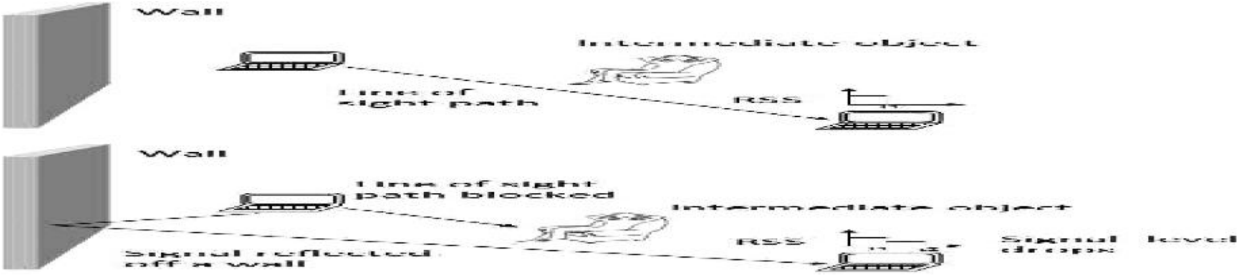
# PROJECTS IN NS 2

## IEEE PROJECTS 2013 – 2014

## NS 1. SECRET KEY EXTRACTION FROM WIRELESS SIGNAL STRENGTH IN REAL ENVIRONMENTS

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios. In the **PROPOSED SYSTEM**, Source Sends a Data to the Destination, Data is forwarded to the intermediate Nodes one by one, based on Received Signal Strength (RSS) Secret Key is Generated which is passed to both the Source and the Destination. A Random Key is parsed by both Source and Destination which is exchanged between both for Verification. Both of them Generates Hash Key of the Secret Keys, which is also Verified by both of them only then the Data can be viewed by the Destination. **MODIFICATION** that we propose, is to have a strong Verification Scheme in the Destination End. Destination's User Name, Password, IP Address, Primary Key, Parsed Random Key, Hash Value of Secret Key, Decryption Key to open the Data, as well as Secondary Key for changing the Primary key is verified for the Secured Communication of Data between Source and any Destination.

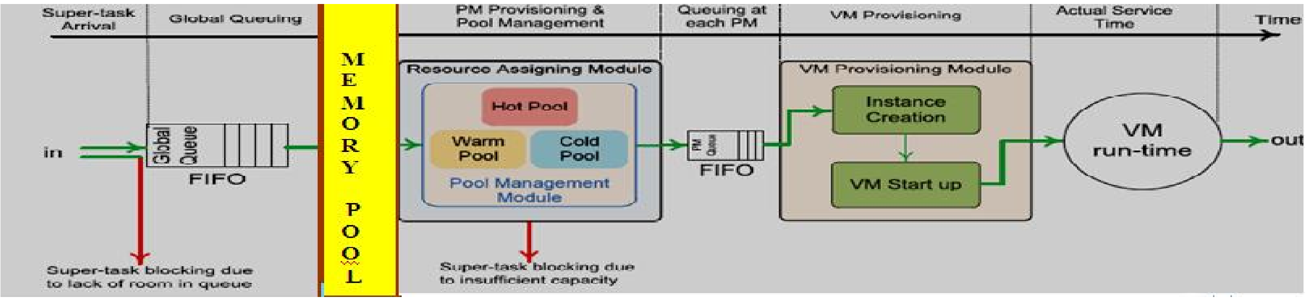
**ALGORITHM / METHODOLOGY:** **Key Extraction Algorithm**

**DOMAIN: Mobile Computing**

**IEEE REFERENCE: IEEE Transactions** on Mobile Computing, 2013

## NS 2. ANALYSIS OF A POOL MANAGEMENT SCHEME FOR CLOUD COMPUTING CENTERS

## ARCHITECTURE DIAGRAM



**DESCRIPTION :** In the **EXISTING SYSTEM,** Service availability and response time are two important quality measures in cloud's users perspective. A monolithic model may suffer from intractability and poor scalability due to large number of parameters. In the **PROPOSED SYSTEM,** User's Request is sent to the Global Queue and then to the Resource Assigning Module via FIFO Model. Then we Assign 3 Types of System. First is HOT, in which the Servers will be handling the Jobs Currently, Second is WARM, in which the Servers are kept in Ideal State, then Finally Cold, in which Servers are Turned Off State. Initial Request is send to HOT – Servers, if those Servers are Busy then the Request is forwarded to Warm – Servers, then finally if required to Cold – Servers if both the Hot and Warm Servers are Busy. In the **MODIFICATION** Process, We Develop a Cache Memory Provision, in which Requested Data is Stored in Memory Pool for a Period of Time. If same Data is requested by another user system Verifies the Data is Stored in the Memory pool, then the Data is downloaded from the Memory Pool itself and not processed by the Request Assigning Module (RAM).

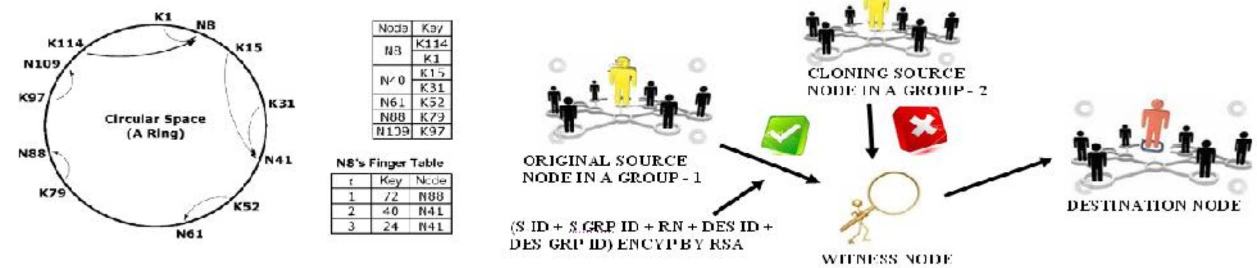
**ALGORITHM / METHODOLOGY: Successive Substitution Method**

**DOMAIN: CLOUD COMPUTING**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems**, 2013**

## NS 3. ON THE NODE CLONE DETECTION IN WIRELESS SENSOR NETWORKS

## ARCHITECTURE DIAGRAM



| Node | Key |
|---|---|
| N8 | K114<br>K1 |
| N40 | K15<br>K31 |
| N61 | K52 |
| N88 | K79 |
| N109 | K97 |

N8's Finger Table

| t | Key | Node |
|---|---|---|
| 1 | 72 | N88 |
| 2 | 40 | N41 |
| 3 | 24 | N41 |

**DESCRIPTION :** In the **EXISTING SYSTEM**, Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. So they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. In the **PROPOSED SYSTEM**, we use two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one is based on a distributed hash table (DHT) in which Chord algorithm is used to detect the cloned node, every node is assigned with the unique key, before it transmits the data it has to give its key which would be verified by the witness node. If same key is given by another Node then the witness node identifies the cloned Node. The second one is based on the Distributed Detection Protocol which is same as DHT, but it is easy and cheaper implementation. Here every node only needs to know the neighbor-list containing all neighbor IDs and its locations. In the **MODIFICATION** Process, we are implementing RDE protocol, by location based nodes identification, where every region/location will have a group leader. The Group leader will generate a random number with time stamp to the available nodes in that location. Witness nodes verify the random number and time stamp to detect the cloned node. The message is also encrypted for security purpose.

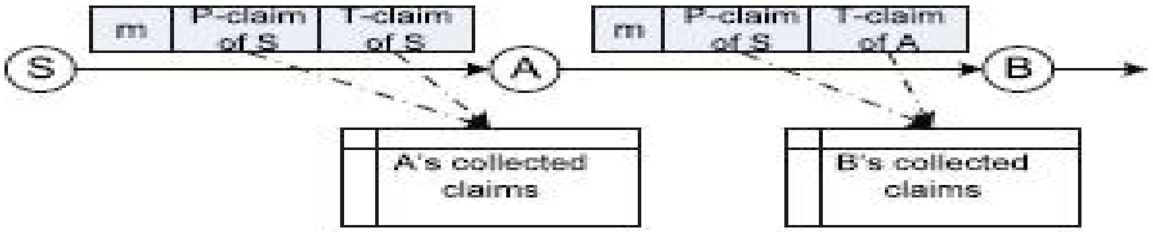
**ALGORITHM / METHODOLOGY: CHORD ALGORITHM**

**DOMAIN: Network Security**

**IEEE REFERENCE: IEEE Transactions** on Networking, **2013**

## NS 4. TO LIE OR TO COMPLY: DEFENDING AGAINST FLOOD ATTACKS IN DISRUPTION TOLERANT NETWORKS

## ARCHITECTURE DIAGRAM



**DESCRIPTION :** In the **EXISTING SYSTEM**, DTNs consist of mobile nodes carried by human beings vehicles etc. when a node receives some packets, it stores in its Buffer and Forwards to another it contacts another. DTNs are vulnerable to flood attacks which would waste Buffer Resources of DTN. In the **PROPOSED SYSTEM**, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval (**P-Claim**). Each node also has a limit over the number of replicas that it can generate for each packet (T-**Claim**) (i.e., the number of nodes that it can forward each packet to). The two limits are used to mitigate packet flood and replica flood attacks, respectively. **MODIFICATION** that we propose is to verify the Content of the Data which is transmitted. Sometimes Attackers would transmit a Worm File within P-Claim & T-Claim.

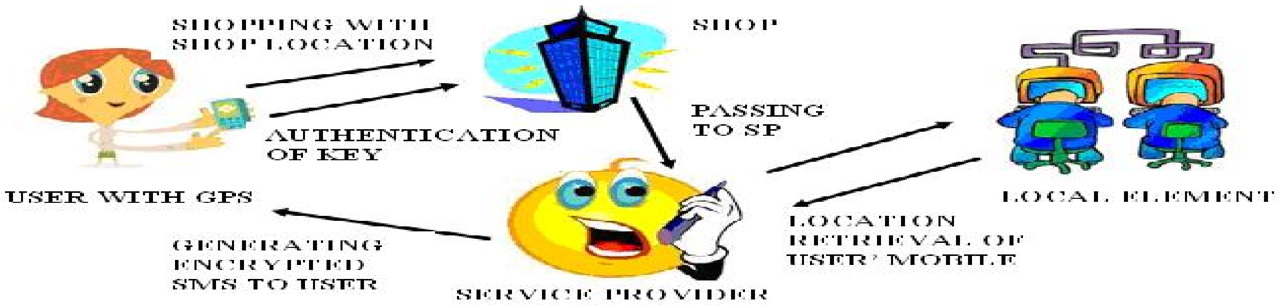
**ALGORITHM / METHODOLOGY: Packet Forwarding Scheme**

**DOMAIN: Network Security**

**IEEE REFERENCE: IEEE Transactions** on Dependable and Secure Computing**, 2013**

## NS 5. LOCATION-AWARE AND SAFER CARDS: ENHANCING RFID SECURITY AND PRIVACY VIA LOCATION SENSING

## ARCHITECTURE DIAGRAM


SHOPPING WITH SHOP LOCATION
SHOP
AUTHENTICATION OF KEY
PASSING TO SP
USER WITH GPS
LOCAL ELEMENT
GENERATING ENCRYPTED SMS TO USER
LOCATION RETRIEVAL OF USER' MOBILE
SERVICE PROVIDER

**DESCRIPTION:** In the **EXISTING SYSTEM**, Credit Card Fraud is the most common occurrence. There is no authenticated step to control Credit Card Fraud in real time. In the **PROPOSED MODEL**, Location based Verification Scheme is implemented by comparing the User's Credit Card Location with the User's Mobile Location. This is very effective to identify the Real User. The **MODIFICATION** we propose is to generate an Encrypted Data to the Real

User's Mobile Number along with the Decrypting Key as SMS only when both the Location of Credit Card and Mobile of the User is Matched. So process would definitely filter credit card fraud totally.

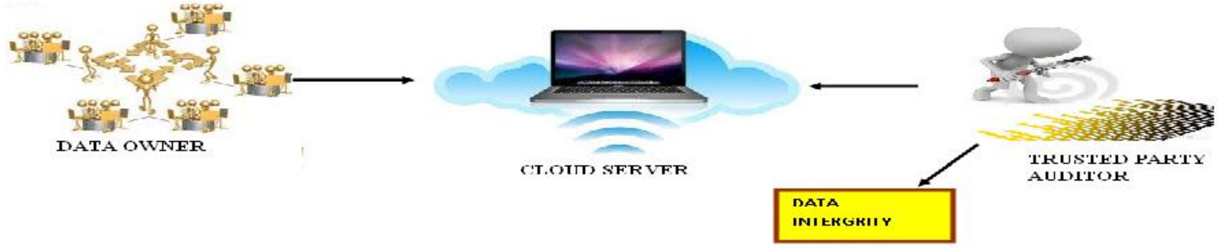
**ALGORITHM / METHODOLOGY: Location Detection Algorithm**

**DOMAIN: Security, Mobile Computing**

**IEEE REFERENCE: IEEE Transactions** on Dependable and Secure Computing**, 2013**

## NS 6. PRIVACY-PRESERVING PUBLIC AUDITING FOR SECURE CLOUD STOREAGE

## ARCHITECTURE DIAGRAM:



**DESCRIPTION:** In the **EXISTING SYSTEM**, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. In the **PROPOSED SYSTEM,** a secure cloud storage system supporting privacy-preserving public auditing. In which the Data owner uploads the data in the Cloud Server and they are allowed to modify the data using the Private Key. The Cloud Sever Stores the data and split those data into the batches using Merkel Hash Tree Algorithm. The TPA will audit the data file that are requested by the Data Owner. The TPA will also audit the multiple files also. In the **MODIFICATION** process, TPA will also audit the files randomly also; even the files which are not requested by the data owner.

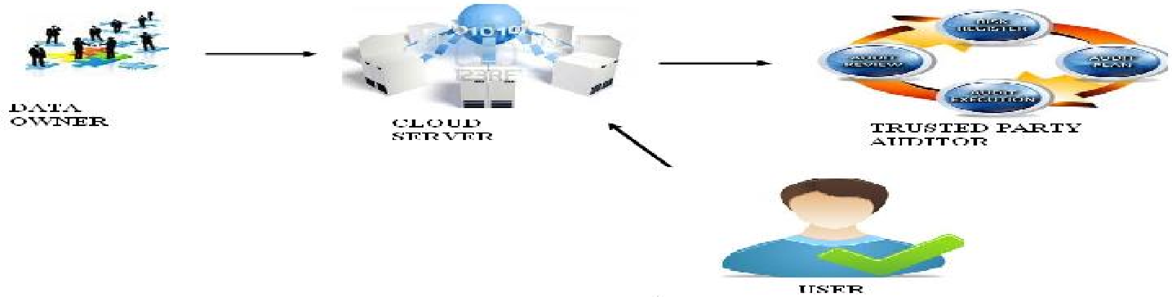
**ALGORITHM / METHODOLOGY: Merkle Hash Tree**

**DOMAIN: Cloud Computing, Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Computers**, 2013**

## NS 7. ENABLING DYNAMIC DATA AND INDIRECT MUTUAL TRUST FOR CLOUD COMPUTING STORAGE SYSTEM

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, there is no big implementation towards security for the data that are stored in the Cloud Server. So the trust worthiness to store the data in the cloud servers is decreased rapidly. In the **PROPOSED SYSTEM,** the data owner uploads the data in the Cloud server in encrypted format. The data in the Cloud Server will be hashed and the hashed values are given to the TPA for auditing purpose. The data will audited by the TPA

Using Merkle Hash Tree technique. If the data owner updates the data the corresponding hash values are also updated. If the authorized user wants to access the data, they (user) have to provide the corresponding decryption key. In the **MODIFICATION** Process, while auditing the data the TPA has to audit it from the IP address in which they (TPA) have registered. Accessing from any other system is not allowed.

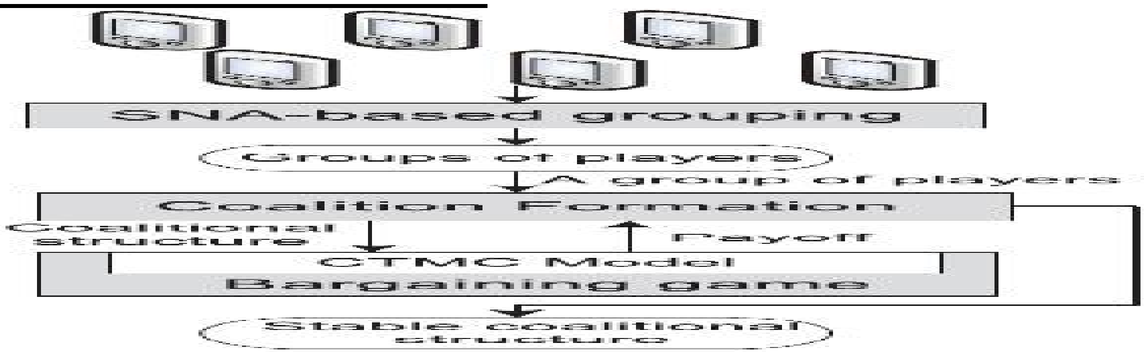
**ALGORITHM / METHODOLOGY:** AES

**DOMAIN: Cloud Computing, Security**

**IEEE REFERENCE: IEEE Transactions** on Dependable and Secure Computing, 2013

## NS 8. COOPERATIVE PACKET DELIVERY IN HYBRID WIRELESS MOBILE NETWORKS: A COALITIONAL GAME APPROACH

## ARCHITECTURE DIAGRAM



**DESCRIPTION :** In the **EXISTING SYSTEM**, Mobile Nodes (e.g., vehicles) in the same group for Data Exchange is always very difficult, Costly, Time Delay in Delivery. We consider the problem of cooperative packet delivery to mobile nodes in a hybrid wireless mobile network. In the **PROPOSED SYSTEM**, a solution is deployed based on a coalition formation among mobile nodes to cooperatively deliver packets among these mobile nodes in the same coalition. Mobile nodes make a decision to join or to leave a coalition based on their individual payoffs. The individual payoff of each mobile node is a function of the average delivery delay for packets transmitted to the mobile node from a base station and the cost incurred by this mobile node for relaying packets to other mobile nodes. Markov chain model is formulated and the expected cost and packet delivery delay. A bargaining game is used to find the optimal helping probabilities. In the **MODIFICATION PROCESS,** Trustworthiness along with the Payoff of a Mobile Node is also considered before forwarding a Data to any Mobile Node.

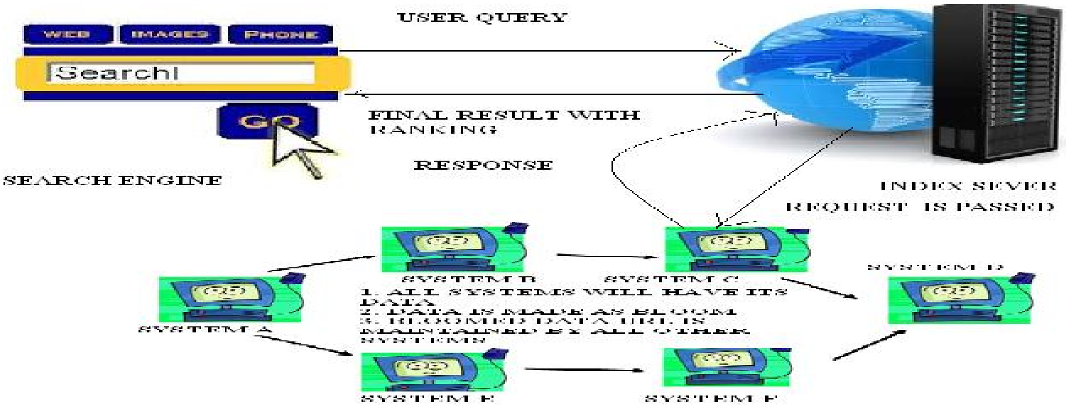
**ALGORITHM / METHODOLOGY: AES**

**DOMAIN: Mobile Computing**

**IEEE REFERENCE: IEEE Transactions** on Mobile Computing**, 2013**

## NS 9. DESIGN OF A MULTIPLE BLOOM FILTER FOR DISTRIBUTED NAVIGATION ROUTING

## ARCHITECTURE DIAGRAM



**<u>DESCRIPTION:</u>** In the **EXISTING SYSTEM**, Single Keyword based Approach is used to be Mapped with the Set of Document in the Nodes. In the **PROPOSED MODEL** Multi Keyword Search is Applied Where lots of Virtual Server is Deployed with Index Information of all the Documents. Peers will contain the Documents. Search is posted to Index Server Which Manages the Address Space of Virtual Server and Identifies the Data Contains Peer List. Best Records are Retrieved Using Ranking Process.

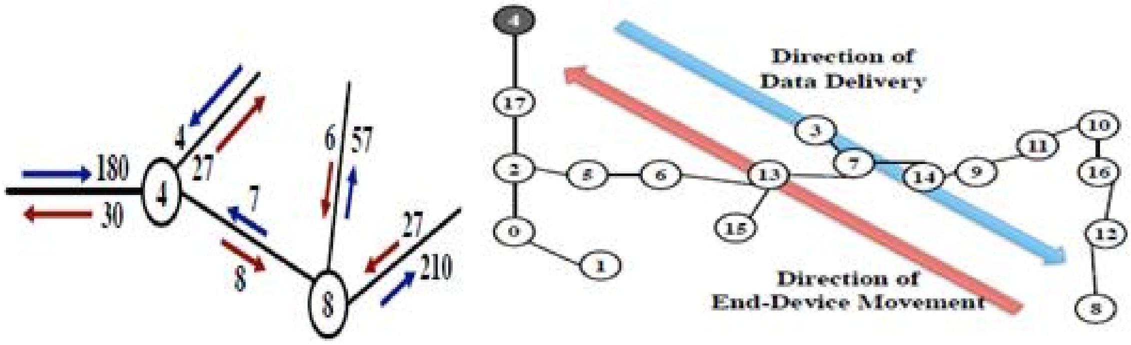
**ALGORITHM / METHODOLOGY:** **Bloom Filter, Stemming, Ranking, Scoring**

**DOMAIN: Data Mining**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Systems, Man And Cybernetics: Systems**, 2013**

## NS 10. A MOBILITY AWARE NODE DEPLOYMENT AND TREE CONSTRUCTION FRAMEWORK FOR ZIGBEE WIRELESS NETWORKS

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM,** the ZigBee networks often uses a tree topology is  to construct a WSN for data delivery applications. However, delivery failures occur constantly in ZigBee wireless applications due to node movements and also utilizes large amount of Resources. In the **PROPOSED SYSTEM**, the positions of the routers and design the tree topology so that most movements are directed towards the root of the tree. We first deploy the Nodes in a Network (**ZND**), then Calculate the Maximum In degree Node to find out Coordinator Node (**ZCD**), and finally Tree Construction in order to send the Data to the Destination (**ZTC**). In the **MODIFICATION PROCESS**, We are implementing the capacity calculation if In Degree node numbers are same in any two Nodes. We are not implementing Zigbee Network in this Project. We implement in Wireless Environment using Wireless LAN.

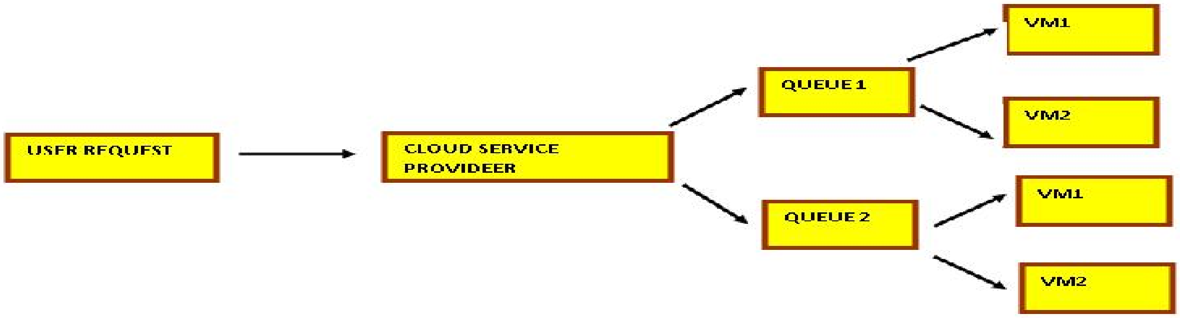
**ALGORITHM / METHODOLOGY:** ZND, ZTC, ZCD

**DOMAIN: Mobile Computing**

**IEEE REFERENCE: IEEE Transactions** on Mobile Computing, **2013**

## NS 11. IMPROVING NETWORK I/O VIRTUALIZATION FOR CLOUD COMPUTING

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, each Cloud Computing User (CCU) requests Cloud Computing Service Provider (CCSP) for use of resources. If CCU finds the server busy, then the user has to wait till the current user completes the job. This may result in increase of queue length as well as waiting time, which may lead to request drop. In the **PROPOSED SYSTEM**, we use a finite Multi Server Queuing Model with Queue Dependent heterogeneous servers where the applications are modeled as queues and the virtual machines are modeled as Service Providers. Request from the User is send to the CSP, where Dispatcher Pool will Redirect to Queue 1 or 2 alternatively and Throughput is calculated in the Virtual Machines for effective Data Processing. In the **MODIFICATION PROCESS**, We assign priority Model for Processing Important Data based High / Medium / Low Priority Model.

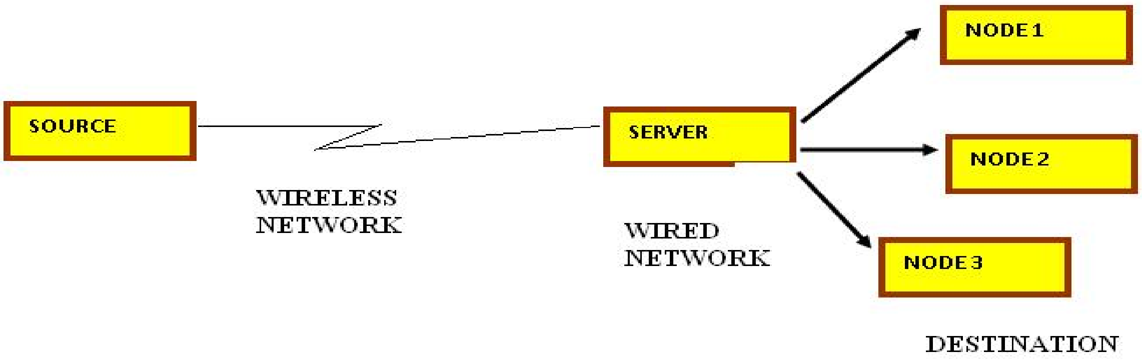
**ALGORITHM / METHODOLOGY:** **Placement, Load Balancing**

**DOMAIN:** **Cloud Computing**

**IEEE REFERENCE:** **IEEE Transactions** on Parallel and Distributed Systems, 2013

# NS 12. A SIMULATION PLATFORM FOR ZIGBEE UMTS HYBRID NETWORKS

## ARCHITECTURE DIAGRAM



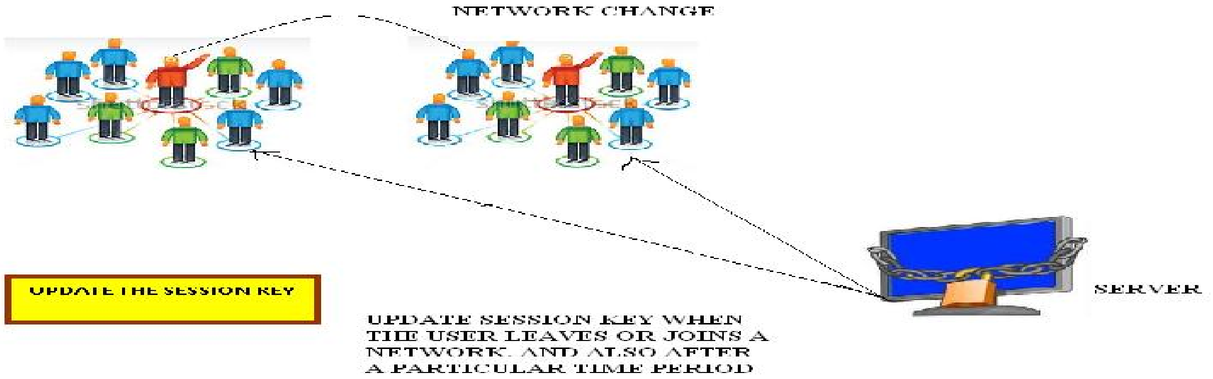
**DESCRIPTION:** In the **EXISTING SYSTEM**, the zigbee networks and UMTS networks are working separately. There is no implementation to merge the two networks and creating a new network for data processing. In the **PROPOSED SYSTEM**, we will combine the two networks and develop the hybrid network in which the data is transferred from source node (Wireless) to the destination node via the server which is connected through LAN. In the **MODIFICATION** Process, We are not implementing Zigbee Network in this Project. We implement in Wireless Environment using Wireless LAN.

**ALGORITHM/METHODOLOGY: Ad hoc On Demand Distance Vector**

**DOMAIN: Wireless Networks**

**IEEE REFERENCE: IEEE Paper** on Communications, **2013**

## NS 13. A SECURE PROTOCOL FOR SPANTENOUS WIRELESS ADHOC NETWORK CREATION


NETWORK CHANGE
UPDATE THE SESSION KEY
SERVER
UPDATE SESSION KEY WHEN THE USER LEAVES OR JOINS A NETWORK. AND ALSO AFTER A PARTICULAR TIME PERIOD

## ARCHITECTURE DIAGRAM

**DESCRIPTION:** In the **EXISTING SYSTEM**, there is no proper security measures were implemented in Wireless Ad-hoc Networks while joining new nodes and exchanging data. In the **PROPOSED SYSTEM,** if a new node want to with the existing node, the new node will send the request to the existing node. Based on the request, the existing node will send its public key to the new node. After that the new node and existing node will share their public and private key components to authenticate each other. For security purpose the data will be Encrypted during transmission. The Certificate Authority is used to authorize the node when it wants joins another node. Secret key is generated, which is used to share the data and it will be changed at a particular period of time. In the **MODIFICATION** process, the secret key is also changed when the node joins a network and leaves a network. So that we can increase the level of security.

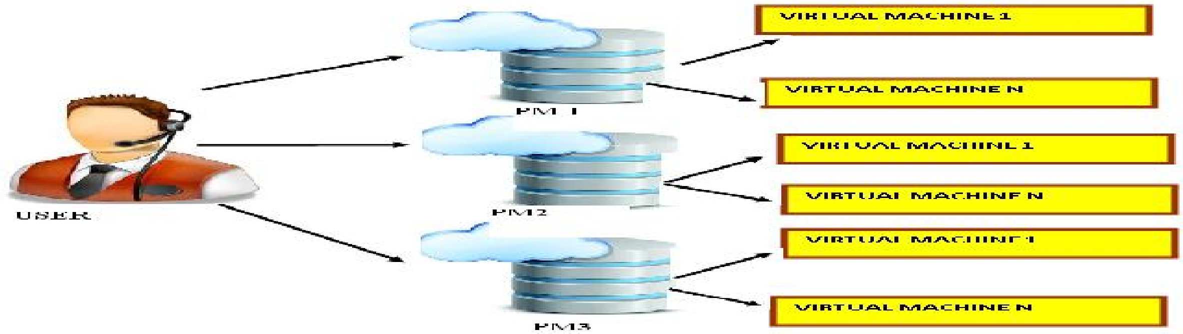
**ALGORITHM / METHODOLOGY:** **AES, RSA**

**DOMAIN: Wireless Ad-hoc Networks**

**IEEE REFERENCE: IEEE Transactions** on Parallel and Distributed Systems, 2013

## NS 14. DYNAMIC RESOURCE ALLOCATION USING VIRTUAL MACHINES FOR CLOUD COMPUTING ENVIRONMENTS

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, resource allocation schemes were not effectively implemented in Cloud environment. So processing the users request is a time consuming process. Also there is no proper methodology to save the energy while less number of jobs are being processed. .In the **PROPOSED SYSTEM,** we are using predictor which predicts the resources that is utilized by the physical machine. Every physical machine is splitted into number of Virtual machines. Job is allocated to each virtual machine, if all the virtual machines is occupied with work, then the machine is named as HOTSPOT so that the work is allotted to another Virtual machine of the another physical machine. CLODSPOT is used to turned off the physically machines to save the power, if all the Virtual Machine has finished their work. Green Computing used to controls the power. In **MODIFICATION** part that we propose in this Project is to calculate the load that requires handling the job.

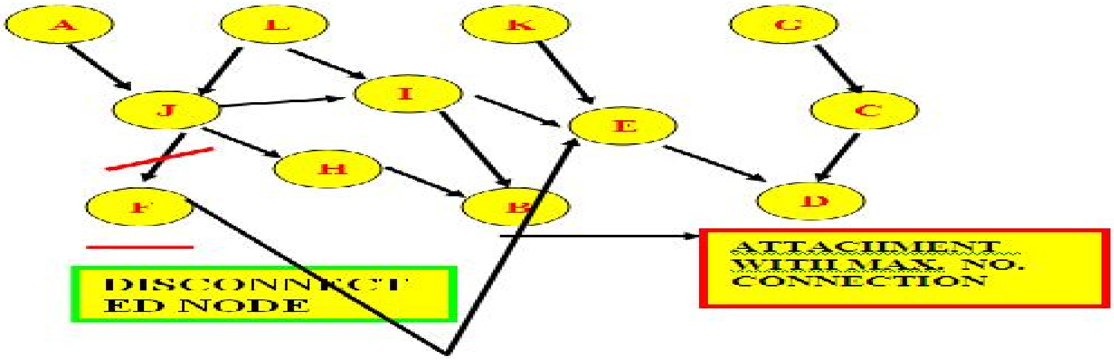
ALGORITHM / METHODOLOGY: **Sknewness, Green Computing**

**DOMAIN: Cloud Computing, Networking**

**IEEE REFERENCE: IEEE Transactions** on Parallel and Distributed Systems, 2013

## NS 15. TULA: BALANCING ENERGY FOR SENSING AND COMMUNICATION IN A PERPETUAL MOBILE SYSTEM

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, the Energy Harvesting variability and the unpredictable network connectivity make mobile networks difficult. In the **PROPOSED SYSTEM,** TULA which has three components namely Adaptive sensing, DTN Routing Algorithm, Rate Allocator. Adaptive Sensing changes their sensing rates according to their energy conditions of the nodes. DTN Routing identifies by which path the data is to be transmitted to the destination node. At last Rate Allocator is used to transmit the data at the specified rate. If a particular data is transferred to the bottom of a leaf node, the root node should maintain a replica in order to avoid same query and data transfer. In the **MODIFICATION** process, if leave node was disconnected from a network, the node will be joined with the highest connectivity node. So that we can avoid node failure.

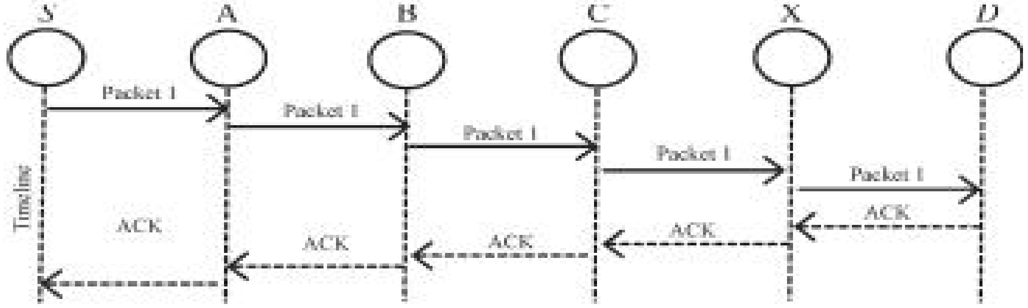
**ALGORITHM / METHODOLOGY: DTN ROUTING**

**DOMAIN: MOBILE COMPUTING**

**IEEE REFERENCE: IEEE Transactions** on Mobile Computing. 2013

## NS 16. EAACK—A SECURE INTRUSION-DETECTION SYSTEM FOR MANETS

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, due to the lack of security in the MANETs, Because of the Open medium and distribution of the nodes in various locations, makes MANET vulnerable to malicious to attackers**.** In the **PROPOSED SYSTEM,** The data is send to the Destination Node via intermediate nodes in the Encrypted format. Each node has to pass the Acknowledgement after the Receiving of the data. If any of the nodes didn't pass the Acknowledgement, then the Source Node will send the data to the Destination via another Route. Then the MRA is filed. If the Destination claims Duplication of the Data then Source will find the Misbehavior. If there is no Data, then resend the Data is stored in the Destination, again the packet dropped node is considered as attacker, and then the node is removed from the network. In the **MODIFICATION** Process, the server will identify the buffer level of the intermediate nodes; If the packets are dropped due to inadequate of Space/Memory then the node is not considered as an attacker.

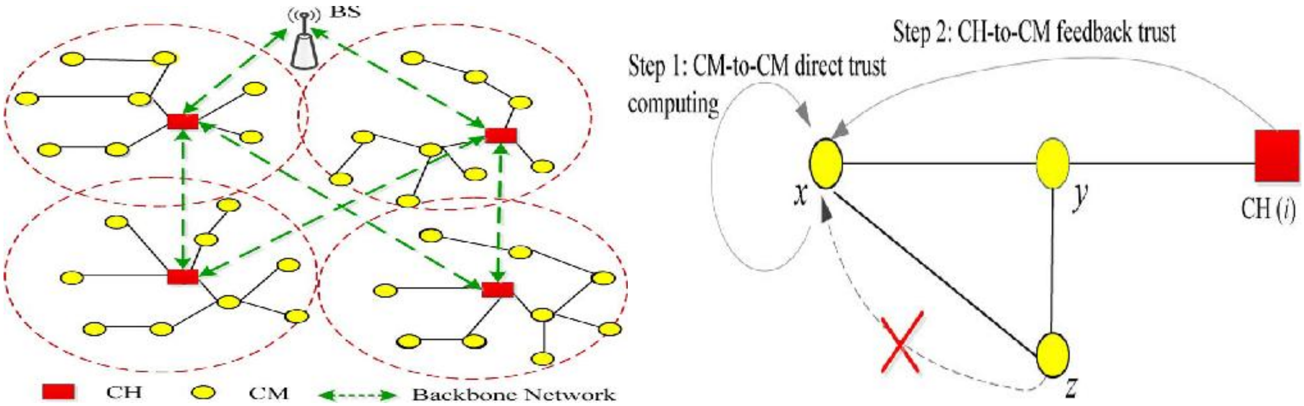
**ALGORITHM / METHODOLOGY:** Digital signature verification

**DOMAIN: MOBILE COMPUTING**

**IEEE REFERENCE: IEEE Transactions** on Industrial Electronics**, 2013**

## NS 17. LDTS: A LIGHTWEIGHT AND DEPENDABLE TRUST SYSTEM FOR CLUSTERED WIRELESS SENSOR NETWORKS

## ARCHITECTURE DIAGRAM


BS
CH
CM
Backbone Network
Step 2: CH-to-CM feedback trust
Step 1: CM-to-CM direct trust computing
x
y
z
CH (i)

**DESCRIPTION:** In the **EXISTING SYSTEM**, In the wireless Sensor Networks are incapable of satisfying the resource efficiency and trust system because of the high overhead and low dependability. In the **PROPOSED MODEL**, Light Weight and Dependable Trust

System (LDTS) is used which employees the Clustering Algorithm. The nodes are registered in every network and the Cluster Head is identified based on the Number of connections. We use feedback model to identify the best and most dependable route to reach the destination. The members are CM and their Heads are CH. Base Station acts as an Intermediate Node to Monitor the Data Transaction. BS will ask to give Feedback about their Neighbors in order to identify Trustworthiness. **MODIFICATION** that we propose is Packets are encrypted at the source.

**ALGORITHM / METHODOLOGY:** **clustering algorithm**

**DOMAIN**: **Mobile Computing**

**IEEE REFERENCE: IEEE Transactions** on Information Forensics and Security**, 2013**

## NS 18. PREVENTIVE ALTERNATE PATH ROUTING ALGORITHM AGAINST INTRUSION IN SENSOR AREA NETWORK

## ARCHITECTURE DIAGRAM

**DESCRIPTION:** In **EXISTING SYSTEM**, the hackers perform the Man in Middle attack by identifying the shortest path and compromising them. So that they can hack the confidential data in the Wireless Sensor Networks. In the **PROPOSED SYSTEM**, we implement the Alternate Path Routing Algorithm to prevent the Intrusion. Here first we'll calculate the available path when a Source node is sending the data to the Destination. From the available path we can randomly choose the path to send the data to destination node except using the Shortest Path in the Network. So that the attackers are not able to find identify the data transmission path.

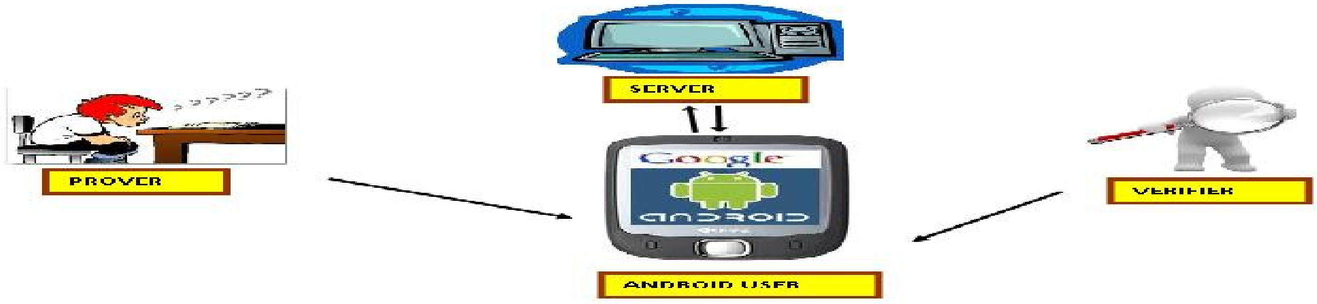
**ALGORITHM / METHODOLOGY:**

**DOMAIN: NETWORKING**

**IEEE REFERENCE: International Journal of** Computer Theory and Engineering**, 2013**

## ANS2 1. SECURED LOCATION TRACKING WITH TAMPER PROOF USER LOCATION IDENTIFICATION TOWARDS EFFECTIVE AND RESTRICTED DATA ACCESS

## ARCHITECTURE DIAGRAM



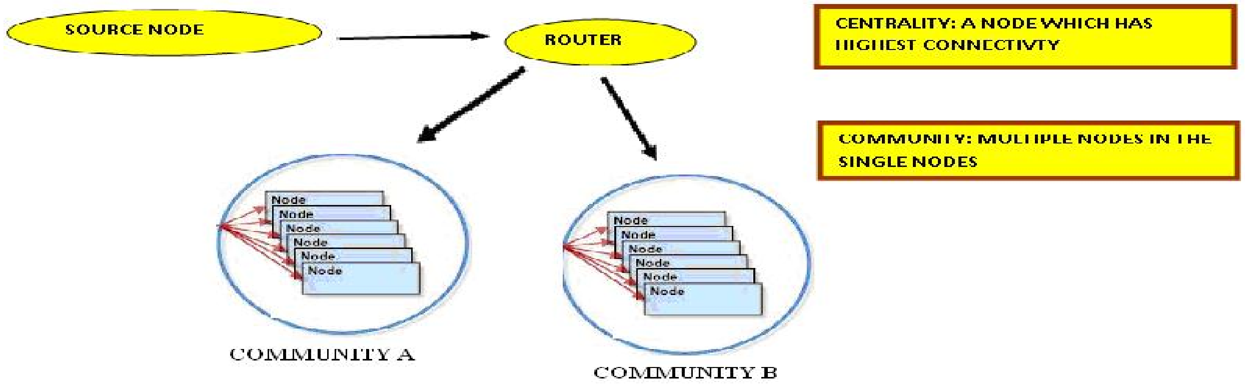
**DESCRIPTION :** In the **EXISTING SYSTEM,** user Location is usually tracked using GPS, but GPS cannot be used or the internal tracking. So there is no effective Location Tracking Mechanism. In the **PROPOSED MODEL,** A Privacy-Preserving LocAtion proof Updating System (APPLAUS) in which colocated mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. **MODIFICATION** that we Propose in this Project, is to Encrypt the Communication Packets of Location Identification in order to avoid Location Data Modification which ensures Security.

**DOMAIN:. Mobile Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile computing, 2013

## ANS2 2. EXPLOITING SOCIAL CONTACT PATTERNS WITH CENTRALITY APPROACH FOR DATA FORWARDING IN DELAY-TOLERANT NETWORKS

## ARCHITECTURE DIAGRAM


SOURCE NODE
ROUTER
CENTRALITY: A NODE WHICH HAS HIGHEST CONNECTIVTY
COMMUNITY: MULTIPLE NODES IN THE SINGLE NODES
Node
Node
Node
Node
Node
Node
Node
Node
Node
Node
Node
Node
COMMUNITY A
COMMUNITY B

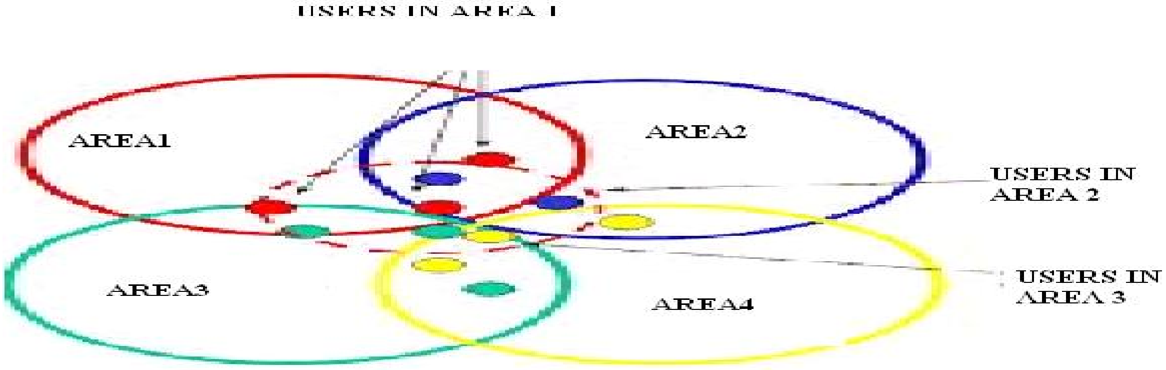
**DESCRIPTION :** In the **EXISTING SYSTEM**, Unpredictable node mobility, low node density, and lack of global information make it challenging to achieve effective data forwarding in Delay-Tolerant Networks (DTNs). Most of the these nodes may not be the best relay choices within a short time period due to the heterogeneity of transient node contact characteristics. In the **PROPOSED SYSTEM,** a novel approach to improve the performance of data forwarding using Two Approaches, 1. Centrality 2. Community. Centrality deals by identifying a node which has Highest Connectivity with other nodes, so this centrality node can definitely deliver the data to the Destination without loss. In the Community Approach, is to find out a Community of Nodes formation where the destination is attached with, so that the data can be delivered to the Destination within the Short Period of time without Loss. The **MODIFICATION** that we propose is the security part, there by we can encrypt the data & can be send to destination safely.

**DOMAIN:. Mobile Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile computing, 2013

## ANS2 3. ROBUST IDENTIFICATION OF USER MOVEMENT WITH LOCATION TRACKING USING SSD

## ARCHITECTURE DIAGRAM



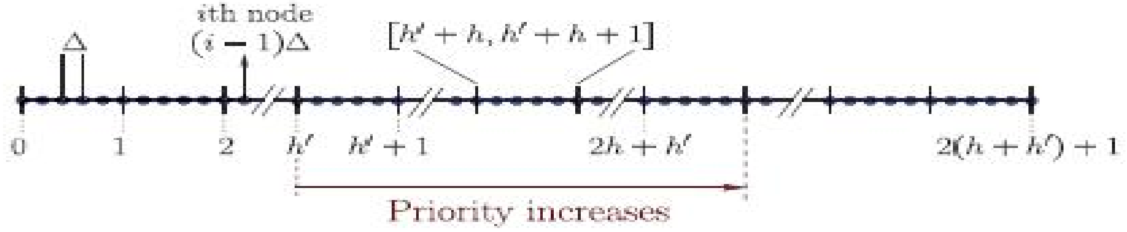
**DESCRIPTION :** In the **EXISTING SYSTEM**, the popular location fingerprint, Received Signal Strength (RSS), is observed to differ significantly across different devices' hardware even under the same wireless conditions. The system was not that Effective when compared to SSD. In the **PROPOSED SYSTEM,** we are using, SSD Approach is used to Identify Best matched Tower from the user's point of Position. User's Signal Strength is calculated so that the difference of the Signal Strength between the user with the different Towers are analyzed to identify a best matched or nearest Tower from the user point of view. We present the results of two well-known localization algorithms (K Nearest Neighbor and Bayesian Inference) when our proposed fingerprint is used. **MODIFICATION** part that we propose in this Project is to stream Advertisement Campaigns (Text) if the user passes best matched Tower by calculating SSD.

**DOMAIN:. Mobile Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile computing, 2013

# ANS2 4. LOCAL BROADCAST ALGORITHMS IN WIRELESS AD HOC NETWORKS: REDUCING THE NUMBER OF TRANSMISSIONS

## ARCHITECTURE DIAGRAM



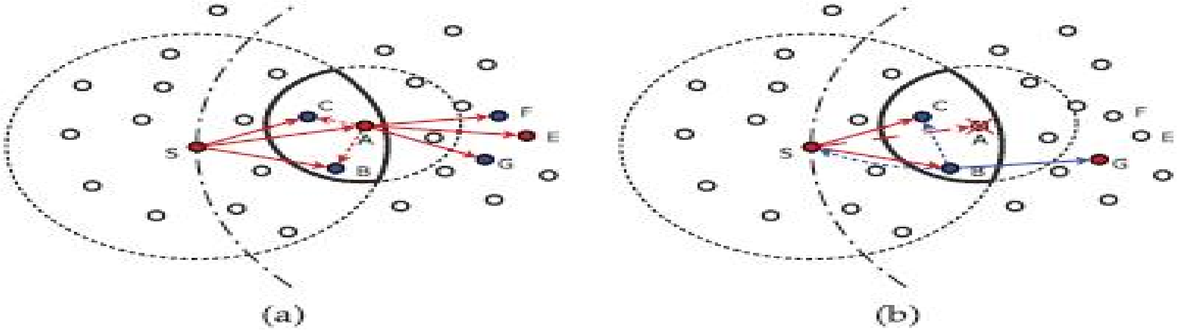
**DESCRIPTION:** There are two main approaches, static and dynamic, to broadcast algorithms in wireless ad hoc networks. In the static approach, local algorithms determine the status (forwarding/nonforwarding) of each node proactively based on local topology information and a globally known priority function. In this paper, we first show that local broadcast algorithms based on the static approach cannot achieve a good approximation factor to the optimum solution (an NP-hard problem). However, we show that a constant approximation factor is achievable if (relative) position information is available. In the dynamic approach, local algorithms determine the status of each node "on-the-fly" based on local topology information and broadcast state information. Using the dynamic approach, it was recently shown that local broadcast algorithms can achieve a constant approximation factor to the optimum solution when (approximate) position information is available. However, using position information can simplify the problem. Also, in some applications it may not be practical to have position information.

## DOMAIN:. Mobile Computing

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile computing, 2012

## ANS2 5. TOWARD RELIABLE DATA DELIVERY FOR HIGHLY DYNAMIC MOBILE AD HOC NETWORKS

## ARCHITECTURE DIAGRAM



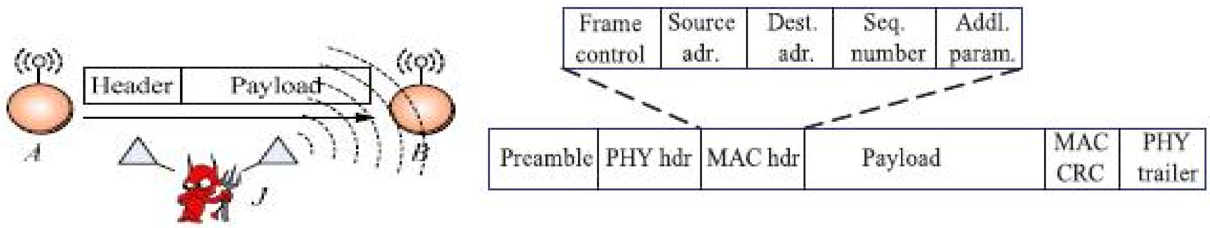
**DESCRIPTION:** This paper addresses the problem of delivering data packets for highly dynamic mobile ad hoc networks in a reliable and timely manner. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. Driven by this issue, we propose an efficient Position-based Opportunistic Routing (POR) protocol which takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. When a data packet is sent out, some of the neighbor nodes that have overheard the transmission will serve as forwarding candidates, and take turn to forward the packet if it is not relayed by the specific best forwarder within a certain period of time. By utilizing such in-the-air backup, communication is maintained without being interrupted. The additional latency incurred by local route recovery is greatly reduced and the duplicate relaying caused by packet reroute is also decreased.

**DOMAIN**:. **Mobile Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile computing, 2012

## ANS2 6. PACKET-HIDING METHODS FOR PREVENTING SELECTIVE JAMMING ATTACKS

## ARCHITECTURE DIAGRAM



**DESCRIPTION:** The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launchpad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

**DOMAIN:. Network Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Dependable and Secure Computing, 2012

## ANS2 7. ZONETRUST: FAST ZONE-BASED NODE COMPROMISE DETECTION AND REVOCATION IN WIRELESS SENSOR NETWORKS USING SEQUENTIAL HYPOTHESIS TESTING

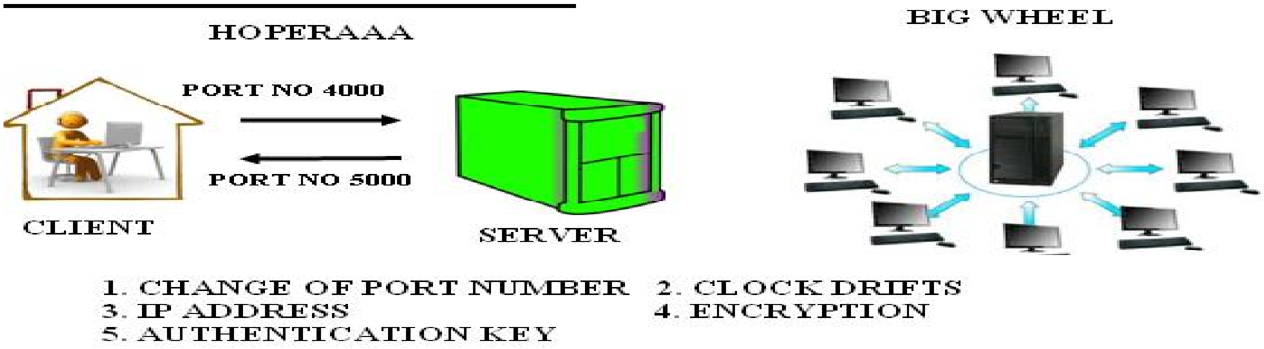
**DESCRIPTION:** Due to the unattended nature of wireless sensor networks, an adversary can physically capture and compromise sensor nodes and then mount a variety of attacks with the compromised nodes. To minimize the damage incurred by the compromised nodes, the system should detect and revoke them as soon as possible. To meet this need, researchers have recently proposed a variety of node compromise detection schemes in wireless ad hoc and sensor networks. For example, reputation-based trust management schemes identify malicious nodes but do not revoke them due to the risk of false positives. Similarly, software-attestation schemes detect the subverted software modules of compromised nodes. However, they require each sensor node to be attested periodically, thus incurring substantial overhead. To mitigate the limitations of the existing schemes, we propose a zone-based node compromise detection and revocation scheme in wireless sensor networks. The main idea behind our scheme is to use sequential hypothesis testing to detect suspect regions in which compromised nodes are likely placed. In these suspect regions, the network operator performs software attestation against sensor nodes, leading to the detection and revocation of the compromised nodes. Through quantitative analysis and simulation experiments, we show that the proposed scheme detects the compromised nodes with a small number of samples while reducing false positive and negative rates, even if a substantial fraction of the nodes in the zone are compromised. Additionally, we model the detection problem using a game theoretic analysis, derive the optimal strategies for the attacker and the defender, and show that the attacker's gain from node compromise is greatly limited by the defender when both the attacker and the defender follow their optimal strategies.

**DOMAIN**:. **Network Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Dependable and Secure Computing, 2012

## NS 9001. PREVENTION OF DDOS ATTACKS USING PORT NUMBER REVOLUTIONIZE AND TIME STAMP – CLOCK DRIFTS

## ARCHITECTURE DIAGRAM



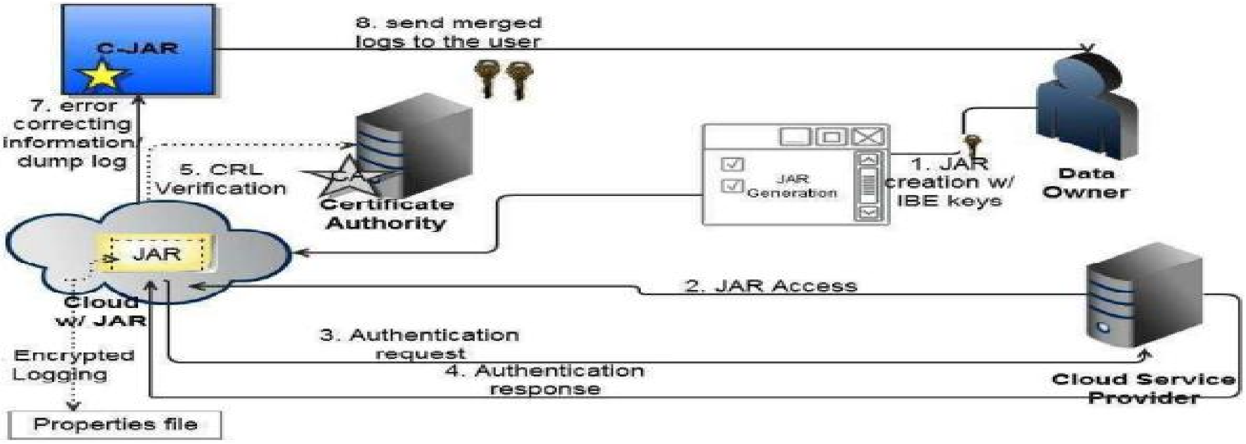
**DESCRIPTION :** In the **EXISTING SYSTEM**, An attacker can possibly launch a DoS attack by studying the flaws of network protocols or applications and then sending malformed packets which might cause the corresponding protocols or applications getting into a faulty state. In the **PROPOSED SYSTEM**, we have two Algorithms namely, HOPERAA Algorithm and Big Wheel Algorithm. HOPERAA Algorithm is used for single client server communication and Big Wheel Algorithm is used for multi client and server communication. In both the part we're verifying the time stamp for the communication as well as continuous changing of port communication medium in a network and this ensures security. In **MODIFICATION**, We verifying the time stamp, communication port id, IP address, Authentication key as well as encryption of data, which ensures proper and secure communication.

**DOMAIN: Network Security**

**IEEE REFERENCE: IEEE Transactions** on Dependable and Secure Computing, 2012

## NS 9002. SECURED DATA SHARING WITH ACCESS PRIVILEGE POLICIES AND DISTRIBUTED ACCOUNTABILITY IN CLOUD COMPUTING

## ARCHITECTURE DIAGRAM



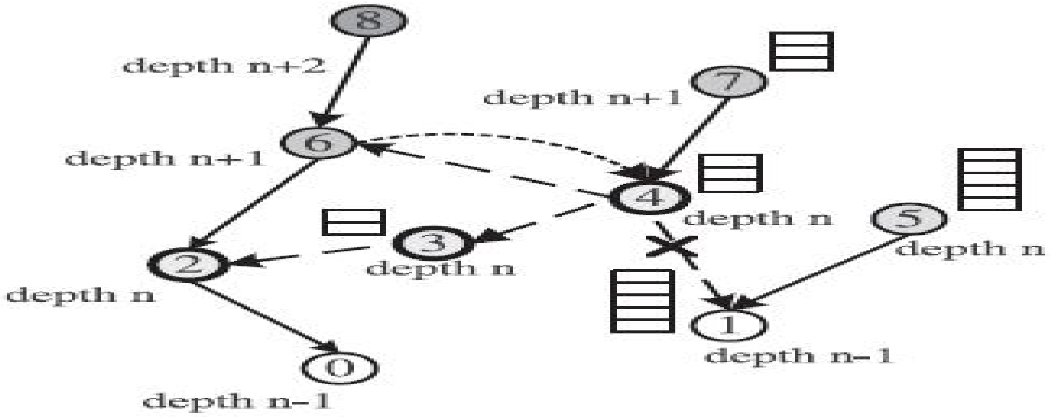
**DESCRIPTION :** In the **EXISTING SYSTEM**, A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by Cloud Computing, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. In the **PROPOSED SYSTEM**, Data Owner can upload the data into cloud server after encryption. User can subscribe into the cloud server with certain access policies such Read, Write and Copy of the Original Data. Logger and Log Harmonizer will a track of the access logs and reports to the Data Owner. This Access ensures Security.

**DOMAIN: Cloud Computing, Security**

**IEEE REFERENCE: IEEE Transactions** on Dependable and Secure Computing, 2012

## NS 9003. AUTONOMOUS BEST ROUTE IDENTIFICATION WITH CAPACITY, TIME AND HOP COUNT MEASURES USING GAUSSIAN ALGORITHM

## ARCHITECTURE DIAGRAM



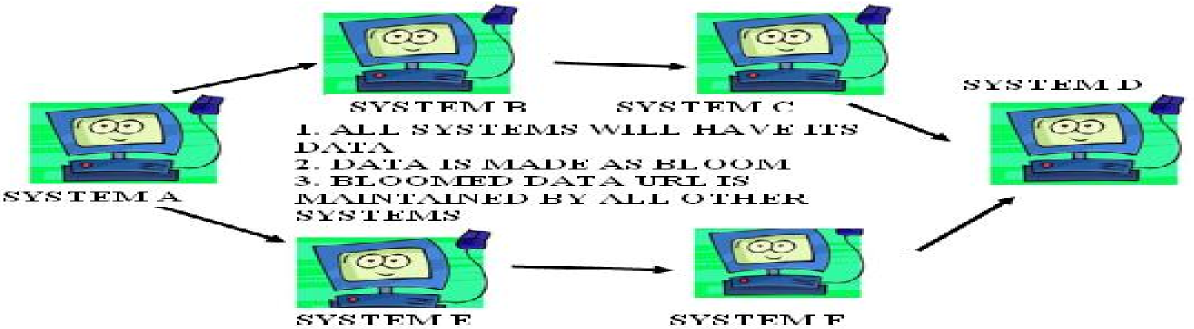
**DESCRIPTION :** In **EXISTING SYSTEM,** Breadth First and Greedy Algorithm is used to send the data by finding the nearest node with fixed time rate. In the **PROPOSED SYSTEM** the Gaussian Channel, which verifies the bandwidth and distance so as to deliver the packets safely to the destination, but if the route fails, it will send the packets via high time consuming route. It supports long distance of data delivery. In the **MODIFICATION**, We also calculate the nodes trustworthiness with respect to the previous experience and history of the nodes.

**DOMAIN: Networking**

**IEEE REFERENCE:** **IEEE Transactions** on Parallel and Distributed Systems, 2012

## NS 9004. BLOOMCAST: EFFICIENT AND EFFECTIVE FULL-TEXT RETRIEVAL IN UNSTRUCTURED P2P NETWORKS

## ARCHITECTURE DIAGRAM


SYSTEM B
SYSTEM C
SYSTEM D
SYSTEM A
1. ALL SYSTEMS WILL HAVE ITS DATA
2. DATA IS MADE AS BLOOM
3. BLOOMED DATA URL IS MAINTAINED BY ALL OTHER SYSTEMS
SYSTEM E
SYSTEM F

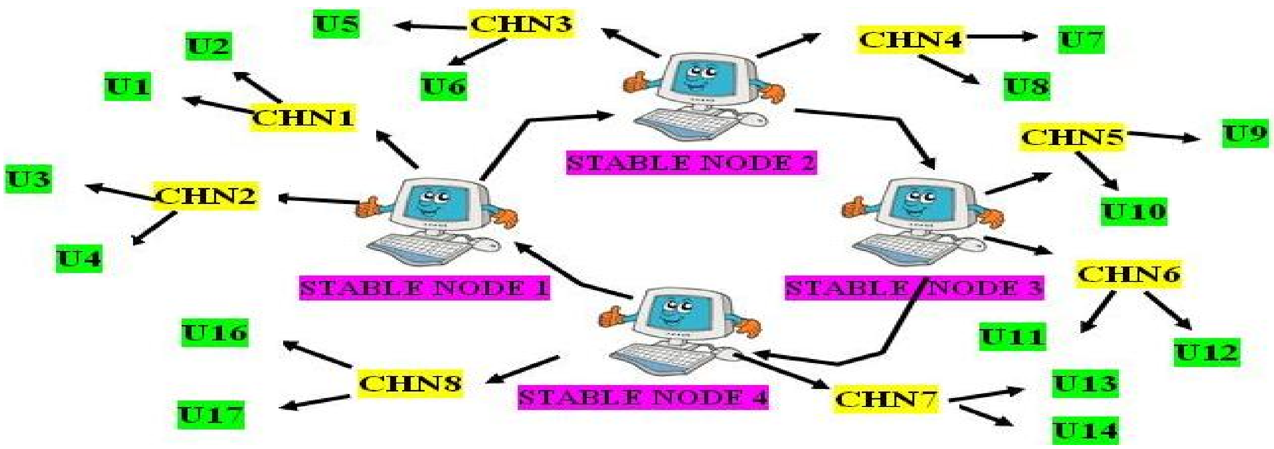
**DESCRIPTION :** In the **EXISTING SYSTEM**, The emergence of P2P file sharing applications, millions of users have used P2P systems to search desired data. Existing P2P full-text search schemes can be divided into two types: DHT based global index and federated search engine over unstructured protocols. Due to the exact match problem of DHTs, such schemes provide poor full-text search capacity. In the **PROPOSED SYSTEM,** To overcome this issues we propose a novel strategy, called BloomCast, to support efficient and effective full-text retrieval in this paper. BloomCast hybridizes a lightweight DHT with an unstructured P2P overlay to support random node sampling and network size estimation. Furthermore, we propose an option of using Bloom Filter encoding instead of replicating the raw data. Using such an option, Bloom Cast replicates Bloom Filters (BF) of a document. A BF is a lossy but succinct and efficient data structure to represent the data. By replicating the encoded term sets using BFs instead of raw documents among peers, the communication/storage costs are greatly reduced, while the full-text multi keyword searching are supported. In the **MODIFICATION** that we propose is to identify the best documentation by applying Stemming Algorithm so that keywords are extracted and compared with requested term frequency using Ranking Process.

**DOMAIN**: **Networking, Data Mining**

**IEEE REFERENCE:** **IEEE Transactions** on Parallel and Distributed Systems, 2012

# NS 9005. EFFECTIVE AND EFFICIENT MULTIMEDIA DATA SHARING SYSTEM WITH LOAD BALANCING AND SECURITY

## ARCHITECTURE DIAGRAM



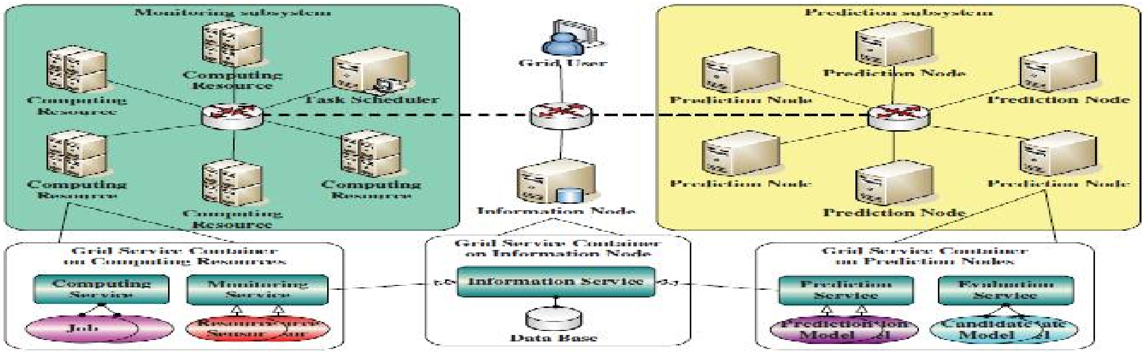
**DESCRIPTION :** In the **EXISTING SYSTEM**, the server-client model were used which fall short in meeting the increasing need of bandwidth and storage resources. In the **PROPOSED SYSTEM**, we’ll have p2p network with stable and child nodes connected to the users in a hierarchy model. Load balancing Process is also implemented effectively by shifting heavily loaded stable node to the position of the lightly loaded stable node. Proper resource utilization is also implemented. . In the **MODIFICATION**, We also provide the security for the File contents by encrypting the data.

**DOMAIN: Networking**

**IEEE REFERENCE:** **IEEE Transactions** on Parallel and Distributed Systems, 2012

# NS 9006. DYNAMIC IDENTIFICATION OF RESOURCE MONITORING & PREDICTION OF EFFECTIVE DATA COMMUNICATION IN GRID ENVIRONMENT

## ARCHITECTURE DIAGRAM



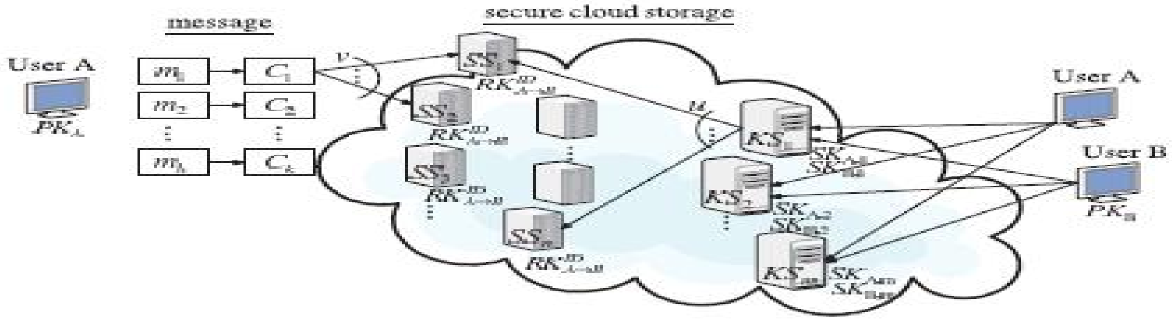
**DESCRIPTION :** In the **EXISTING SYSTEM** Integration Resource Allocation and Job Scheduling Process in the Grid Environment is the Challenging Task. So We **PROPOSE,** a Model by Which Grid Resource Monitoring will Monitor the Resource Utilized Currently and the available Resource in the Grid Server and the Grid Resource Predication is to Verify the Historical Data to Predict Amount of Resource Required to Process the Request. We use PH-PSO for this Process. The **MODIFICATION** we Propose is Same Data is Requested Again by Some other User, then the Information Server (IS) will have Catch Memory and IS will Forwarded the Data rather Disturbing the Grid Resource Server.

**DOMAIN: Grid Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9007. DISTRIBUTION OF SECRET KEYS AND THE PACKETS FOR SECURED DATA FORWARDING SCHEME IN CLOUD SERVER

## ARCHITECTURE DIAGRAM



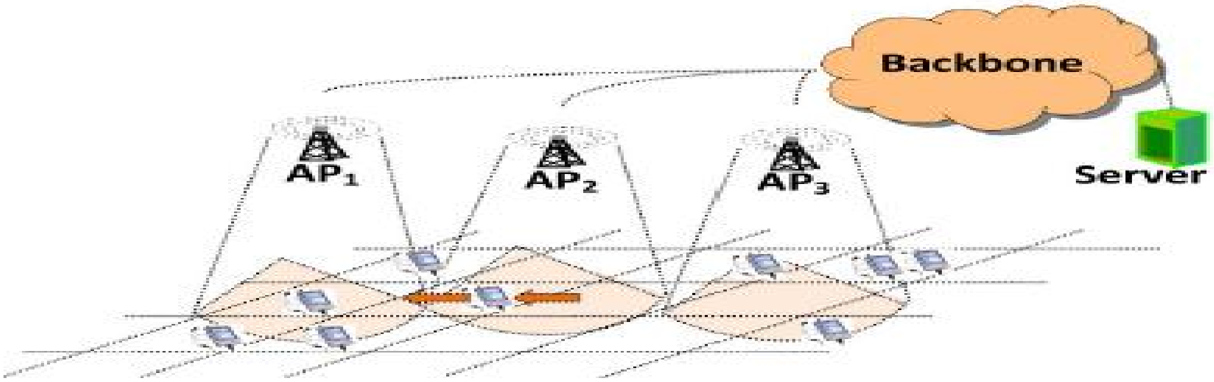
**DESCRIPTION :** In the **EXISTING SYSTEM**, Cloud Computing is the Process of Storing the Data in the Remote Server. This Process Doesn’t Speak about Confidentiality of the Data. So in the **PROPOSED MODEL**, the Uploaded file from a Data Owner is Splitted into Multiple Packets and Stored in Multiple Cloud Servers. These Packets are Encrypted Using the Primary Key. These Different Keys are also distributed in Multiple Key Servers. User ID is Appended for Verification. If the Data Owner Forwards the file then the Keys are Verified for the Data Access.

**DOMAIN: Cloud Computing, Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9008. DYNAMIC ACCESS SERVER REASSIGNMENT USING IDENTIFING OPTIMIZED THROUGHPUT CALCULATION IN WIRELESS CLUSTER

## ARCHITECTURE DIAGRAM



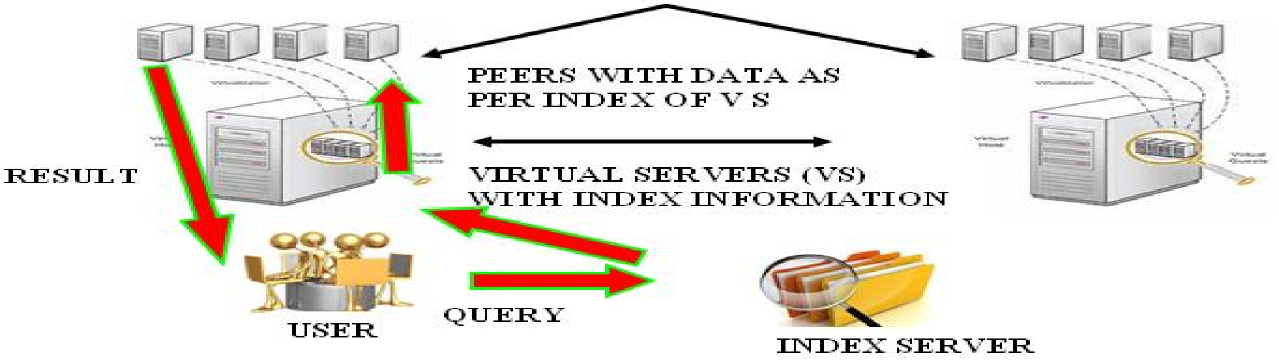
**DESCRIPTION :** In the **EXISTING SYSTEM**, In a constructed wireless sensor network, the information about some area of interest may require further investigation such that more traffic will be generated. However, the restricted routing of a ZigBee cluster-tree network may not be able to provide sufficient bandwidth for the increased traffic load, so the additional information may not be delivered successfully. In the **PROPOSED SYSTEM**, the aim is to avoid the traffic via overload, so as the deliver the packets to the destination we apply push pull re-label algorithm which measures capacity distance number of packets so that the delivery is corrected by the next region head. In the **MODIFICATION**, We apply security part of the implementation by the encryption of packets. We implement using wireless networks and not using zigbee hardware.

**DOMAIN: Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9009. IMPLEMENTATION OF BLOOM FILTER FOR EFFECTIVE MULTI KEY WORD SEARCHING PROCESS & DEPLOYMENT OF VIRTUAL SERVER

## ARCHITECTURE DIAGRAM


PEERS WITH DATA AS PER INDEX OF V S
RESULT
VIRTUAL SERVERS (VS) WITH INDEX INFORMATION
USER
QUERY
INDEX SERVER

**DESCRIPTION :** In the **EXISTING SYSTEM**, Single Keyword based Approach is used to be Mapped with the Set of Document in the Nodes. In the **PROPOSED MODEL** Multi Keyword Search is Applied Where lots of Virtual Server is Deployed with Index Information of all the Documents. Peers will contain the Documents. Search is posted to Index Server Which

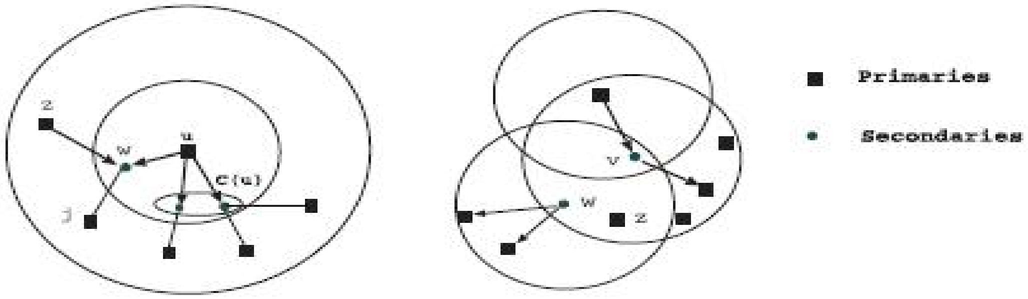
Manages the Address Space of Virtual Server and Identifies the Data Contains Peer List. Best Records are Retrieved Using Ranking Process.

**DOMAIN: Data Mining**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Knowledge and Data Engineering, 2012

## NS 9010. APPROXIMATION ALGORITHMS FOR DATA BROADCAST IN WIRELESS NETWORKS

## ARCHITECTURE DIAGRAM



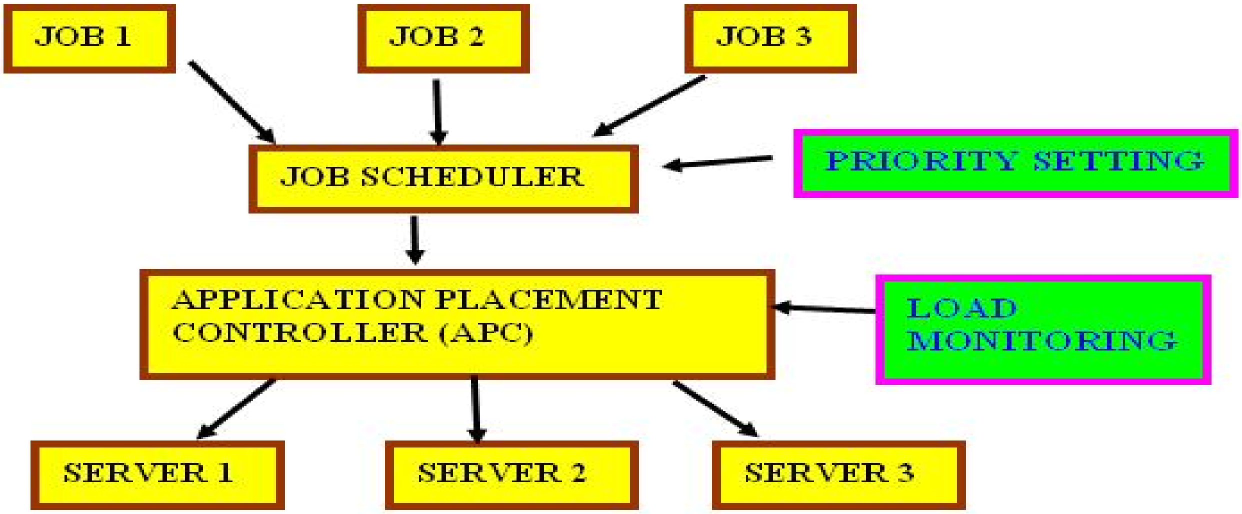
**DESCRIPTION :** Broadcasting is a fundamental operation in wireless networks and plays an important role in the communication protocol design. In multihop wireless networks, however, interference at a node due to simultaneous transmissions from its neighbors makes it nontrivial to design a minimum-latency broadcast algorithm, which is known to be NP-complete. We present a simple 12-approximation algorithm for the one-to-all broadcast problem that improves all previously known guarantees for this problem. We then consider the all-to-all broadcast problem where each node sends its own message to all other nodes. For the all-to-all broadcast problem, we present two algorithms with approximation ratios of 20 and 34, improving the best result available in the literature. Finally, we report experimental evaluation of our algorithms

**DOMAIN: Mobile Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile Computing 2012

## NS 9011. AUTOMATIC LOAD MONITORING SYSTEM WITH PRIORITY SETTINGS FOR EFFECTIVE TRANSACTIONAL WORKLOADS

## ARCHITECTURE DIAGRAM



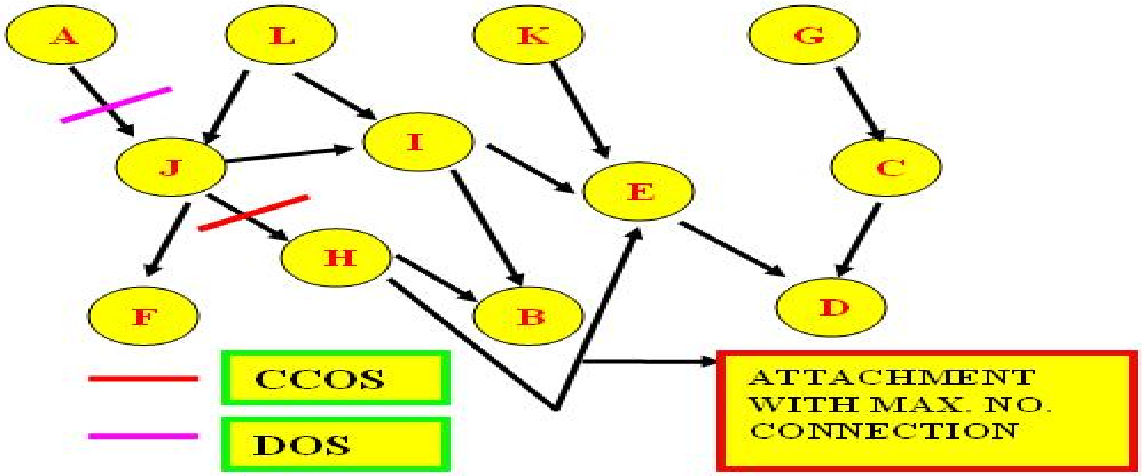
**DESCRIPTION :** In the **EXISTING SYSTEM**, one server will carry the entire workload (or) multiple server can carry without the proper scheduling. In the **PROPOSED SYSTEM,** Jobs are allotted to Job scheduler, then to the Application Placement Controller (APC), where it identifies the load of every server and allocates the job accordingly. In the **MODIFICATION PART**, we setting the Priority checking in the Job scheduler itself, where user can specify the priority status of a job so the job scheduler first transmits High then Medium and finally low priority job to APC, then the to the best server.

**DOMAIN**:. **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9012. CUT DETECTION & AUTOMATIC REJOINING OF ISOLATED NODES IN WSN

## ARCHITECTURE DIAGRAM



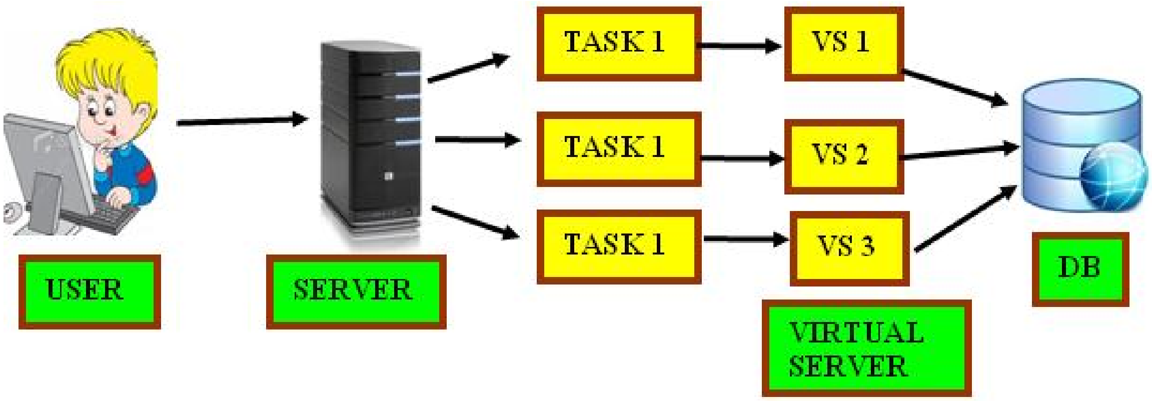
**DESCRIPTION :** In the **EXISTING SYSTEM**, Link(or) the nodes can be disconnected which cannot be detected. So packets are lost again and again as the cut in the networks aren't identified. In the **PROPOSED MODEL,** the cut detection is identified using CCOS (or) DOS Algorithm, in order to verify it leaf nodes are disconnected or Direct Nodes are disconnected. We calculate Hop Count and Time Stamp to identify the disconnection. The **MODIFICATION** that we propose is, to add the disconnected nodes to the node which has maximum number of connections.

**DOMAIN**:. **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9013. EFFICIENT SERVER PROVISIONING WITH CONTROL FOR END-TO-END RESPONSE TIME GUARANTEE ON MULTITIER CLUSTERS

## ARCHITECTURE DIAGRAM



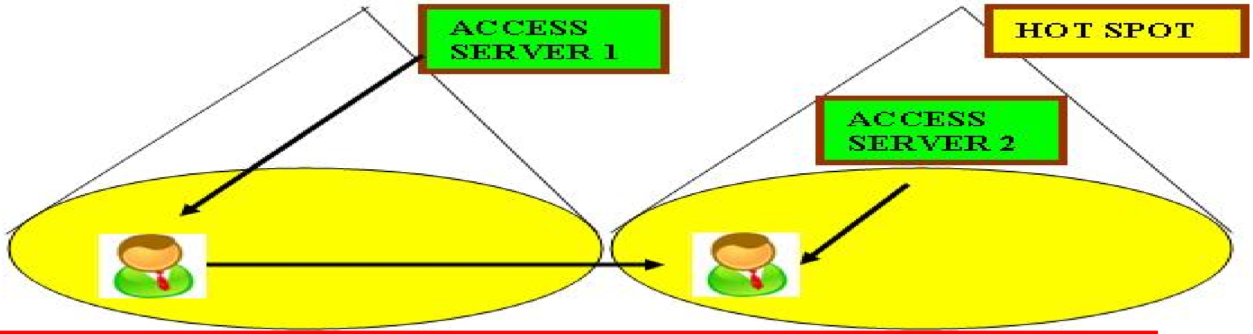
**DESCRIPTION :** In the **EXISTING SYSTEM**, there will be lots of server will be available but then, one server will carry all the jobs at a time, so load imbalance will occur. In the **PROPOSED MODEL**, user's request is splitted into multiple task and virtual server is created according to the load of task. All the Virtual Server submit the corresponding task to Application server and then to the Database. We also implement this for a Money transferring/ Banking Process. The **MODIFICATION** that we propose is to encrypt the Data during Communication.

**DOMAIN**:. **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

# NS 9014. FINGERPRINTING MOBILE USER POSITIONS IN SENSOR NETWORKS: ATTACKS AND COUNTERMEASURES

## ARCHITECTURE DIAGRAM



**MONITORING USER'S MOVEMENT, HOT SPOT IS IDENTIFIED FOR EFFECTIVE & SPEEDY DATA DELIVERY DURING HIGH TRAFFIC ALONG WITH THE ADVERTISEMENTS TO THE USER.**

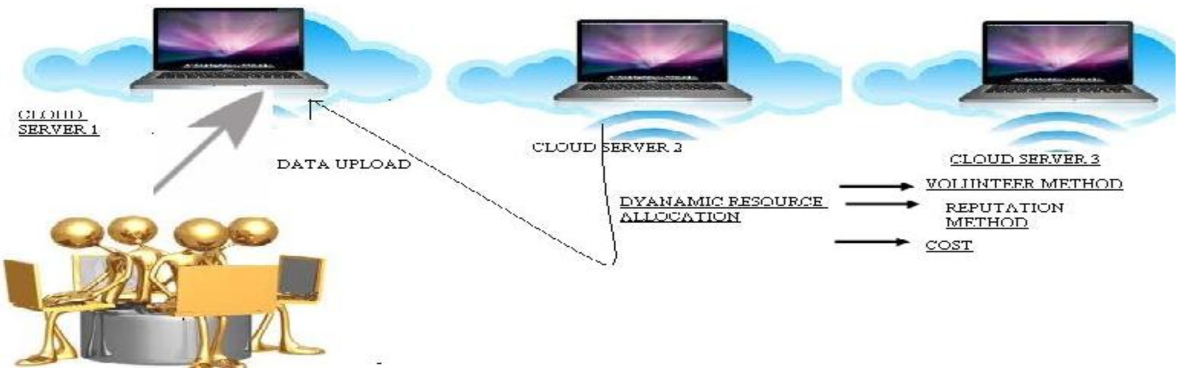
**DESCRIPTION :** In the **EXISTING SYSTEM**, the adversaries are able to build a mapping between the instant distribution of mobile users and the observed network flux. Due to this traffic packets are lost and generate High traffic. In the **PROPOSED SYSTEM**, we apply network flux model for effective data delivery from network wide data collection tree. Mobile user's activity monitoring via prediction and filtering technique is used to find the next Expected Movement of the user. So that if the traffic is High on the current area access server, the next excepted Area Access server is identified as Hot SPOT for Effective Data Delivery. **MODIFICATION**, We Propose is automatic alert of the advertisement of the current location to the user. As user moves from one location to another, the corresponding advertisements are provided to them.

**DOMAIN**:. **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9015. DYNAMIC RESOURCE ALLOCATION IN MULTI CLOUD DEPLOYMENT SYSTEM FOR EFFECTIVE DATA PROCESS

## ARCHITECTURE DIAGRAM



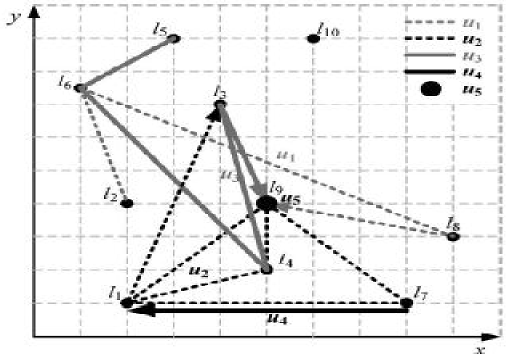
**DESCRIPTION :** In the **EXISTING SYSTEM**, there is no security in cloud, resource is fixed and is not allocated to the all the Clouds. Resources aren't expandable. In the **PROPOSED SYSTEM**, initially Resource is allotted to all the Clouds, when high demand of data storage comes Resource is expanded dynamically. **MODIFICATION** we propose is that Resource Allocation can either happen by Reputation, Volunteer (or) Cost methods.

**DOMAIN**: **Cloud Computing**, **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9016. IDENTIFICATION OF USER INTEREST SERVICES AND LOCATION PATTERNS USING USER ACTIVITY MONITORING SYSTEM

## ARCHITECTURE DIAGRAM



- ❖ **USER TRACKING - UMD**
- ❖ **LOCATION INTEREST – LMD**
- ❖ **SERVICE INTEREST - SRD**

**DESCRIPTION :** In the **EXISTING SYSTEM**, there is no exact tracking mechanism for identifying the users likes and dislikes of location based services. So this may not be helpful to identify the best service provided to the user. In the **PROPOSED MODEL**, we track the users movement based behavior pattern and which helps to identify a location on which user stays for longer time and helpful to identify user's favorite services. UMD (User Movement Database) is to track user's movement. LMD (Location Movement Database) is to identify user's desired Location. SRD (Service Request Database) is to identify the user's desired Service.

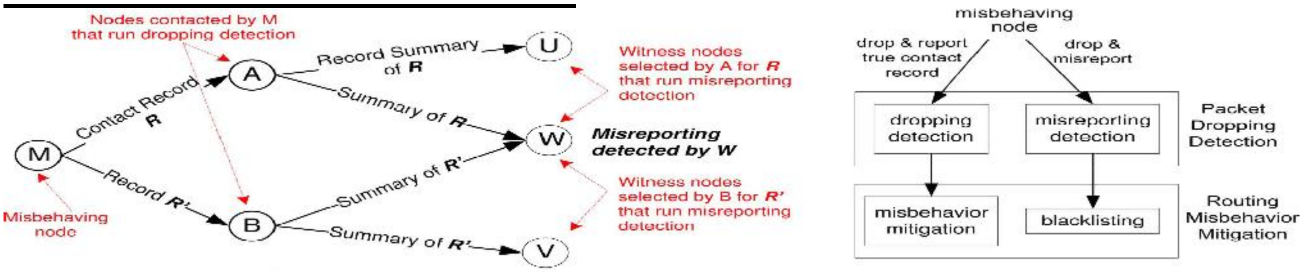
**MODIFICATION** that we propose is, a new user enter can verify the most liked services by plenty of previous users which helps them to choose the right service at right location.

## DOMAIN:. Mobile Computing and Data Mining

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9017. IDENTIFICATION OF MALICIOUS PACKET LOSS DURING ROUTING MISBEHAVIOUR IN DISRUPTION TOLERENT NETWORK

## ARCHITECTURE DIAGRAM


Nodes contacted by M that run dropping detection
Record Summary of R
U
A
Contact Record R
Summary of R
W
M
Witness nodes selected by A for R that run misreporting detection
Misreporting detected by W
Record R'
Summary of R'
B
Misbehaving node
Witness nodes selected by B for R' that run misreporting detection
Summary of R'
V
misbehaving node
drop & report true contact record
drop & misreport
dropping detection
misreporting detection
Packet Dropping Detection
misbehavior mitigation
blacklisting
Routing Misbehavior Mitigation

**(a) PACKET DROPPING DETECTING MISBEHAVING NODE M REPORTS TWO FORGED CONTACT RECORDS R AND R^ WHICH ARE IN CONSISTENT.**
**(b) MISBEHAVIOR MITIGATION**

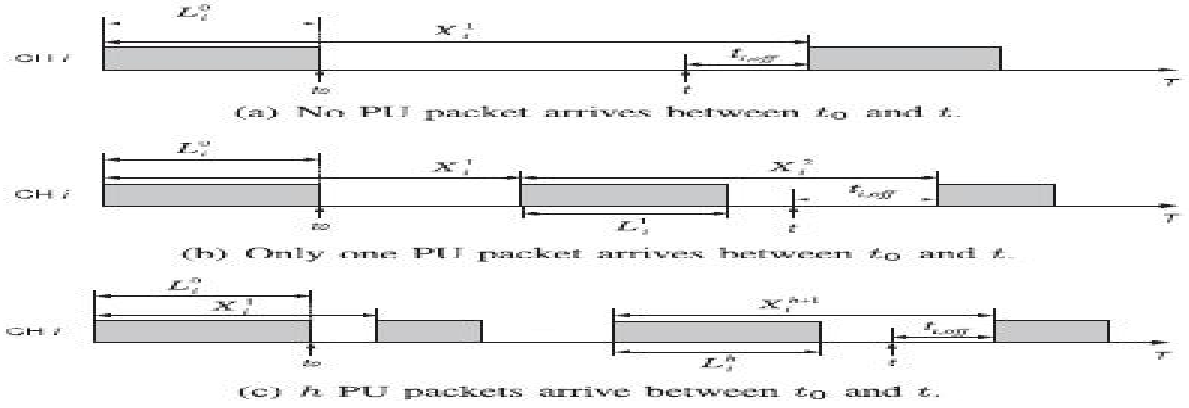
**DESCRIPTION :** In **EXISTING SYSTEM** Disruption tolerant networks (DTNs), selfish or malicious nodes may drop received packets. Such routing misbehavior reduces the packet delivery ratio and wastes system resources. In the **PROPOSED SYSTEM** distributed scheme to detect packet dropping in DTNs. In our scheme, DTN is required to keep a few signed contact records with mobile nodes. This Previous Records is utilized to verify the trustworthiness of DTN. For every mobile node Records Handler is maintained to track the incoming and outgoing Records of it. Witness Node will identify real misbehavioring node by comparing the Records Handler and DTN In the **MODIFICATION**, we’re differentiating genuine traffic packet loss with malicious packet loss by comparing the Buffer level of every nodes, We encrypt the data packets for security.

**DOMAIN: Network Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Information Forensics and Security, 2012

## NS 9018. AUTONOMOUS SPECTRUM HANDOFF FRAMEWORK IN ADHOC NETWORK WITH DYNAMIC LOAD BALANCING

## ARCHITECTURE DIAGRAM



(a) No PU packet arrives between $t_0$ and $t$.

(b) Only one PU packet arrives between $t_0$ and $t$.

(c) $h$ PU packets arrive between $t_0$ and $t$.

**DESCRIPTION :** In the **EXISTING SYSTEM**, Although the Cognitive Radio (CR) technology is a promising solution to enhance the spectrum, only it provides sufficient support to the licensed users or primary users and not to the Unlicensed Users. In the **PROPOSED**

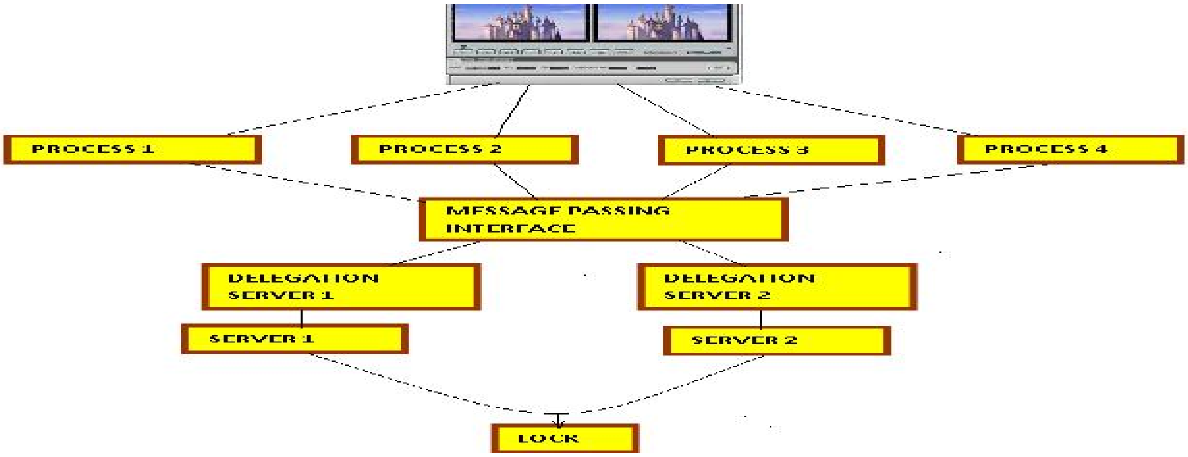
**MODEL**, a proactive spectrum handoff framework for CR ad hoc networks, ProSpect, is proposed to address these concerns. In the proposed framework, Channel-Switching (CW) policies and a proactive spectrum handoff protocol are proposed to let unlicensed users vacate a channel before a licensed user utilizes it to avoid unwanted interference. Network coordination schemes for unlicensed users are also incorporated into the spectrum handoff protocol design. In the **MODIFICATION** that we propose is a unlicensed user is handled by the spectrum and receives the request from the licensed user, the system automatically transfer the unlicensed user into another spectrum which reduces load and the waiting time for particular unlicensed user.

**DOMAIN:. Mobile Computing**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Mobile Computing, 2012

## NS 9019. DELEGATION-BASED I/O MECHANISM FOR HIGH PERFORMANCE COMPUTING SYSTEMS

## ARCHITECTURE DIAGRAM



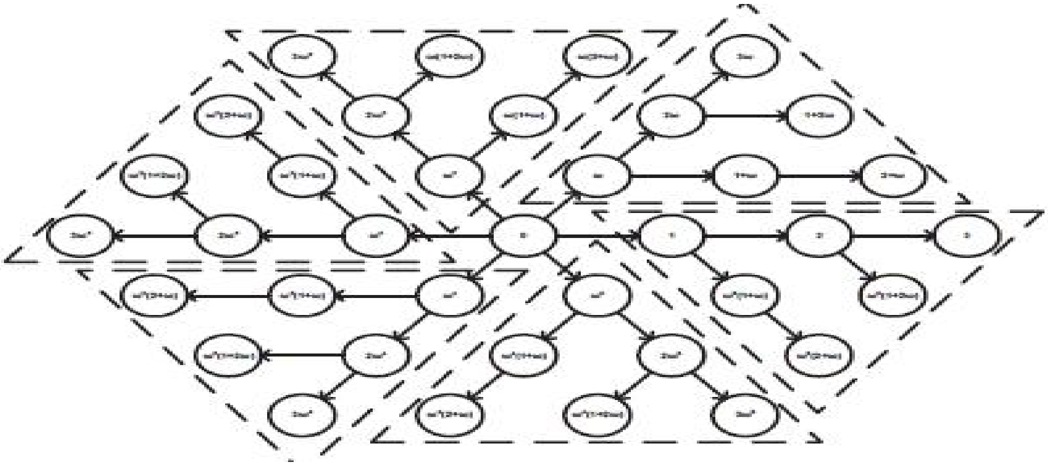
**DESCRIPTION :** In the **EXISTING SYSTEM**, Strict data consistency semantics adopted from traditional file systems are inadequate for homogeneous parallel computing platforms. For high performance parallel applications independent I/O is critical, particularly if check pointing data are dynamically created or irregularly partitioned. In the **PROPOSED MODEL**, the user requested videos are divided into multiple process, those process are passed to Message Passing Interface (MPI) which then allocates delegate system according to the available server. so that speedy and easy handling is assured. These Jobs are allocated to the delegate Via Round Robin Method. **MODIFICATION** that we propose is peer to peer streaming without disturbing the load of the Main Server. We also add up the security by encryption.

**DOMAIN:. Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9020. EFFICIENT COMMUNICATION ALGORITHMS IN HEXAGONAL MESH INTERCONNECTION NETWORKS

## ARCHITECTURE DIAGRAM



**DESCRIPTION :** In this paper, we show that the hexagonal mesh networks developed in the early 1990s are a special case of the EJ networks that have been considered more recently. Using a node addressing scheme based on the EJ number system, we give a shortest path routing algorithm for hexagonal mesh networks. We also extend the known efficient one-to-all broadcasting algorithm on hexagonal mesh networks to algorithms for one-to-one personalized broadcasting, all-to-all broadcasting, and all-to-all personalized broadcasting algorithms. Their time complexity and optimality are analyzed.

**DOMAIN**:. **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9021. EXTREMA PROPAGATION: FAST DISTRIBUTED ESTIMATION OF SUMS AND NETWORK SIZES

## ARCHITECTURE DIAGRAM

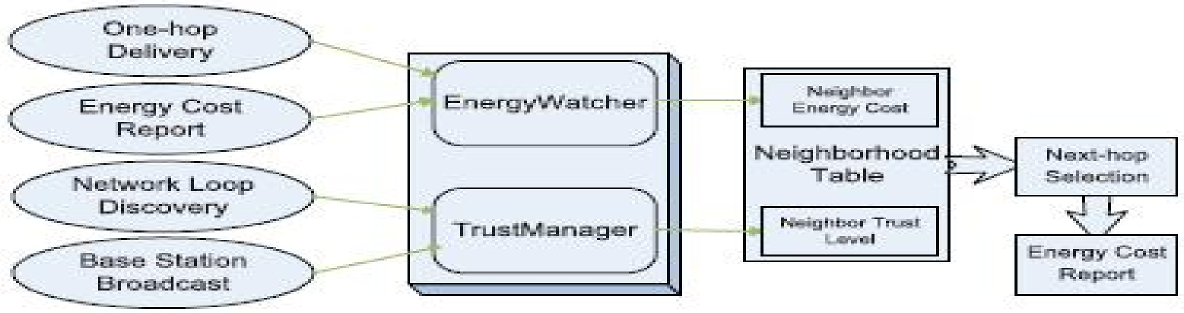
**DESCRIPTION :** Aggregation of data values plays an important role on distributed computations, in particular, over peer-to-peer and sensor networks, as it can provide a summary of some global system property and direct the actions of self-adaptive distributed algorithms. Examples include using estimates of the network size to dimension distributed hash tables or estimates of the average system load to direct load balancing. Distributed aggregation using non idempotent functions, like sums, is not trivial as it is not easy to prevent a given value from being accounted for multiple times; this is especially the case if no centralized algorithms or global identifiers can be used. This paper introduces Extrema Propagation, a probabilistic technique for distributed estimation of the sum of positive real numbers. The technique relies on the exchange of duplicate insensitive messages and can be applied in flood and/or epidemic settings, where multipath routing occurs; it is tolerant of message loss; it is fast, as the number of message exchange steps can be made just slightly above the theoretical minimum; and it is fully distributed, with no single point of failure and the result produced at every node.

**DOMAIN**:. **Networking**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Parallel and Distributed Systems, 2012

## NS 9022. DESIGN AND IMPLEMENTATION OF TARF: A TRUST-AWARE ROUTING FRAMEWORK FOR WSNS

## ARCHITECTURE DIAGRAM



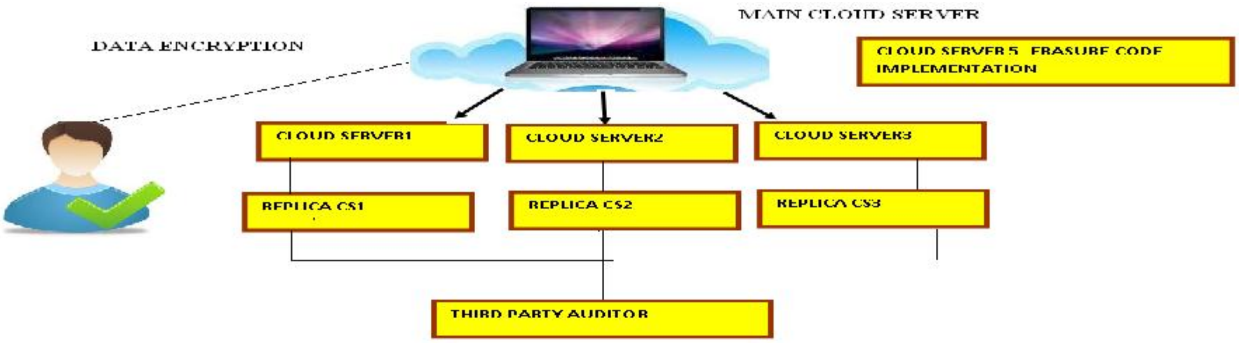
**DESCRIPTION :** The multi-hop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks, and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multi-hop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route.

**DOMAIN**:. **Network Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Dependable and Secure Computing, 2012

# NS 9023. TOWARD SECURE AND DEPENDABLE STORAGE SERVICES IN CLOUD COMPUTING

## ARCHITECTURE DIAGRAM



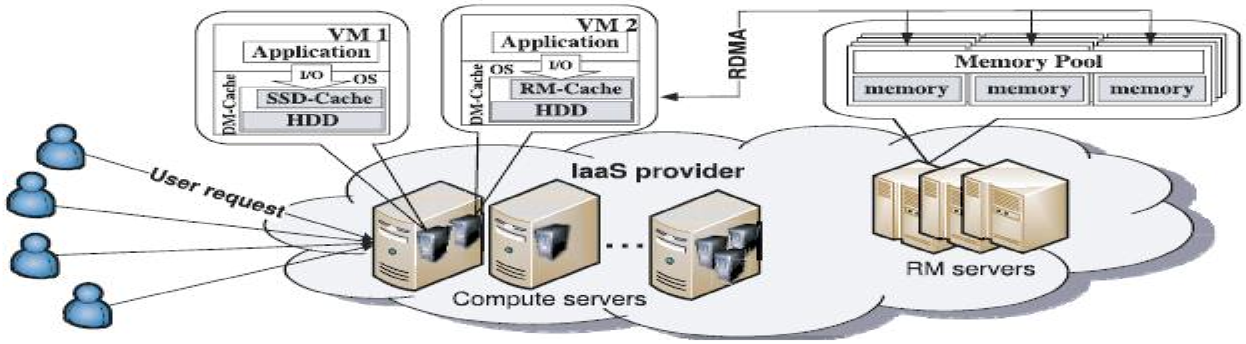
**DESCRIPTION :** In the **EXISTING SYSTEM**, there is no big security provided in the Cloud server for data safety. If at all security exists, the third party auditor should be allowed to access the entire data packets for verification. In the **PROPOSED SYSTEM**, Cloud server spilt the file into batches and allowed for encryption. The corresponding encrypted batches are kept in different Cloud servers and their keys are distributed in different key server. These encrypted batches are kept in replica servers as a backup. This encrypted data are converted into bytes and added parity bit process by the data owner in order to restrict TPA by accessing the original data. The Cloud server generates the token number from the parity added encrypted data and compared with the signature provided to the TPA to verify the Data Integrity. We also implement Erasure Code for the back-up of the data. The **MODIFICATION** that we propose is the encryption process of the data by the data owner before it reaches the Cloud server.

**DOMAIN: Network Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Service Computing, 2012

## NS 9024. CASHING IN ON THE CACHE IN THE CLOUD

## ARCHITECTURE DIAGRAM



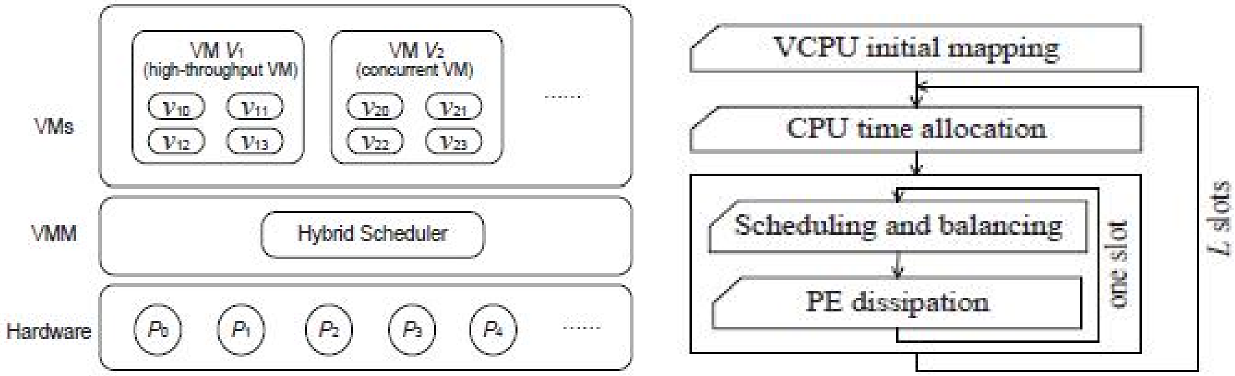
**DESCRIPTION :** Over the past decades, caching has become the key technology used for bridging the performance gap across memory hierarchies via temporal or spatial localities; in particular, the effect is prominent in disk storage systems. In this paper, we present the cache as a service (CaaS) model as an optional service to typical infrastructure service offerings. Specifically, the cloud provider sets aside a large pool of memory that can be dynamically partitioned and allocated to standard infrastructure services as disk cache. We first investigate the feasibility of providing CaaS with the proof-of-concept elastic cache system (using dedicated remote memory servers) built and validated on the actual system, and practical benefits of CaaS for both users and providers (i.e., performance and profit, respectively) are thoroughly studied with a novel pricing scheme. Our CaaS model helps to leverage the cloud economy greatly in that 1) the extra user cost for I/O performance gain is minimal if ever exists, and 2) the provider's profit increases due to improvements in server consolidation resulting from that performance gain.

**DOMAIN: Cloud Computing**

**IEEE REFERENCE:** **IEEE Transactions** on Parallel and Distributed Systems, 2012

## NS 9025. HYBRID CPU MANAGEMENT FOR ADAPTING TO THE DIVERSITY OF VIRTUAL MACHINES

## ARCHITECTURE DIAGRAM



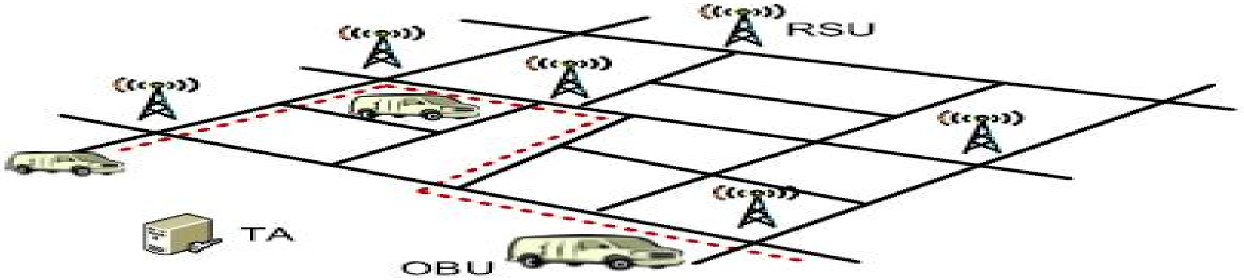
**DESCRIPTION :** As an important cornerstone for clouds, virtualization plays a vital role in building this emerging infrastructure. Virtual machines (VMs) with a variety of workloads may run simultaneously on a physical machine in the cloud platform. We present a hybrid scheduling framework for CPU management in the VMM to adapt to the diversity of VMs running simultaneously on a physical machine. We implement a hybrid scheduler, and experimental results indicate that the hybrid CPU management method is feasible to mitigate the negative influence of virtualization on synchronization, and improve the performance of concurrent applications in the virtualized system, while maintaining the performance of high-throughput applications.

**DOMAIN: Cloud Computing**

**IEEE REFERENCE: IEEE Transactions** on Computers, 2012

## NS 9026. FOOTPRINT: DETECTING SYBIL ATTACKS IN URBAN VEHICULAR NETWORKS

## ARCHITECTURE DIAGRAM



**DESCRIPTION :** In urban vehicular networks, where privacy, especially the location privacy of anonymous vehicles is highly concerned, anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining a disproportionately large influence. In this paper, we propose a novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the appearance time at this RSU. We design a location-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification.

**DOMAIN: Mobile Computing, Security**

**IEEE REFERENCE: IEEE Transactions** on Parallel and Distributed Systems, 2012

## NS 9027. A POLICY ENFORCING MECHANISM FOR TRUSTED ADHOC NETWORKS

**DOMAIN:. Network Security**

**IEEE REFERENCE: IEEE TRANSACTIONS** on Dependable and Secure Computing, 2011

## NS 9028. A FUZZY TOPSIS DECISION MAKING MODEL WITH ENTROPY WEIGHT UNDER INTUITIONISTIC FUZZY ENVIRONMENT

**IEEE REFERENCE: IEEE Paper** on IMECS, 2009

# YOUR OWN IDEAS ALSO