over time, the defender can observe and learn the same behaviour and can broadcast occasional updates to the object movement model. Thus, it is often reasonable to assume that the adversary and the defender have similar knowledge about the behavior of real objects. Thus more useful candidate traces in the field are created to hide real objects.

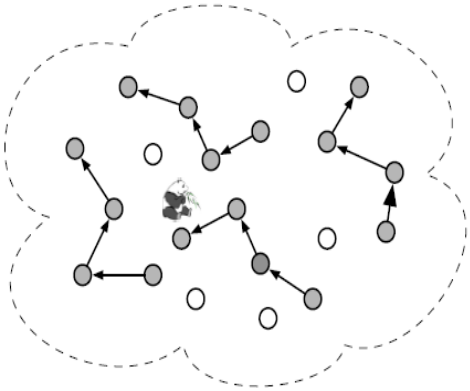

Fig No. 2.2 Simulating Fake Source in the Field

B. Sink-Location Privacy Techniques

The two techniques provide protection of passive sinks in sensor networks [1]. Sink simulation method achieves location privacy by simulating sinks at specified locations. Backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks.

1). Sink Simulation

Sink location privacy confuse the adversary by creating virtual sinks. For this purpose, multiple candidate traces are created toward the fake sinks in the network to hide the traffic between real objects and real sinks [10]. Fake sinks receive traffic similar to the traffic received by a real sink. So it is hard to differentiate fake and real sinks while sensors send packets to the destination sink.

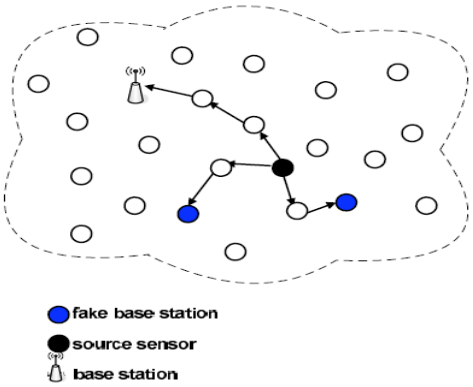

Fig No. 2.3 Simulating Fake Sink in the Field

2). Backbone Flooding

When large number of fake sinks is created to meet high location privacy requirements, the sink simulation approach is very expensive. The reason is that a lot of extra communication is wasted during the routing of packets to randomly selected fake sinks. Thus instead of sending them directly to a few sinks, backbone flooding technique is used.

The main component of backbone flooding is the construction of the backbone. They flood the packets to cover an area large enough to achieve the desired level of location privacy. Such that each sink is within the range of at least one backbone member.

The packets are sending to a connected portion of the network called as backbone. Those packets are only flooded among the backbone members. As long as the real sinks are located in the communication range of at least one backbone. Backbone member, they can receive packets from any source in the field. Clearly, for a global eavesdropper, the sink could be anywhere near the backbone.

C. Drawbacks of Existing System

The main drawbacks of the existing systems are of high time delay maid by the observation of adversarial node

D. Problem Definition

- Assumption: global eavesdropper does not compromise sensor nodes. Practical: global eavesdropper may be able to compromise a subset of the sensor nodes in the field. So seek solutions to the problem of providing location privacy even though nodes being compromised .
- The passive sinks that receive data from sensors are protected. But location privacy for sinks that broadcast packets is not deployed in existing work.
- It takes time for the observations made by the adversarial network.
- So impact of such "delayed" analysis and reaction is considered to minimize. Dummy sequences usually require the addition of dummy traffic into the network leading to more communication overhead might be reduced.

III. PROPOSED SYSTEM

Some source nodes are transferring relatively large amounts of data. As a result, these nodes run out of battery faster due to improper position of nodes and sinks. Thus the sinks should be located as optimally as possible to reduce traffic flow and energy consumption for sensor nodes. Hence Sink placement problem [15] is resolved for minimizing the delay as well as maximizing the lifetime of a WSN.

A. Strategies for Minimizing the Maximum Delay

1) *RSP* - Random sink placement is used as a lower bound for other strategies.
2) *GSP* - Geographic sink placement is used as target sink placement whose sensor nodes positions are unknown.
3) *ISP* - Intelligent sink placement is used as optimal sink placement whose sensor nodes positions are known.

4) GASP - Genetic Algorithm-based sink placement is good approximation for ISP.

Finally, numerical results are obtained using DISCO network calculator. Thus GSP proved to be a good heuristic for large-scale WSNs with uniform node distributions. It does not take much computation time and is suitable for the sink placement of general WSN applications.

B. Issues in Sink Location

1). Communication spends a lot of energy while sensor nodes have limited battery power in single sink deployment.
2). Messages are sent to their destination via multi-hop communication. Thus traffic intensity in the network becomes high and data transfer is delayed

C. Algorithm

1). Algorithm for Minimizing the Delay using GSP
Step 1: Deploy uniform random node distribution
i. unknown positions of sensor nodes - GSP or RSP strategy.
(Or)
ii. Known positions of sensor nodes - ISP or GASP strategy. (Calculate candidate locations)
Step 2: Iteration:
i. place sensor nodes
ii. Place sink strategy
iii. Connect all nodes
iv. Check connectivity of network
v. choose the nearest sink
vi. Calculate the maximum delay
Step 3: Repeat 2 according to the selected sink placement strategy
Step 4: Select the locations with minimum worst-case delay
Step 5: GSP strategy runs only a single iteration as the sinks are placed at fixed positions

2). Calculating Delay using Network Calculus

Data should not be dropped during the transmission and it should be guaranteed not to exceed a maximum worst-case delay. Network calculus is proposed for worst-case analysis in WSNs.

Bounding (limiting) processes called arrival curve (α) and service curves (β) can capture maximum delay. The arrival curve bounds the input function which is the sensed data of each sensor node, whereas the service curve depends on the duty cycle and therefore it can be adjusted to achieve certain energy efficiency goals.
Sensor network calculus is a tool for worst-case traffic analysis in WSNs. It calculates maximum delay in message transfer, maximum buffer requirements at each sensor node and lower bounds on duty cycles. Sensor network calculus is of three bounds: backlog bound, delay bound and output bound.

- Backlog bound is the vertical deviation(distance or positions) between and β.
- Delay bound is the horizontal deviation (message transfer) between α and β.
- The output bound of each server can be calculated by deconvoluting curves α and β. (Reverse the effects of convolution on recorded data-{Produces modified version of overlap between the two functions}).
- From these definitions calculate total delay for each flow. Thus using network calculus delay is captured.

D. Minimizing the Delay by GSP

It is used where sinks are placed at the center of gravity of a sector.This is for uniformly distributed networks when there is no information about sensor nodes locations. In GSP [16], the sinks are placed at the center of gravity of a sector of a circle (CGSC). It requires only the number of the sinks and the radius of the field to calculate the centers of gravity. The center of gravity is simply found by multiplying with radius R using eq(4.1).

$$CGSC=F(\alpha) * R \quad (1)$$

The center of gravity of a sector with angle α always lies on the middle radial line (α/2) of the sector. Eq(4.2) calculates the ratio where to place the sink at the middle radial line of a sector.

$$F(\alpha) = \frac{\frac{4}{3}sin(\frac{\alpha}{2})}{\alpha} \quad (2)$$

The value of α must be within the range 0 to π/2 if it is in radians. Degree of a sector can be obtained from eq(4.3).

$$sDegree = 2\pi / \#sinks \quad (3)$$

The degree depends on the number of sinks. For single sink WSNs places the sink at the center of the circle. For two sinks placement, sinks are placed at the center of gravity of the semi-circles.

E. Flow deviation method

Flow deviation (FD) method is a general method for solving nonlinear programming problems. A FD-based algorithm isdivided into two phases: the *initialization* phase and the *updating* phase. In the initialization phase, an initial solution of the problem is found. In our case, to form the initial solution, we choose a shortest hop path for each end-to-end flow. Then the FD algorithm enters *updating* phase in which the initial solution is improved incrementally by changing the routing paths of some end-to-end flows. The rerouting of end-to-end flows is not made simultaneously;

instead, one end-to-end flow is selected at one time whose path is established with the goal to optimize the objective function. Through coordinated rerouting process, a locally optimal routing solution can be reached ultimately.

1).FD-based Routing Algorithm

Step 1: Compute the shortest hop path for each end-to-end flow.
Step 2: Select an end-to-end flow wrandomly or according to a sequence defined in advance. If the sequence is exhausted, it is simply repeated.
Step 3: Remove the traffic requirement rw for w from the network.
Step 4: Fix the routing paths for all other end-to-end flows and reroute the selected end-to-end flow waiming to optimize the objective function.
Step 5: If rerouting of flow w does not improve the objective function, restore its old routing path.
Step 6: Go to step (2) until all the end-to-end flows have been examined once, but no further improvements are possible.

In the worst case, the algorithm takes exponential time to converge. But it can be efficient in a probabilistic sense proves that the algorithm takes iterations on average where is the number of nodes in the network.

IV. RESULT

Location privacy measures need to be developed to prevent the adversary from determining the physical locations of source sensors and sinks. An adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. On the other hand, sensors usually have limited processing speed and energy supplies. The source-location privacy technique protects the location of monitored objects to increase the number of messages sent by the source before the object is located by the attacker

The techniques provide location privacy to objects and sinks against a global eavesdropper. The periodic collection method provides the highest location privacy to monitor highly valuable objects with less cost. This method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. Thus it is suitable for applications that collect data at a low rate from the network about many objects.

The source simulation method provides a trade-off between privacy and communication costs. The sink simulation and backbone flooding methods provide location privacy for the sinks. The backbone flooding method is clearly more suitable for the cases where a high level of location privacy is needed. The sink simulation method is more robust to node failure in the network. In the backbone flooding idea, it need to always keep the backbone connected and rebuild the backbone from time to time to balance the communication costs between nodes. Backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks.

In the GSP system the sinks should be located as optimally as possible to reduce traffic flow and energy consumption for sensor nodes. Hence Sink placement problem is resolved for minimizing the delay as well as maximizing the lifetime of a Wireless Sensor Networks. Thus GSP system is efficient in terms of delay, overhead and functionality when compared to existing system. The delay made by the observation of network node in the existing system is greater .Thus efficiently the delay can be reduced by the GSP technique

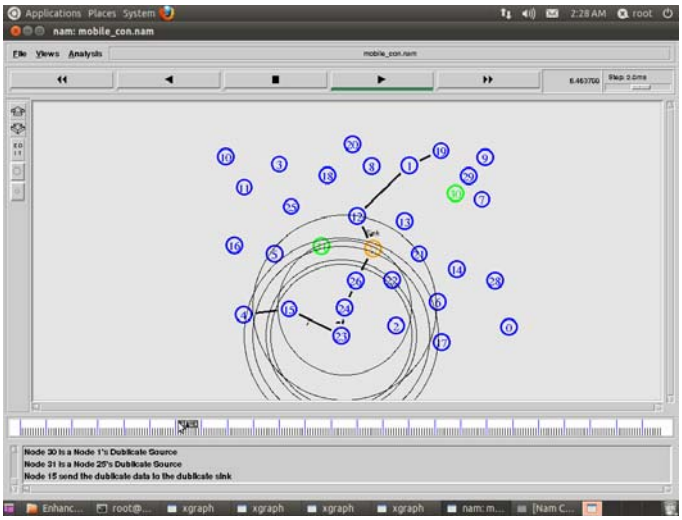

Fig 4.1GSP Method

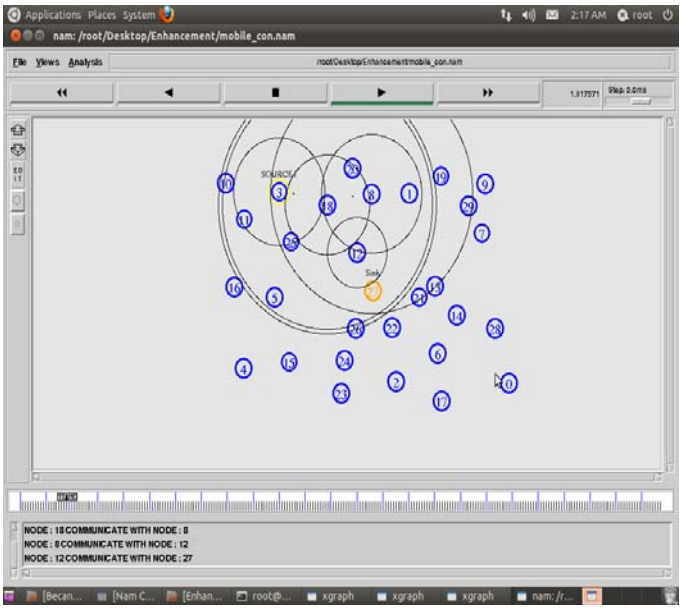

Fig 4.2 Flow Deviation Method

A.Comparison Graph

Sink and source nodes are deployed in the networks. Here 30 nodes are initialized .Sink send request message to all sensor nodes. Hop count is compared to hop value and then request is processed. Sensor node gives response to the sink node. During response passing hop count value is increased. It sends packets to a connected portion of the network , the backbone, instead of sending them directly to a few sink .Create multiple candidate traces in the network to hide the traffic generated by real objects. Each of the fake object generate traffic pattern similar to that of a real object to confuse the adversary. The packets are only flooded among the backbone members, the sensors that belong to this backbone. Every sensor node independently and periodically send packets at a reasonable frequency regardless of whether there are real data to send or not. Create multiple candidate traces towards the fake sinks in the network to hide the traffic between real objects and real sinks.

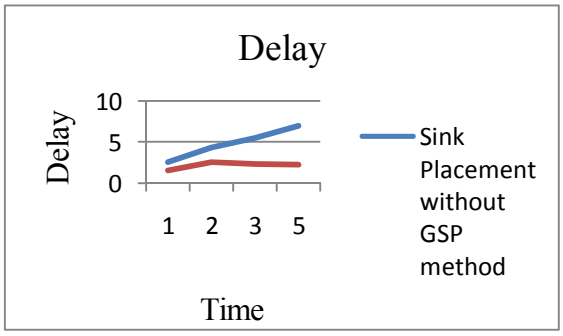

Fig No 5.1Comparison of Delay

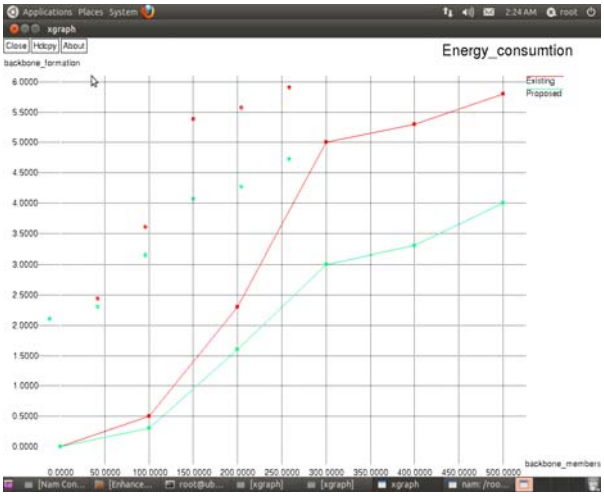

Fig No 5.2 Comparison of Energy

The above comparison graph shows the delay made by the node with and without GSP technique. In GSP technique Delay can be reduced by placing the sink in the center of gravity. The delay can be 95% decreased in the system.In Flow Deviation Method Optimum path will be find out.Only through this path message cane be passed.By using the Flow Deviation Method Energy Consumption is reduced.

V. CONCLUSION

The techniques provide location privacy to objects and sinks against a global eavesdropper. The periodic collection method provides the highest location privacy to monitor highly valuable objects with less cost. The source simulation method provides a trade-off between privacy and communication costs. The sink simulation and backbone flooding methods provide location privacy for the sinks. The sink simulation method is more robust to node failure in the network. In future the existing approach is extended in such a way that global eavesdropper may be able to compromise a subset of the sensor nodes in the field. Delay made by the observation of adversarial node will be reduced by GSP method. Energy consumption and overheads are reduced by Flow Deviation Methods .So seek solutions to the problem of providing location privacy even though nodes being compromised in future work. On the other hand the passive sinks that receive data from sensors are protected. But location privacy for sinks that broadcast packets is not deployed in existing work

REFERENCE

[1] Bo An, Victor Lesser, David Irwin,Michael Zink "Automated Negotiation with Decommitment for Dynamic Resource Allocation in Cloud Computing" , Proc. of 9th Int. Conf. on Autonomous Agents and Multiagent System, May, 10–14, 2010

[2] Chris Peiris, Dharmendra Sharma "C2TP: A Service Model for Cloud" CLOUD COMPUTING 2010 : The First International Conference on Cloud Computing, GRIDs, and Virtualization Volume 1, Issue 4, June 2013

[3] Divya Jyothi **"**Ecommerce Dealer Agent Mechanism in Cloud Computing Environment" International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 4, June 2012

[4] *Edwin* Yaqub, Philipp Wieder, " A Generic Platform for Conducting SLA Negotiations"

[5] Gaurav Raj, Ankit Nischal "Efficient Resource Allocation in Resource provisioning policies over Resource Cloud Communication Paradigm"

ICCSA,Vol.2,No.3,June 2012

[6] Kwang Mong Sim "Grid Resource Negotiation:Survey and New Directions" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 40, NO. 3, MAY 2010 245

[7] Kwang Mong Sim, Senior Member, IEEE, and Benyun Shi "Concurrent Negotiation and Coordination for *Grid Resource* Coallocation" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: CYBERNETICS, VOL. 40, NO. 3, JUNE 20.

[8] Mario Macıas, J. Oriol Fito and Jordi Guitart "Rule-based SLA Management for Revenue Maximisation in Cloud Computing Markets", CNSM 2010

[9] Mario Macías, Jordi Guitart "A Genetic Model for Pricing in Cloud Computing Markets"

[10] Rabi Prasad Padhy, Dr. Manas Ranjan Patra,Dr. Suresh Chandra Satapathy"SLAs in Cloud Systems: The Business Perspective", InternatIonalJournal ofComputerSCIenCe and technology Vol. 3, ISSue1, Jan. - MarCh2012.

[11] Rajkumar Buyya, Chee Shin Yeo and Srikumar Venugopal " Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities"

[12] Rajkumar Buyya,Rajiv Ranjan, Rodrigo N.C "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services"

[13] Seokho Son and Kwang Mong Sim "A Price- and-Time-Slot-Negotiation Mechanism for Cloud Service Reservations", IEEE TRANSACTIO03.+6603.+6

[14] NS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 42, NO. 3,JUNE 2012

[15] Vivek Shrivastava, D.S. Bhilare "Algorithms to Improve Resource Utilization and Request Acceptance Rate in IaaS Cloud Scheduling"Int. J. Advanced Networking and Applications 1367 Volume: 03, Issue: 05, Pages: 1367-1374 (2012)

[16] Wang Xiaojing,Tong Wei,Ren Jia,Ding Linjie,Liu Jingning"Weighted Fairness Resource Allocationof Disks in XEN" IJCCSA,Vol.2, No.3, June 2012

AUTHORS PROFILE

Soumya S.M has completed his Bachelor of Technology in Ponjesly College Of engineering in 2011 under Anna University Thirunelveli. Pursuing Mater of Engineering in Computer and Communication Engineering in SNS College of Technology 2011-2013 under Anna University Chennai.

G.Selvavinayagam has completed Bachelor of Engineering in Computer Science and Engineering in 2003 under Bharathiar University, Master of Engineering in Computer and Communication Engineering in 2009 under Anna University Chennai, Master of Science in Psychology in 2009 under University of Madras, Master of Business Administration in Human Resource in 2010 under Bharathiar University Chennai and pursuing Ph.D in Computer Science under Anna University Chennai. He has published many research paper in National and International Journals. Currently he is a member of Professional Bodies like ISTE, IACSIT,etc. His area of interest includes Theoretical Computer science, Automata Theory,Crytography and Network Security.