# End-To-End Trust Based Transmission Optimization in Smartgrid Network Architecture

M.Ramasaravanan[1], M.Kirithikadevi[2]
*Department of Computer Science and Engineering*
*Chendhuran College of Engineering and Technology*
*Anna University*
*Tamilnadu*
*India*

***Abstract*-- The end to end trust based transmission architecture usually crosses several ages to achieve their accuracy and defense tolerated mechanisms. In this trend the forced communication network brings more weakness to the evolving smart grid. Therefore, defensive techniques such as intrusion detection will need to be deployed in this already complicated system. Deployment and runtime cost due to the defensive trust systems will affect the original function of smart grid system without careful planning and design. For the above mentioned problem the new system is required which covers the approach in the following areas: 1) Trust based optimization in source end 2) Applying the new configuration mechanism in the transmission medium 3) Guaranteed the destination end to receive the quantity of stuff received in that system capacity(destination capacity). So that the new system should applying the configuration to the transmission medium to set and check the receiving ration of the destination end at each and every time. If the receiving capacity of the destination is equal to the transmission ratio, the configuration does not required to act; otherwise the configuration mechanism brings the technique to set the forced packets into the receiving capacity of the receiving end. This system is an effort to address this important issue. In particular, the set packing algorithm is used to optimize the placement of the trust nodes of the defensive system in the multiple layer architecture of the smart grid. After the trust nodes are placed, a trust node aware optimal routing algorithm is used to find the least cost routing in the communications of the nodes. The proposal of an algorithm is to identify new trust node to address the fault tolerance requirement of the smart grid system, and talented by providing safe, competent, and trustworthy communications in the smart grid network.**

***Keywords*—Smart grid, End to End Trust Based Transmission Architecture, Intrusion Detection System, Wide Area Network.**

## I. INTRODUCTION

The power grid we are utilizing is one-century old and aging for the modern industry. The dramatic economic loss brought by the obsolete power system triggers the research of the smart grid. The new electric grid being developed in this century should have the ability or potential of transforming renewable energy, preventing cyber intrusions to the critical infrastructure, and providing effective and real-time computing and communication technologies to the customers. As the new systems are designed and the new devices are utilized, the flaws may occur as some new problems are ignored. In particular, the security of the smart grid network becomes one of the crucial issues that deserve a systematic study.

According to recent standards such as the North American Synchrophasor Initiative (NASPI), and the Smart Grid standardization effort, smart grid will be more communication-oriented and open standards-based. And the intrusions will more likely happen in the communication network infrastructure of the power system. The supervisory control and data acquisition (SCADA) and its sub-equipment are the vulnerable targets of the intrusions. Intrusion detection systems (IDSs) can be used to defend various attacks in the smart grid system, for instance, in an AMI monitoring architecture was proposed and demonstrated that the detection mechanisms should be deployed and coordinated.

Also, the communication network of the smart grid is distribute data multiple levels, WAN (wide area networks) by wired network; and NAN (neighborhood area networks) by mesh wireless network. As the communication mechanisms and the security requirements are different in networks of different levels, the multi-layered IDS system is more suitable for the smart grid. But the deployment of such a system can be time consuming and cost prohibitive without a careful design and planning. In order to decrease the energy cost and processing time of the communication nodes, as well as improving the efficiency, the trust systems are embedded into the communication nodes, and the nodes with the trust systems can be seen as the trust nodes. The trust nodes can be considered as the combination of the firewall, and/or the intrusion detection systems.

Since it is inefficient and expensive to deploy the trust system in each node, the appropriate approach is to use a limited number of trust nodes, which can both ensure the security of the whole communication network of the smart grid, and decrease the overall cost of the system.

Thus the objective is then turned into optimizing both the static placement of the trust nodes and the dynamic routing of communicating nodes in the smart grid network. As in the environment of the smart grid communication

system, the communication nodes should be small formed, such as carrying only a small battery, or owning limited energy and bandwidth so that they can be applied unobtrusively.

What's more, the same routing mechanism shall have the ability to discover the status of the trust nodes and recover from failures of trust nodes and communicating nodes. Without the intelligence in the routing algorithm, damages of the communication nodes, especially the trust nodes may bring paralysis to the whole network. It is crucial that the nodes be able to communicate with each other by alternative routes while keeping the least cost on the communication.

The Smart grid designed for the future electricity system encompasses many of these solutions and technologies. It empowers energy consumers as well as utilities to gain better control over energy consumption.

However, it seems that these are all impossible with-out considering the key role of communication technology. In fact, various communication technologies have the potential to revolutionize today's grid and expedite renewable energy projects.

Smart Grid can be described as an energy network, a network just like the internet. Rather than downloading and uploading data, customers will download and upload electricity. Rather than having a modem indicating how many megabytes of data downloaded or uploaded, customers will have smart meters showing the kilowatts they used or generated and the price according to the time of use. Smart Grid is information technology infra-structure meeting electrical infrastructure to satisfy future energy needs; it will combine the maturity of the electric grid with the efficiency, connectivity, and cost gains brought about by information technology

This approach aims at addressing the problem by focusing on these important aspects of the trust system deployment: 1) static trust node placement, 2) dynamic optimal communication between the selected nodes, and 3) a routing algorithm which is fault-tolerant and cost-sensitive. A three-layer distributed intrusion detection system architecture we proposed in is used as the trust system to be deployed in the smart grid network; in particular, it is used to locate the trust nodes and implement the optimal routings.

Integrated, high performance, highly reliable, scalable, ubiquitous, and secure-these are the characteristics de-scribing the smart grid communication network. The communication network will be responsible for gathering and routing data, monitoring all nodes and acting upon the data received.

## II. Related Work

In the modern trend of network architecture raises so much of challenges in the transmission medium which includes the data secrecy, transmission of packets, traffic, congestion, and so on. The regular network medium shares the packet to the destination in the asynchronous manner. The possibility of data loss occurs in each and every transaction, so the sender or client does not guaranteed about the data reached into the destination. It requires lots and lots of time and cost to retransmit the packet to the destination.

Adaptive decisions are made solely based on the long-term average channel conditions instead of fast channel fading. Specifically channel parameters are replaced by their mean values, resulting in a deterministic rather than stochastic optimization problem. By doing so, quality-of-service (QoS) can only be guaranteed in a long-term average sense, since the short-term fluctuation of the channel is not considered in the problem formulation. With the increasing popularity of wireless applications, however, there will be more and more inelastic traffic that require a guarantee on the minimum short-term data rate. As such, adaptation schemes based on average channel conditions cannot provide a satisfactory QoS.

### *A. SET PACKING ALGORITHM*

Set packing is a classical NP-complete problem in computational complexity theory and combinatory, and was one of the NP-complete problems. Suppose we have a finite set S and a list of subsets of S.

Then, the set packing problem asks if some k subsets in the list are pair wise disjoint (in other words, no two of them intersect).

### *B. OPTIMAL ROUTING ALGORITHM*

There are many optimal routing algorithms are available to provide the path between source and destination. Especially the Dijkstra's algorithm, conceived by Dutch computer scientist is a search algorithm that solves the single-source shortest path problem for a graph with non-negative edge path costs, producing a shortest path tree. This algorithm is often used in routing and as a subroutine in other graph algorithms.

### *C. HEURISTIC ALGORITHM*

In computer science, artificial intelligence, and mathematical optimization, a heuristic is a technique designed for solving a problem more quickly when classic methods are too slow, or for finding an approximate solution when classic methods fail to find any exact solution. This is achieved by trading optimality, completeness, accuracy, or precision for speed.

The objective of a heuristic is to produce quickly enough a solution that is good enough for solving the problem at hand. This solution may not be the best of all the actual solutions to this problem, or it may simply approximate the exact solution. But it is still valuable because finding it does not require a prohibitively long time.

Heuristics may produce results by themselves, or they may be used in conjunction with optimization algorithms to improve their efficiency (e.g., they may be used to generate good seed values).

For the real-time search type of routing strategies, if the initial estimates are close to optimal, the actual time of

delivering a single packet and the actual time of convergence to optimal routes are close to the minimum.

For search-based routing, the initialization phase is to establish a neighborhood structure, i.e., each node has a list of
its neighbors. To do so, each node sends out a few "hello" packets with its attributes. If the destination is known at initialization time, which is common for applications of sensor
networks (e.g., a base station), initialization can be instead a flooding from the destination. Each packet carries a Q-value of the node, and Q-values are propagated through the network.

### *D. FAULT TOLERANCE AND RECOVERY ALGORITHM*

Fault Tolerant was designed as a solution to allow applications different methods to handle process failures beyond simple check-point restart schemes. The initial implementation of FT included a robust heavy weight system state recovery algorithm that was designed to manage the membership of communicators during multiple failures. The algorithm and its implementation although robust, was very conservative and this effected its scalability on both very large clusters as well as on distributed systems.

## III. SYSTEM ARCHITECTURE

Client-server computing or networking is a distributed between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

Adaptive system exploits time, frequency, and multi-user diversity by quickly adapting sub carrier allocation (SCA) to the instantaneous channel state information (CSI) of all users. Such "fast" adaptation suffers from high computational complexity, since an optimization problem required for adaptation has to be solved by the base station (BS) every time the channel changes. Considering the fact that wireless channel fading can vary quickly. Implementation of fast adaptive system becomes infeasible for practical systems, even when the number of users is small. Recent work on reducing complexity of fast adaptive systems includes more over; fast adaptation requires frequent signaling between the BS and mobile users in order to inform the users of their latest allocation decisions. The overhead thus incurred is likely to negate the performance gain obtained by the fast adaptation schemes.

A scheme that aims at maximizing the long-term system throughput while satisfying with high probability the short-term data rate requirements. We design the adaptive Smartgrid Network system based on chance constrained programming techniques. Our formulation guarantees the short-term data rate requirements of individual users except in rare occasions. To the best of our knowledge, this is the first work that uses chance constrained programming in the context of resource allocation in wireless systems.

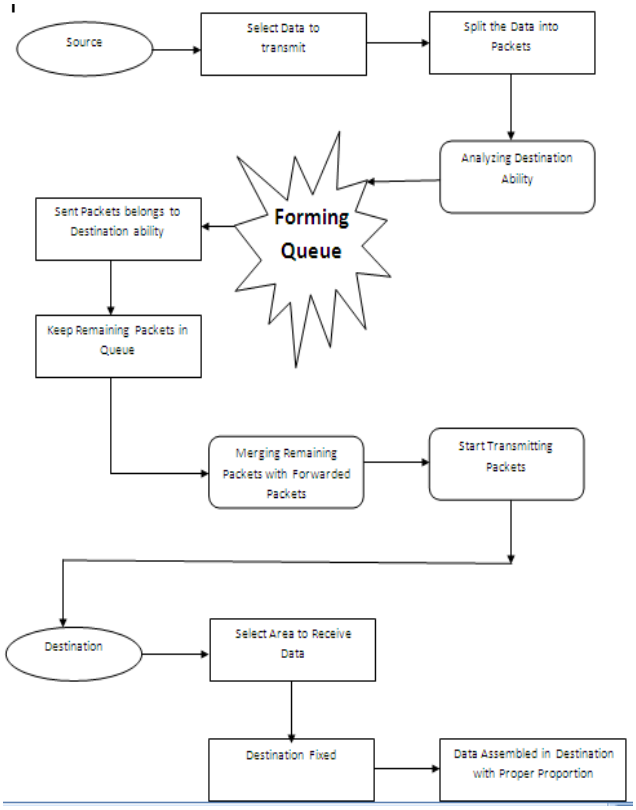
We exploit the special structure of the probabilistic constraints in our problem to construct safe tractable constraints (STC) based on recent advances in the chance constrained programming.

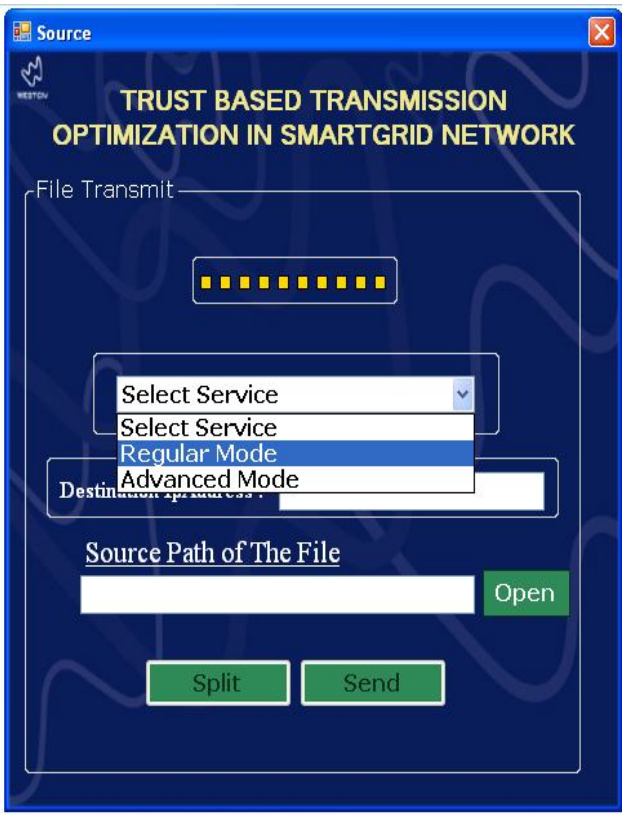
This implies that channel conditions over the adaptation win do ware uncertain at the decision time, thus presenting a new challenge in the design of Smartgrid network architecture schemes. An important question is how to find a valid allocation decision that remains optimal and feasible for the entire adaptation window. Such a problem can be formulated as a stochastic programming problem, where the channel coefficients are random rather than deterministic. Therein, adaptation decisions are made solely based on the long-term average transmission conditions instead of fast channel fading.

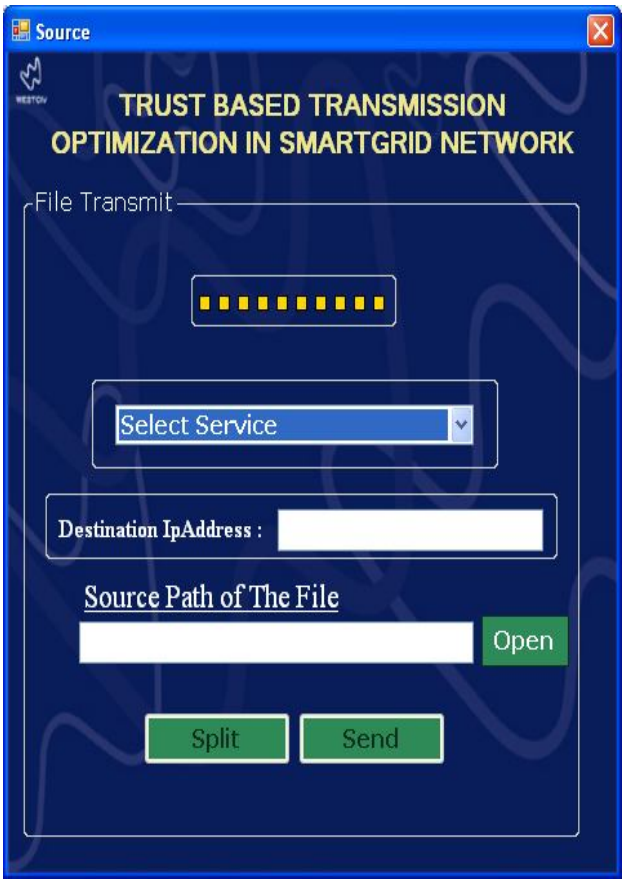
Specifically random channel parameters are replaced by their mean values, resulting in a deterministic rather than stochastic optimization problem. By doing so, quality-of-service (QoS) can only be guaranteed in a long-term average sense, since the short-term fluctuation of the system is not considered in the problem formulation. With the increasing popularity of wireless multimedia applications less multimedia applications, however, there will be more and more inelastic traffic that require a guarantee on the minimum short-term data rate. As such, adaptation schemes based on average transmission conditions cannot provide a satisfactory QoS.

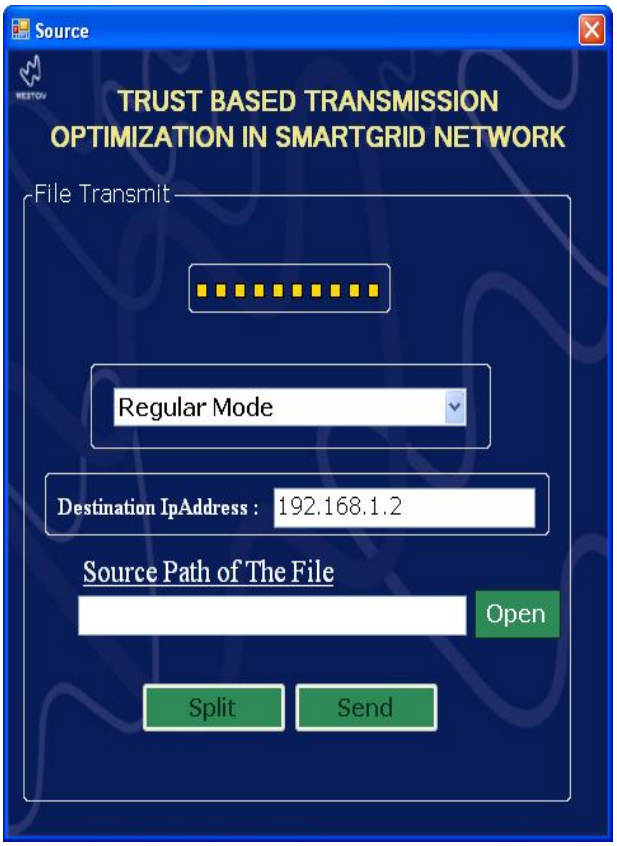
This network architecture scheme that can achieve a throughput close to that of fast adaptive schemes, while significantly reducing the computational complexity and control signaling overhead in regular network architecture. Our scheme can satisfy user data rate requirement with high probability. This is achieved by formulating our problem as a stochastic optimization problem. Based on this formulation, we design a polynomial-time algorithm for sub carrier allocation in smartgrid architecture.

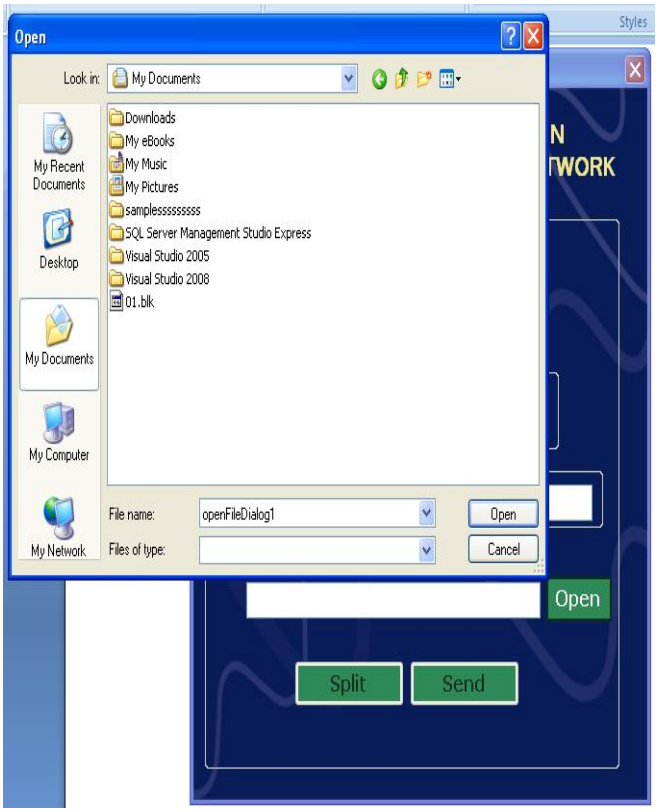
We have only considered fast as one of the typical formulations of fast methodology in our comparisons. However, we should point out that there are some works on smartgrid systems which impose less restrictive constraints on user data rate requirement. Considered average user data rate constraints which exploits time diversity to achieve higher spectral efficiency.

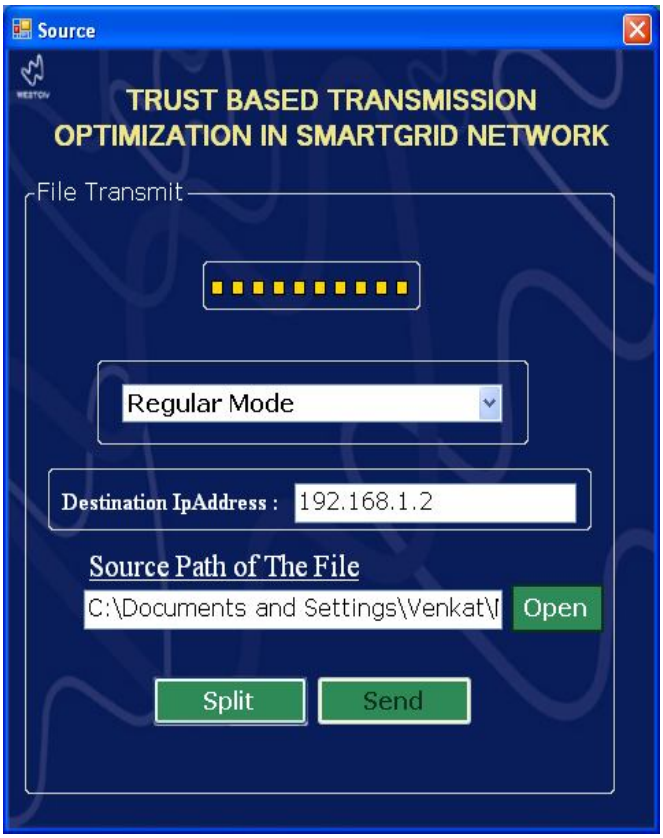

Source
Select Data to transmit
Split the Data into Packets
Analyzing Destination Ability
Forming Queue
Sent Packets belongs to Destination ability
Keep Remaining Packets in Queue
Merging Remaining Packets with Forwarded Packets
Start Transmitting Packets
Destination
Select Area to Receive Data
Destination Fixed
Data Assembled in Destination with Proper Proportion


Source
TRUST BASED TRANSMISSION OPTIMIZATION IN SMARTGRID NETWORK
File Transmit
Select Service
Select Service
Regular Mode
Advanced Mode
Source Path of The File
Open
Split
Send


Source
TRUST BASED TRANSMISSION OPTIMIZATION IN SMARTGRID NETWORK
File Transmit
Select Service
Destination IpAddress :
Source Path of The File
Open
Split
Send


Source
TRUST BASED TRANSMISSION OPTIMIZATION IN SMARTGRID NETWORK
File Transmit
Regular Mode
Destination IpAddress :
192.168.1.2
Source Path of The File
Open
Split
Send




## IV. Conclusion

To avoid the difficulty of network oriented issues, a methodology is to formulate for safe tractable constraints for the problem based on recent advances in chance constrained programming. A polynomial-time algorithm is developed for computing an optimal solution to the reformulated problem. The result reduces both computational Cost and control signaling overhead when compared with the conventional transmission. This work can be viewed as an initial attempt to apply the chance constrained transmission methodology to wireless system designs. Given that most wireless systems can tolerate an occasional dip in the quality of service, we hope that this methodology will find further applications in wireless communications.

## References

[1] J. M. C. Gonzalez, K. M. Hopkinson, G. H. Greve, M. D. Compton, J.Wilhelm, S. H. Kurkowski, and R. W. Thomas, "Optimization of trust system placement for power grid security and compartmentalization,"IEEE Trans. Power Syst., vol. 26, no. 2, pp. 550–563, 2011.

[2] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," IEEE Trans.Power Del., vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy Mag., vol. 7, no. 3, pp. 75–77, May 2009.

[4] G. N. Ericsson and A. Torkilseng, "Management of information security for an electric power utility—on security domains and use of ISO/IEC17799 standard," IEEE Trans. Power Del., vol. 20, no. 2, pp. 683–690, Apr. 2005

[5] G. N. Ericsson, "Classification of power systems communications needs and requirements: Experiences from case studies at Swedish national grid," IEEE Trans. Power Del., vol. 17, no. 2, pp. 345–347, Apr. 2002.

[6] S. B. Jeong, Y.Woo, and S. Kim, "An effective placement of detection systems for distributed attack detection in large scale networks," in Proc. WISA 2004, 2004, LNCS 3325, pp. 204–210.

[7] R. Chandra, L. Qiu, K. Jain, and M. Mahdian, "Optimizing the placement of internet TAPs in wireless neighborhood networks," in Proc. ICNP, Oct. 2004, pp. 271–282.

BIOGRAPHY

**M.Ramasaravanan** is currently a PG scholar in Computer Science Engineering from the Department of Computer Science and Engineering at Chendhuran College of Engineering and Technology, Pudukkottai. He received his Bachelor Degree in Computer Science Engineering from Shanmuganathan Engineering College. Pudukkottai and Tamilnadu. His Research areas include grid computing, cloud computing and wireless sensor network security.

**M.Kirithikadevi** is currently working as an Asst. Prof. from the Department of Computer Science and Engineering at Chendhuran College of Engineering and Technology, Pudukkottai. She received his Bachelor Degree from Bharathidasan University Trichy and Master Degree in Computer Science & Engineering from Anna University, Trichy. She Published 1 national Conference. Her main research interests lie in the area of wireless sensor networks