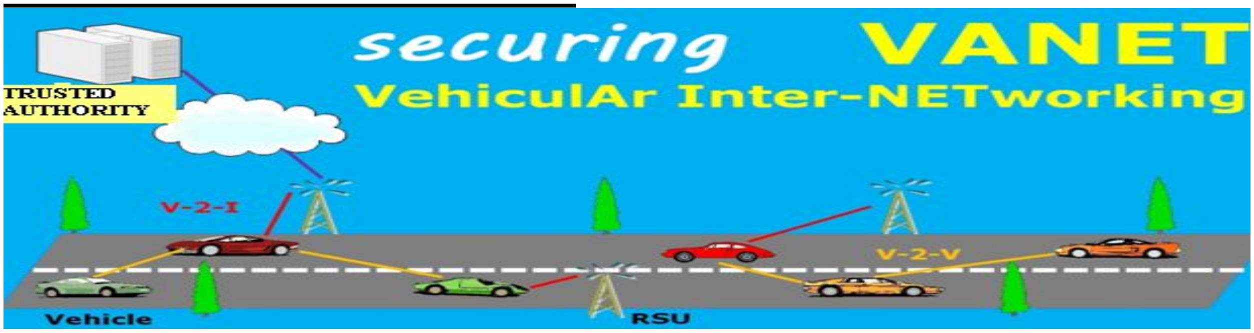
PROJECTS IN NS2

IEEE PROJECTS 2014 – 2015

NS 001: VANET–BASED SECURE AND PRIVACY-PRESERVING NAVIGATION

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, Computing real-time road condition is really tough and it is not achieved using GPS. In the **PROPOSED SYSTEM**, Initially A vehicle should be authenticated by Trusted Authority (TA) via RSU, only then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighboring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key. Finally it decrypts the message using its own private key. In the **MODIFICATION PROCESS**, network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm.

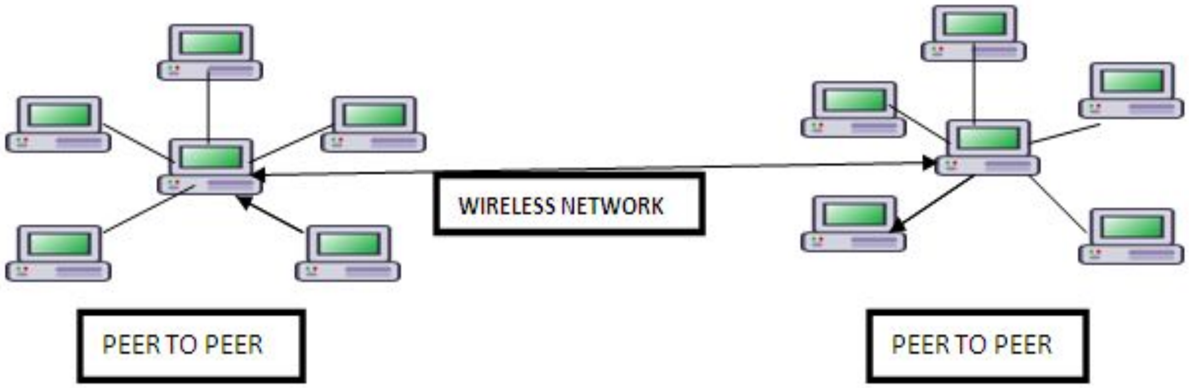
ALGORITHM / METHODOLOGY: CHORD ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed System, 2014

NS 002: RATELESS CODE BASED DATA DISCOVERY IN P2P NETWORK WITH ERASURE CODE

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, query resolution for locating resources and update information on their own resource status in these systems can be abstracted as the problem of allowing one peer. Communication overhead is high. In the **PROPOSED SYSTEM**, We are Identifying Interface Peer (IP), a node which has number of connections, in a wireless network. IP will collect all the resources in the rest of nodes in that network. Packets exchanged among the nodes in network using random walk principle. It‘s also used to avoid or control traffic. All data’s are encoded and decoded using Rateless Code. In the **MODIFICATION PROCESS**, we are using Erasure Code for encode and decode the original information. It will maximize the data persistence. It also reduces the time required to communicate the information.

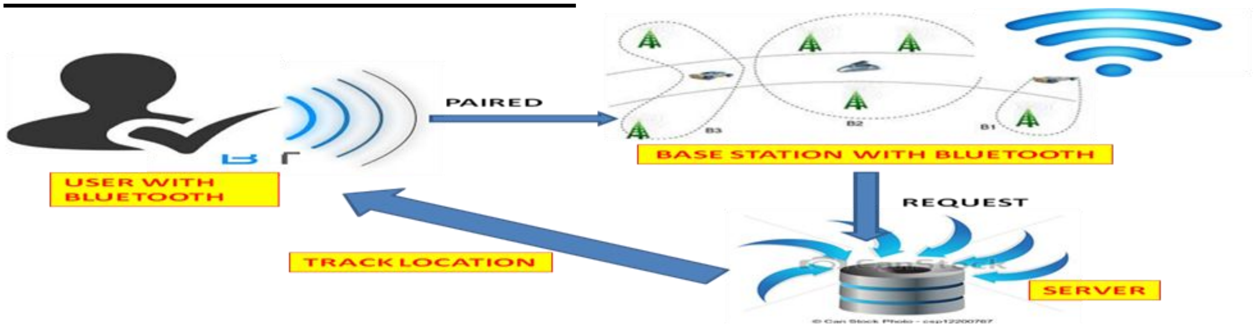
ALGORITHM / METHODOLOGY: ERASURE CODES

DOMAIN: Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Sensor Network, 2014

NS 003: IMPLEMENTATION OF COOPERATIVE TRACKING AND POSITION DETECTION FOR NON-GPS MOBILES USING BLUTOOTH TOWERS & GPS MOBILES

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM** the location of the person will be tracked only by the tower or GPS. In the **PROPOSED SYSTEM**, the main Aim of the Project is to Track Exactly the Non GPS Mobile User. The Bluetooth Server is deployed at different Areas and it's ID is transmitted to the Server. GPS Enabled will also Roam around the City everywhere. If Non GPS Mobile User is available within the Limit of Bluetooth Accessibility, then User's Location is easily tracked. If User is out of Bluetooth Coverage area, then GPS Enabled Users will communicate with Non GPS Users via Bluetooth and the location is communicated to the Server. In our **MODIFICATION**, User can download a File from the Server without GPRS Connection through Bluetooth Communication from Rest of the Users. We also find out the intruder based on primary key of GPS mobile user's using fast randomized algorithm.

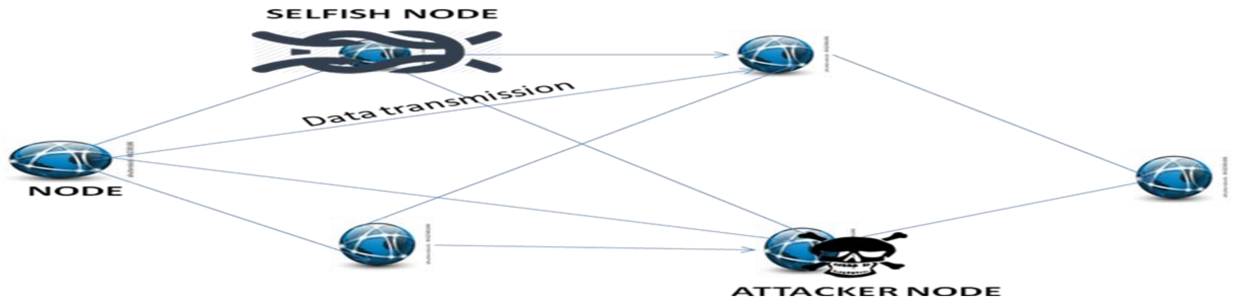
ALGORITHM / METHODOLOGY: FAST RANDOMIZED ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Transaction on Parallel and Distributed System, 2014

NS 004: IDENTIFICATION, DETECTION & ELIMINATION OF SELFISH & MALICIOUS NODES WITH BUFFER LEVEL MONITORING FOR SECURED DATA COMMUNICATION IN DTN

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM** there is no energy level will be maintained in the network also there is a packet loss between the network when the node try to transfer the data. In the **PROPOSED SYSTEM** we are Detecting Selfish & Malicious Nodes so that an Alternative Best Route is chosen. Selfish Nodes are Harmless but it will Transmit / Receive Data from their Friends List. Malicious Nodes will Drop / Redirect Packets once they are attacked. In the **MODIFICATION** part of this Project, we implement Information Centric Network (ICN) for validating the node history based on payoff calculation of node. It provides security and less time consumption. Before data transmission, ICN identifies the malicious node and selfish node based on Repetitive Trust Management and Adversary Detection scheme.

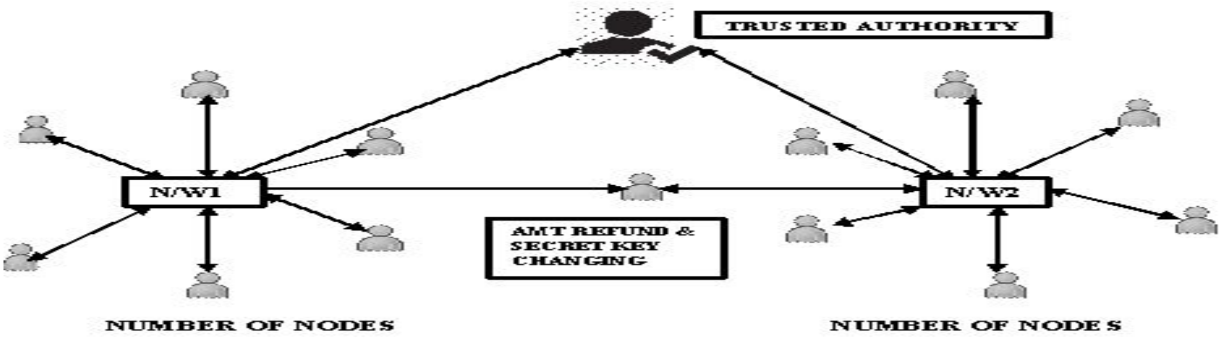
ALGORITHM / METHODOLOGY: MULTI-HOP FORWARDING ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Transaction on Parallel and Distributed System, 2014

NS 005: DETECTION OF NODE TRUSTWORTHY, HISTORY ANALYSIS, FLEXIBLE KEY GENERATION AND REWARD & PUNISHMENT SYSTEM IN DTN

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM**, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data. Routing misbehavior can be caused by Malicious nodes that drop packets or modifying the packets to launch attacks. Thus, pose a serious threat against the network performance of DTN. In the **PROPOSED SYSTEM,** we propose iTrust introduces a periodically available TA, which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then, TA could punish or compensate the node based on its behaviors. We assume that each node must pay a deposit amount before it joins the network, and the deposit will be paid back after the node leaves if there is no misbehavior activity of the node. TA could ensure the security of DTN routing at a reduced cost. **MODIFICATION** Secret key is generated on each node, which is used to share the data. The secret key is also automatically changed when the node joins a network and leaves a network based on fast randomized algorithm.

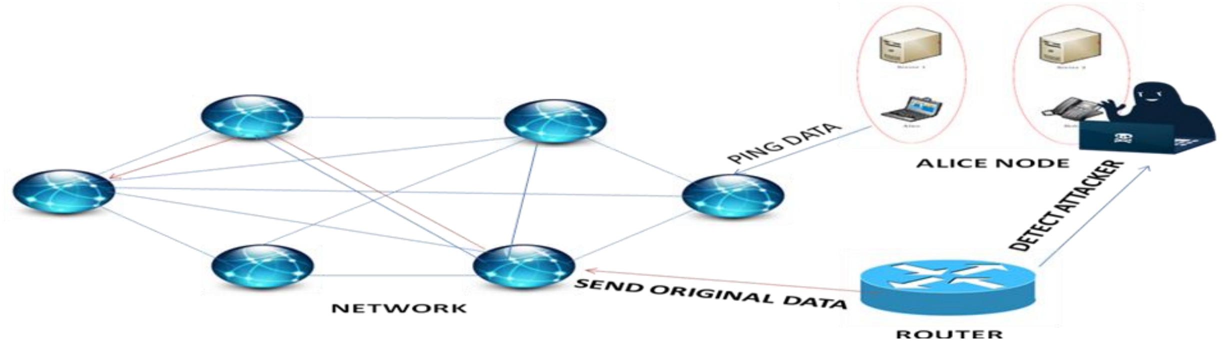
ALGORITHM / METHODOLOGY: BASIC MISBEHAVIOR DETECTION ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel and Distributed System, 2014

NS 006: ANALYSIS & MONITORING OF NETWORK NODE, ALICE NODE BEHAVIOR & BEST ROUTE IDENTIFICATION VIA SERVER DEPLOYMENT

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM** debugging the network is becoming very harder. There is a vast chance to lost the original packet. In the **PROPOSED SYSTEM** Alice node will examine the other node's behavior in the network and it will pass the sample packets to examine the node's Capacity in the Network. It will also identify the Best Route for Data Transfer. **MODIFICATION** of the Project is to verify the Behavior of the Alice Node. Attacker would attack the Alice and can change it's Behavior. Every Node has to report it's Data Transmitting / Receiving History to both Alice & Server Node. Alice Node will also report it's Examination Details to Server. Server Verify all the Nodes and also Alice Node Behavior. Network is monitored by both Alice & Server Node.

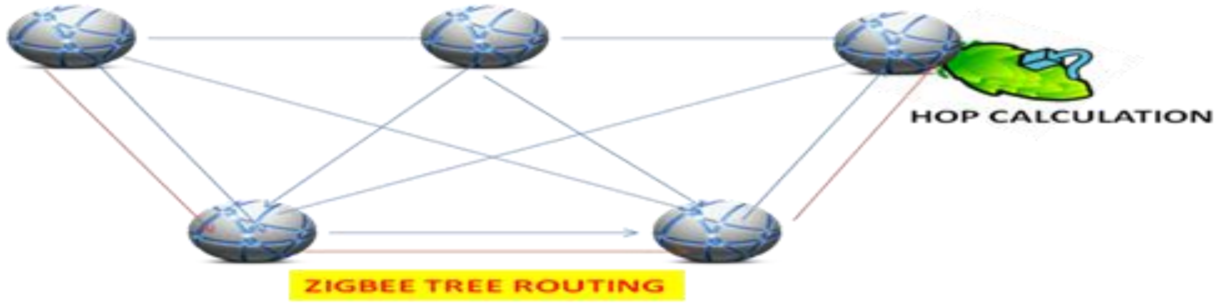
ALGORITHM / METHODOLOGY: TEST PACKET GENERATION ALGORITHM

DOMAIN: Networking, Security

IEEE REFERENCE: IEEE TRANSACTIONS on Networking, 2014

NS 007: IMPLEMENTATION OF AUTONOMOUS ROUTE DISCOVERY THROUGH SHORTEST ROUTING, ENERGY LEVEL, COST & INDEGREE

ARCHITECTUREDIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM**, DLSR & DSDU Protocols are used which causes long delay in Packets Transmission. In the **PROPOSED SYSTEM**, Zigbee based Data Transmission is used. Zigbee Tree Routing (ZTR) is used. Paper specifies to implement Shortcut Tree Routing (STR) to implement. In the **MODIFICATION** part of the Project, We implement this Project in both Wired and Wireless Environment instead of Zigbee. We implement of STR along with calculating Energy Level and Cost of Energy Node. Based on Hop Calculation, Cost & Energy Level of every Node Best Route is identified & Packets are transmitted. We also assign Coordinator Node to do these calculations based on Indegree Implementations.

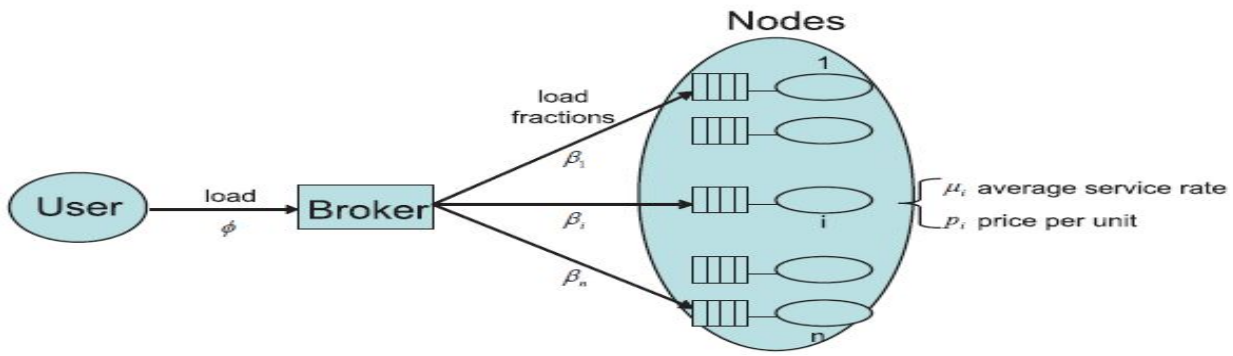
ALGORITHM / METHODOLOGY: STR PROTOCOL

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed System, 2014

NS 008: IMPLEMENTATION OF OPTIMISED COST, LOAD & SERVICE MONITORING FOR GRID COMPUTING

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM**, Managing Resources and Pricing them is a Challenging Task. There is no Win - Win Situation between resource Providers and Users. In the **PROPOSED SYSTEM**, Broker plays a vital role between users and Resource Providers. User will the Data and then Processed by the Broker. Service Providers will specify their Cost & Efficiency to Perform the Job. The main Objective is to identify the Optimum Cost and efficiency o the Grid Resource Providers. In the Modification part of the Project, Service Providers are deployed with Multiple Jobs. Based on the Job requested by the User, Broker will first find list of Resource Providers who can process the Work. Then work is splitted and allotted based on the Optimum Cost and the Performance.

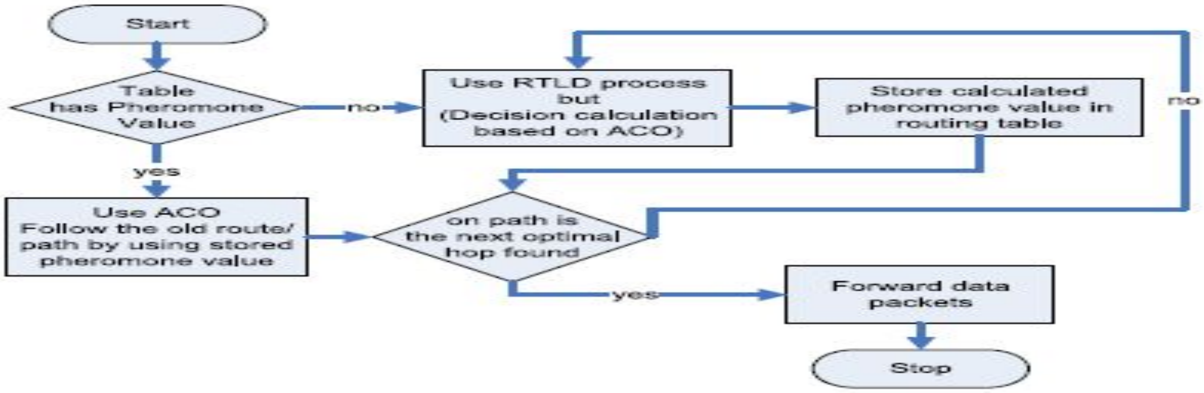
ALGORITHM/METHODOLOGY: OPTIMIZED PRICE CALCULATION, LOAD BALANCING

DOMAIN: Grid Computing, Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Computers, 2014.

NS 009: IMPLEMENTATION OF BIO INSPIRED ALGORITHM IN IDENTIFICATION OF BEST ROUTE VIA ANT COLONY OPTIMIZATION, ENERGY LEVEL & THROUGHPUT WITH ENCRYPTION

ARCHITECTURE DIAGRAM:


Start
Table has Pheromone Value
no
Use RTLD process but (Decision calculation based on ACO)
Store calculated pheromone value in routing table
no
yes
Use ACO Follow the old route/ path by using stored pheromone value
on path is the next optimal hop found
yes
Forward data packets
Stop

DESCRIPTION: In the **EXISTING SYSTEM**, The major factor to be tackled in the WSN is the network lifetime. A recent WSN routing protocol defined as secure real-time load distribution (SRTLD) uses broadcast packets to perform neighbor discovery and calculation at every hop while transferring data packets. Thus, it has high energy consumption. In the **PROPOSED SYSTEM**, BIOSARP has been designed to reduce the broadcast and packet overhead in order to minimize the delay, packet loss, and power consumption in the WSN using improved ant colony optimization (IACO). In IACO, the pheromone value/probability is computed based on routing table checking. Although it conducts recycling process based on node energy. In the **MODIFICATION** part of the Project, we also consider recycling node energy based on threshold value with TTL (time to live) during after data transmission for Secured Communication.

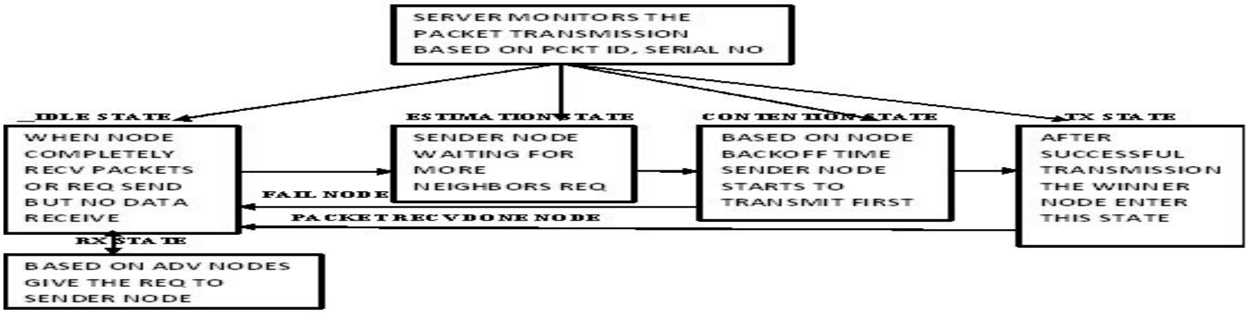
ALGORITHM / METHODOLOGY: **IACO, BIOSARP**

DOMAIN: Networking

IEEE REFERENCE: IEEE Journal on Sensors, 2014.

NS 010: LINK QUALITY AWARE CODE DISSEMINATION IN WIRELESS SENSOR NETWORKS

ARCHITECTURE DIAGRAM


SERVER MONITORS THE PACKET TRANSMISSION BASED ON PCKT ID, SERIAL NO
IDLE STATE
WHEN NODE COMPLETELY RECV PACKETS OR REQ SEND BUT NO DATA RECEIVE
ESTIMATION STATE
SENDER NODE WAITING FOR MORE NEIGHBORS REQ
CONTENTION STATE
BASED ON NODE BACKOFF TIME SENDER NODE STARTS TO TRANSMIT FIRST
TX STATE
AFTER SUCCESSFUL TRANSMISSION THE WINNER NODE ENTER THIS STATE
FAIL NODE
PACKET RECV DONE NODE
RX STATE
BASED ON ADV NODES GIVE THE REQ TO SENDER NODE

DESCRIPTION: In the **EXISTING SYSTEM,** needs multiple rounds of message exchanges, resulting in transmission redundancy based on code dissemination protocol (MNP) and long completion time based on link quality of nodes. In the **PROPOSED SYSTEM,** we are using Efficient Code Dissemination protocol (ECD) for increase the packet size to improve the transmission efficiency. Although based on received number of distinct request sender is selected because sender with more requests is suitable for transmission. The packet transmission is based on nodes back off time. ECD protocol has five states like IDLE, ESTIMATION, CONTENTION, RX and TX states. Suppose the node completely gets all packets, the winner node goes to TX State. The failed node goes to IDLE state. The IDLE state has two conditions, when node completely receives the packets and when a specified number of REQ message are sent and no DATA packets are received. In the **MODIFICATION,** server monitors the second sender node packet transmission based on checking the packet ID, packets serial number for security purpose. So it avoids the misbehaving activity of node.

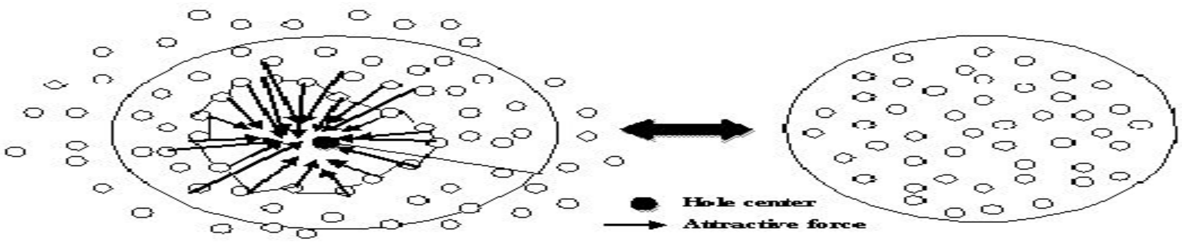
ALGORITHM / METHODOLOGY: **ECD, PACKET ID MONITORING**

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Parallel & Distributed Systems, 2014.

NS 011: LOCALIZED MOVEMENT-ASSISTED SENSOR DEPLOYMENT ALGORITHM FOR HOLE DETECTION AND HEALING

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **Existing System,** the emergence of holes in the Region of Interest is unavoidable due to the inner nature of WSNs, random deployment, environmental factors, and external attacks. Thus, an event occurring within these holes is neither detected nor reported and, therefore, the main task of the network will not be completed. In the **Proposed System,** to address the problem of hole detection and healing. The Distributed hole detection (DHD), is proposed to identify the boundary nodes and discover holes. We have conducted extensive simulations to validate DHD. Second, we present a virtual forces-based hole healing algorithm. Unlike existing algorithms, our algorithm relocates only the adequate nodes within the shortest times with the lowest cost. In the **Modification Process**, each and every nodes sending request to the hole manager and those manager received the all incoming messages from one location to the another location. So, it reduces time for sending error nodes message using Packet forwarding algorithm as well as the detection of the hole where replaced into the proper nodes due to the movable nodes.

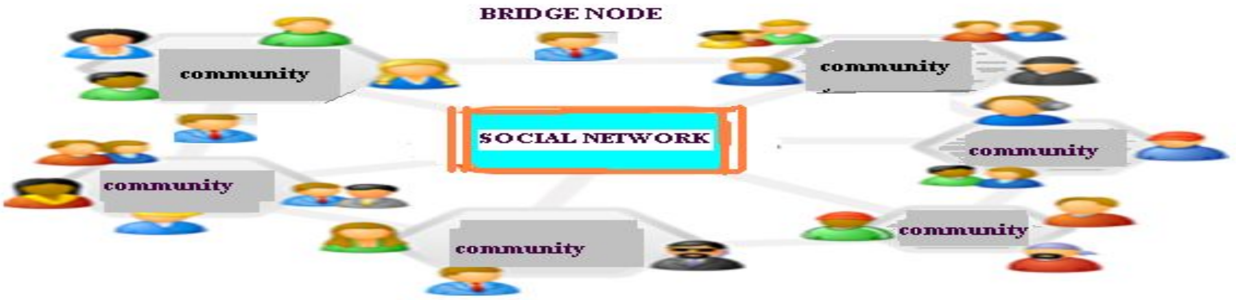
ALGORITHM /METHODOLOGY: VIRTUAL FORCE-BASED HOLE HEALING ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel & Distributed System, 2014

NS 012: ON SOCIAL DELAY-TOLERANT NETWORKING: AGGREGATION, TIE DETECTION, AND ROUTING

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **Existing System,** community structure could be affected once edge appearance or disappearance. It ignores node leaving from a community. In the **Proposed System,** each node maintains a local social graph and forward candidate set. Each community interconnected by edges or bridge node. Connection Strength Aware Routing Algorithm is used to address the problem of forward ordering, message copy control, buffer management and social-tie detection. Although new edge added in social graph, community structure on node shall be updated using Distributed Density Based Algorithm. In the **Modification Process,** We also detect the replica packet in more than one DTN based on packet ID.

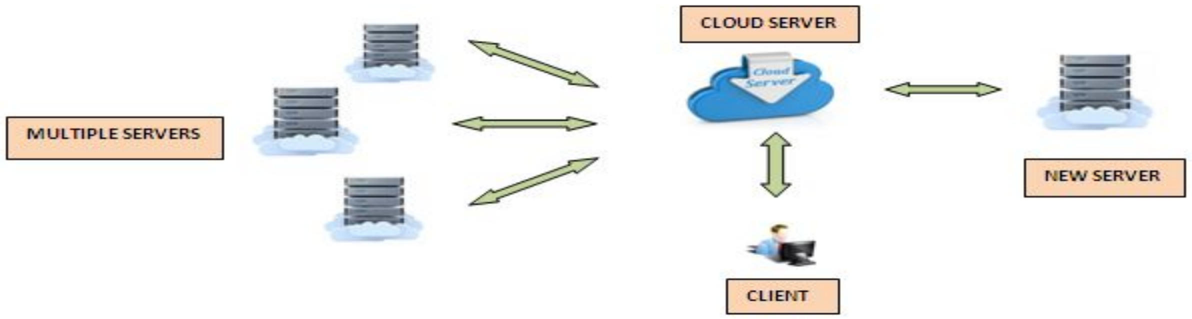
ALGORITHM / METHODOLOGY: CONNECTION STRENGTH AWARE ROUTING ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel & Distributed System, 2014

NS 013: ENABLING DATA INTEGRITY PROTECTION IN REGENERATING-CODING-BASED CLOUD STORAGE: THEORY AND IMPLEMENTATION

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM**, cloud computing uses MRPDP and HAIL method for regenerating code has to minimize repair traffic. In the **PROPOSED SYSTEM**, using Functional Minimum-Storage Regenerating-Data Integrity Protection (FMSR-DIP) codes for allow clients to remotely verify the integrity of random subsets of long term archival data under multi server setting. FMSR-DIP codes perform basic file operations Upload, Download, Check and Repair for 1. Read data from the other surviving servers, 2. Reconstruct the corrupted data of the failed server, and 3. Write the reconstructed data to a new server using NCCloud. FMSR-DIP codes preserve fault tolerance and repair traffic saving. **MODIFICATION** of this Project is Data is encrypted, splitted and stored in separate Servers. We use Erasure Code implementation for Code Reconstruction Technique. Auditor is deployed to verify the data

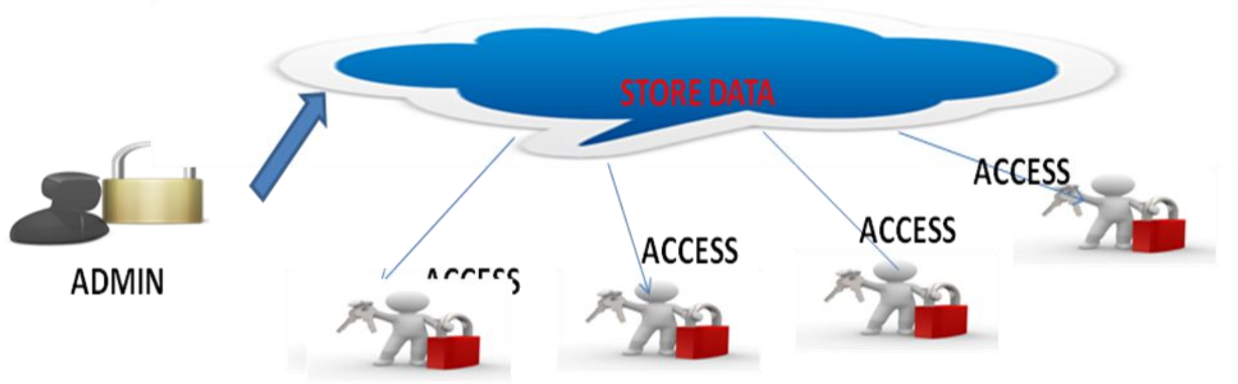
ALGORITHM / METHODOLOGY: ERASURE CODES

DOMAIN: Cloud Computing

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel & Distributed System, 2014

NS 014: PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN THE CLOUD

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **PROPOSED SYSTEM,** Data Owner updates the information to the Remote Cloud Server for Data Access. Data owner appoints Members of Data Utility and Data updation. Members have to get permission for the Data updation from the Data Owner. Members will have ther User Name, Key, Group Key for Access. Either If Existing member is removed from that Group, Group Key is automatically changed and updated to all the Members of that Group. The **MODIFICATION** is Group Key can be changed in case of New Member is added in that Group also. Member can Resign from the Group by themselves or Data Owner can Terminate the Member or can be Cloud Terminates the Member in case of Misbehavior (DDOS Attack, Same Data Download)

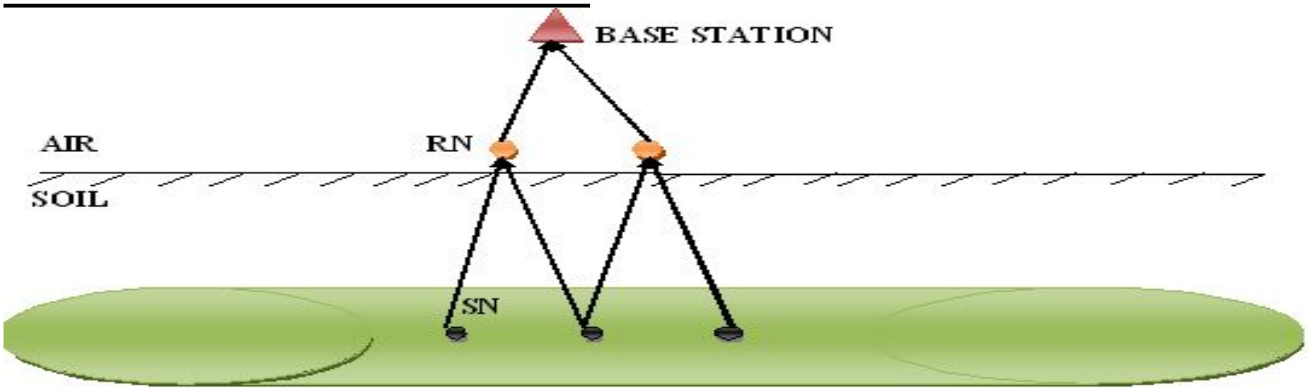
ALGORITHM / METHODOLOGY: FAST RANDOMIZED ALGORITHM

DOMAIN: Cloud & Security

IEEE REFERENCE: IEEE TRANSACTIONS on Services Computing, 2014

NS 015: CHANNEL-AWARE RELAY NODE PLACEMENT IN WIRELESS SENSOR NETWORKS FOR PIPELINE INSPECTION

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM,** radio propagation is complex because radio waves travel in a multi-medium environment. Finally, the SNs have limited energy supply. Therefore, proper deployment of a WSN is critical to providing reliable communications and efficient inspection. In the **PROPOSED SYSTEM,** we implement the channel-aware methodology for deploying above ground Relay Nodes in WSNs for underground pipeline inspection. Specifically, first, the paper provides a path loss model for radio propagation over multiple transmission media. Then, based on the path loss model a method is developed for optimum placement of the RNs so as to minimize the energy use of SNs and allow reliable communications.

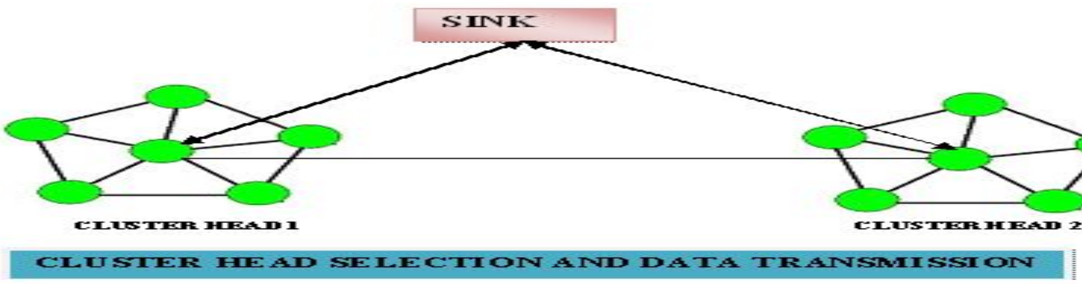
ALGORITHM / METHODOLOGY: THE PROPOSED SEARCH ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Wireless communication, 2014

NS 016: ENERGY EFFICIENT CLUSTER ARRANGEMENT IN MULTIHOP WIRELESS NETWORKS

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **Existing System,** a traditional setting, investigations on group communication focus on system reliability in the face of network failures or group member changes. In the **Proposed System,** sink selects the nodes to create a cluster head based on node energy. Each node transmit packet to sink through cluster head using packet distribution algorithm. After packet transmission sink conduct recycling process to select new cluster head based on node energy. Although the packet transmission each node affect active or passive attack based on external node arrival. Passive attack does not affect the packet transmission, node identify that attack itself. But each node mainly affected on active attack so it losses it energy. In the **Modification Process,** we introduce Intrusion Detection System (IDS) to detect the attack in cluster head. Sink to detect the active attack using IDS. Although cluster head check the new node arrival based on node id using localization algorithm. After identification of attacker, that attacker node goes to inactive state.

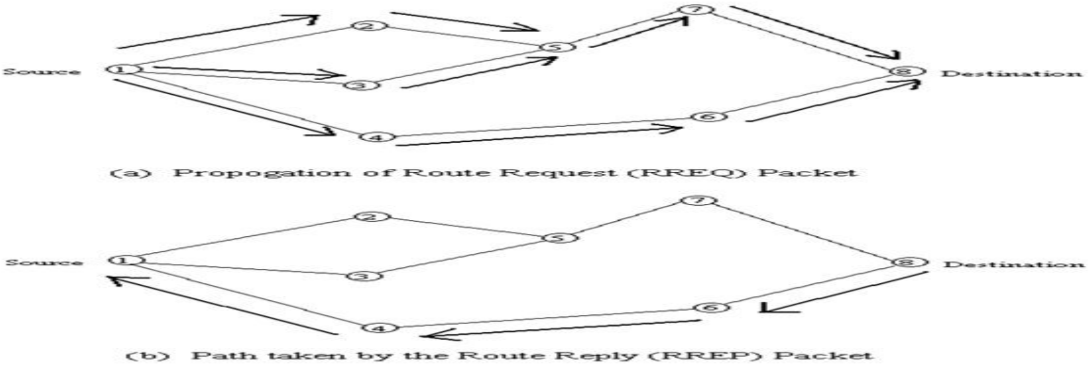
ALGORITHM / METHODOLOGY: LOCALIZATION ALGORITHM

DOMAIN: Network Security

IEEE REFERENCE: IEEE TRANSACTIONS on Vehicular Technology, 2014

NS 017: QOS AWARE GEOGRAPHIC OPPORTUNISTIC ROUTING IN WIRELESS SENSOR NETWORKS

ARCHITECTURE DIAGRAM



(a) Propogation of Route Request (RREQ) Packet

(b) Path taken by the Route Reply (RREP) Packet

DESCRIPTION: In the **EXISTING SYSTEM**, due to the mobility of the nodes in WSN, the Network faces a frequent link breakage problem which also leads to data loss, so it is time consuming process. However, the multipath routing approach suffers from a significant energy cost. In the **PROPOSED SYSTEM,** In proposed system, request is passed to all intermediate nodes based on node id and node color using forward candidate set. In routing table, each node has includes three colors like green color nodes intimates it already receives the request, red color nodes intimates it moves to another location based on send error message, black color nodes intimate idle state. If anyone neighbor node will receive the route error message, that node verify the candidate set then only it removes that node from list. After remove that node it automatically updated on table using EQGOR. In the **MODIFICATION PROCESS,** after completing the data transmission network conduct recycling process. Network recycles the node energy based on TTL.

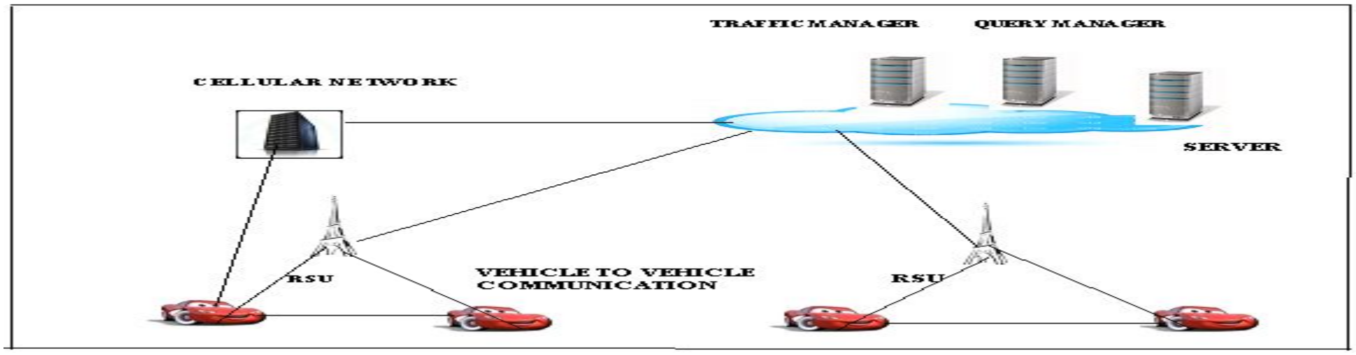
ALGORITHM / METHODOLOGY: EQGOR PROTOCOL

DOMAIN: NETWORKING

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed System, 2014

NS 018: CONTENT DOWNLOAD IN VEHICULAR NETWORKS IN PRESENCE OF NOISY MOBILITY PREDICTION

ARCHITECTURE DIAGRAM:



DESCRIPTION:

In the **EXISTING SYSTEM,** all vehicles are available for traffic relay whenever they are not receiving data from RSU. So it increases the time complexity. In the **PROPOSED SYSTEM,** user gives a request to the query management server via RSU or cellular network. Query manager forwards the pending request to RSU. Then RSU fetch portion of the content from server storing it. Finally they deliver the data to target downloader directly. Traffic manager collects information on the position, speed and heading cards through a real-time traffic monitoring system. So it predicts vehicle mobility and contacts. Contact prediction generated by the traffic manager based fog of war model. Although downloader acknowledges to content server, based on acknowledge it keeps track of data downloaded by each user. In the **MODIFICATION PROCESS,** if same Data is requested by another user system Verifies the Data is issued any other user, then the Data is downloaded directly from existing user and not processed by the server.

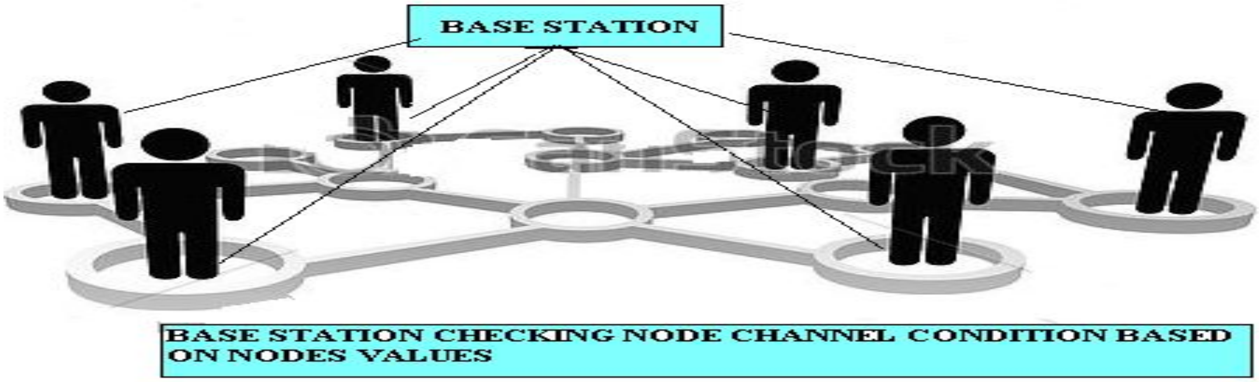
ALGORITHM / METHODOLOGY: OJF ALGORITHM

DOMAIN: Vanet

IEEE REFERENCE: IEEE Transactions on Mobile Computing, 2014

NS 019: A STUDY ON FALSE CHANNEL CONDITION REPORTING ATTACKS IN WIRELESS NETWORKS

ARCHITECTURE DIAGRAM:


BASE STATION
BASE STATION CHECKING NODE CHANNEL CONDITION BASED ON NODES VALUES

DESCRIPTION: In the **Existing System,** intermediate node can falsely report its channel condition via two ways. Underclaiming is not an effective attack but overclaiming node can maliciously intercept packets. In the **PROPOSED SYSTEM,** we implement secure channel condition estimation scheme, to prevent an overclaiming attacker. Base station sends a challenge (i.e. packet) to a user. Challenge includes a value known only to the base station. Upon receiving the challenge, a user returns the value in that challenge to the base station which can then compare the received value to the transmitted value. If both values are identical means that node is a good channel condition or not identical means that node has bad channel condition. In the **MODIFICATION PROCESS,** base station sends challenge to all nodes that challenge includes request need for not only that particular node channel condition value also includes neighbor node channel condition values. Based on those values it identifies the false channel condition node easily.

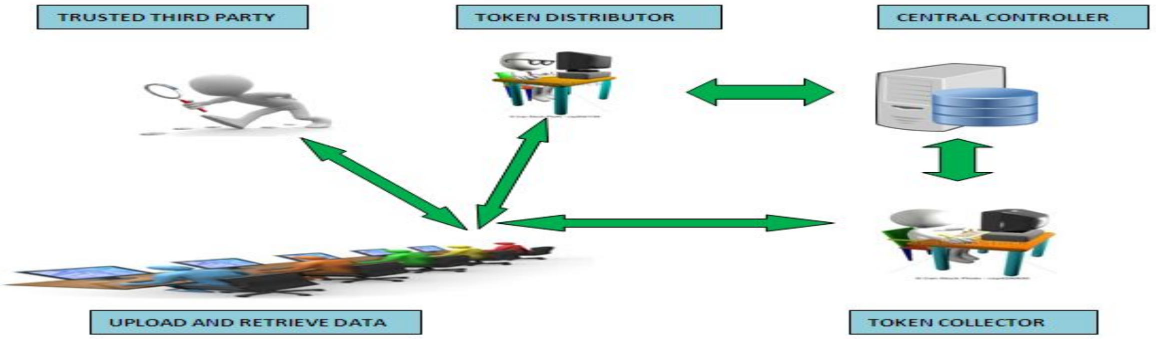
ALGORITHM / METHODOLOGY: SECURE CHANNEL CONDITION ESTIMATION SCHEME

DOMAIN: Network Security

IEEE REFERENCE: IEEE Transactions on Mobile Computing, 2014

NS 020: A SECURITY AND PRIVACY AWARE LOCATION-BASED REWARDING SYSTEM

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, Mobile Location-Based Services (MLBSs) have a lot of limitations and raise many concerns, especially about system security and user's location & identity privacy. In the **PROPOSED SYSTEM,** we develop a security and privacy aware location-based rewarding protocol for the LocaWard system. This protocol includes, Identity Initiation, Token Distribution and Token Redemption. In Identity initiation phase, Trusted Third Party (TTP) issues certificate in each Mobile User (MU) for authentication purpose. In Token distribution phase, Token Distributor (TD) is equipped with a Wi-Fi access point which can distribute location-based tokens based on MU request. TD also generates corresponding audition information and stores it in the Central Controller (CC) for future token verification. In Token redemption phase, Token Collector (TC) verifies the MU's token redemptions and reward the MU's with benefits. In the **MODIFICATION PROCESS**, Customer will be giving their Feedback about the Product & it's Usage and based on the Maximum Feedback Rating for a Particular Product, Our Portal would be giving Rewards to that Manufacturer.

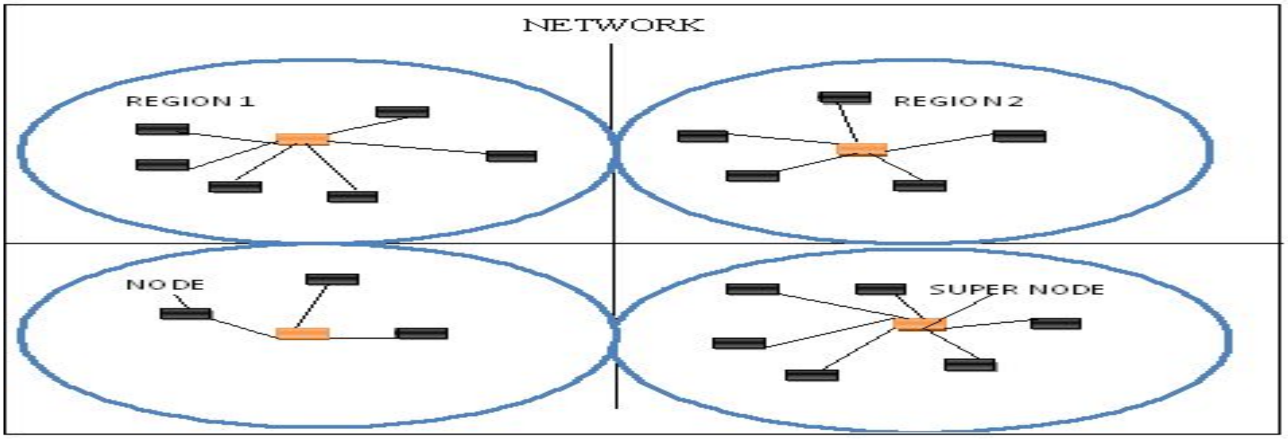
ALGORITHM / METHODOLOGY: LOCATION BASED REWARDING PROTOCOL (LOCAWARD)

DOMAIN: Mobile Computing

IEEE REFERENCE: *IEEE Transactions* on Parallel and Distributed System, 2014

NS 021: STARS: A STATISTICAL TRAFFIC PATTERN DISCOVERY SYSTEM FOR MANETS

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM,** it does not provide a method to identify the actual source and destination nodes. it is difficult to identify the end to end communication relations. Passive signal detectors can still eavesdrop on the wireless channels, intercept the transmissions, and then perform traffic analysis attacks. In the **PROPOSED SYSTEM,** Construct point-to-point traffic matrices using the TTL (time to live) based on statistical traffic pattern discovery system (STARS) protocol. Apply a neighbor statistical trust table algorithm to identify the actual source and relay nodes, and then correlate the source nodes with their corresponding destinations based on node table. It findout the passive attack in after data transmission based on intimation destination node. In the **MODIFICATION PROCESS,** we will implement Generalized STARS protocol to easily find out the passive attack based on super node of each region. It is easily identify the end to end communication relation.

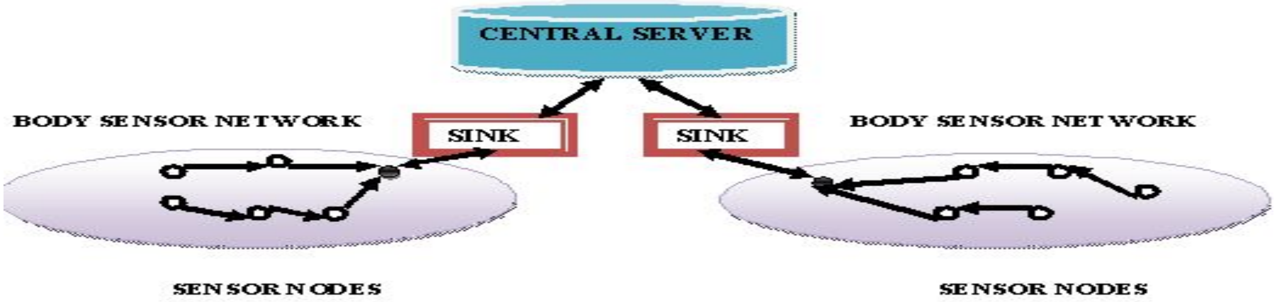
ALGORITHM / METHODOLOGY: STARS PROTOCOL

DOMAIN: Manet

IEEE REFERENCE: IEEE TRANSACTIONS on Dependable and secure computing, 2014.

NS 022: ENERGY-AWARE ROUTING FOR BIOMEDICAL WIRELESS SENSOR NETWORKS

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM,** wireless sensor networks targeting the domain of healthcare enables the development of new applications and services in the context of E-Health. Sensors are quite fragile and vulnerable to various forms of failure or depletion of their limited energy resources. In the **PROPOSED SYSTEM**, this paper offers a solution to increase the network lifetime based on a new Energy-Aware Objective Function used to design a Routing Protocol for Low-Power and Lossy Networks. The proposed Objective Function uses the Expected Transmission Count Metric and the Remaining Energy on each sensor node to compute the best paths to route data packets across the network. So EAOF prolongs the network lifetime and reduces the need for human intervention on battery changing, thereby enhancing the system wearability and reducing operational costs. In **MODIFICATION PROCESS**, we identify the unnecessary sensor request based on node location information using localization algorithm. So it saves node energy.

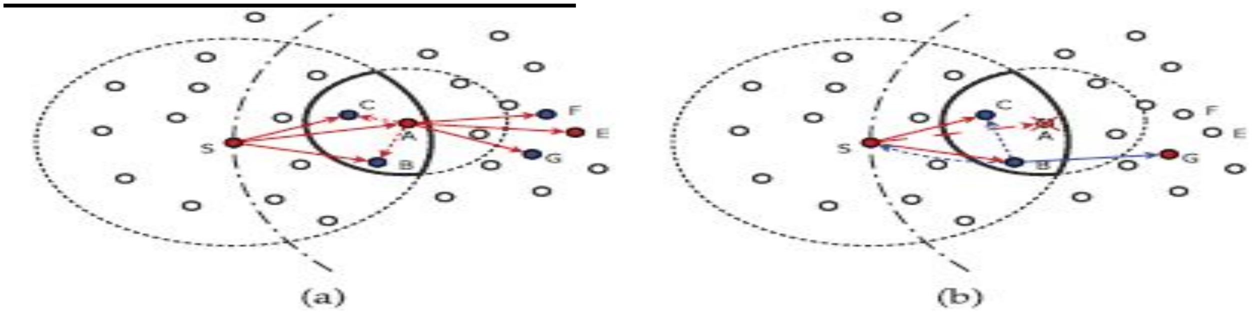
ALGORITHM / METHODOLOGY: EAOF, RIP

DOMAIN: Networking

IEEE REFERENCE: IEEE paper on HNAS, 2014

NS 023: ENABLING GRASSROOTS COMMUNICATION: A MEMORY-AIDED BROADCAST MECHANISM FOR AN AD HOC DEVICE-TO-DEVICE MOBILE NETWORK

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM,** it is very difficult to maintain a deterministic route. The discovery and recovery procedures are also time and energy consuming, energy consumption remains as a major obstacle for full deployment. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. In the **PROPOSED SYSTEM,** To minimize the communication energy consumption of the sensor node, the distance between the source and destination node is estimated before available transmission based on broadcasting the hello message. In our scheme called Environs Aware Broadcast Mechanism (EABA), a node gauges the local mobility around itself and uses that to decide which of two broadcast mechanisms to use. When mobility is high it uses SBA (Scalable Broadcast Algorithm), a well-known neighbor knowledge broadcast algorithm with relatively high overheads; but when mobility is low it switches to MaBA. After the route selection, the audio file is transmitted from source to destination node. The mobile nodes are goes to sleep mode, when node energy is minimized. In **MODIFICATION PROCESS**, it uses TTL (time to live) for estimating the energy consumption within the whole network.

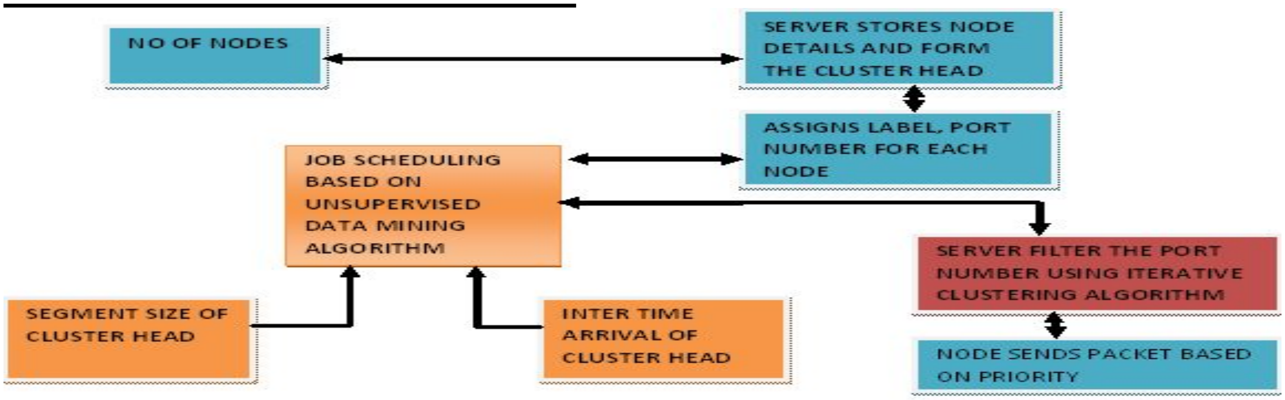
ALGORITHM / METHODOLOGY: ENVIRONS AWARE BROADCAST MECHANISM

DOMAIN: Mobile Ad-Hoc Networks

IEEE REFERENCE: *IEEE Transactions* on Communication, 2014

NS 024: SELECT: SELF-LEARNING CLASSIFIER FOR INTERNET TRAFFIC

ARCHITECTURE DIAGRAM


NO OF NODES
SERVER STORES NODE DETAILS AND FORM THE CLUSTER HEAD
ASSIGNS LABEL, PORT NUMBER FOR EACH NODE
JOB SCHEDULING BASED ON UNSUPERVISED DATA MINING ALGORITHM
SERVER FILTER THE PORT NUMBER USING ITERATIVE CLUSTERING ALGORITHM
SEGMENT SIZE OF CLUSTER HEAD
INTER TIME ARRIVAL OF CLUSTER HEAD
NODE SENDS PACKET BASED ON PRIORITY

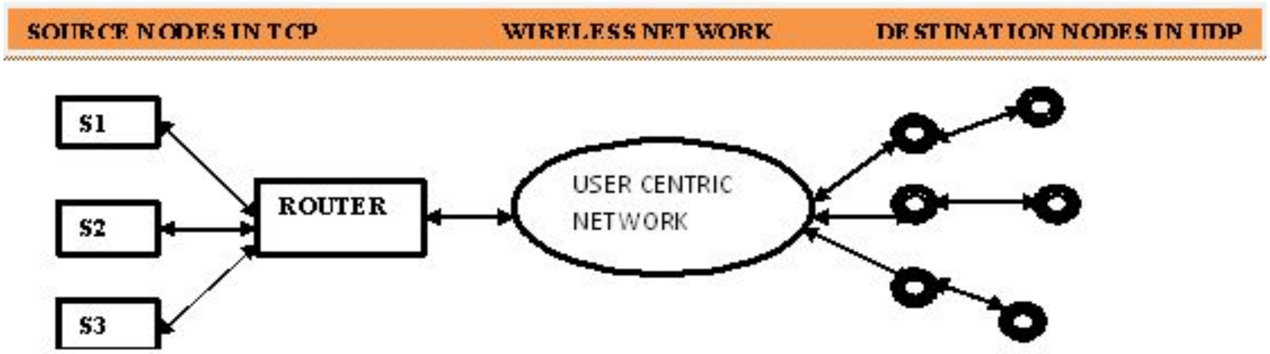
DESCRIPTION: In the **EXISTING SYSTEM,** Network visibility is a critical part of traffic engineering, network management, and security. The Deep Packet Inspection (DPI) , deeply rely on the availability of a training set. The DPI classifiers have some limitations. The classifiers can identify and visible only the specific applications, suppose traffic occurs means, it didn't allow the classification. In the **PROPOSED SYSTEM,** Unsupervised algorithms have been envisioned as a viable alternative to automatically identify and visible the classes of traffic based on segment size and inter time arrival of sub nodes. Unsupervised data mining algorithms to automatically split traffic into homogeneous subsets or clusters. Although server filter the port number based on iterative clustering algorithm for avoid traffic. In **MODIFICATION PROCESS**, we will introduce priority based on cluster head segment size for avoid time consumption.

ALGORITHM / METHODOLOGY: UNSUPERVISED DATA MINING ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Network and Service Management, 2014

NS 025: NETWORK RESOURCE ALLOCATION FOR USERS WITH MULTIPLE CONNECTIONS: FAIRNESS AND STABILITY ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM,** the problem of TCP in MANET's environment is clearly its disability to distinguish between losses induced by network congestion and types of losses. Because it uses wireless channels for the communication of ad hoc network nodes. So temporary link failure may occur frequently, these may lead to packet loss. In the **PROPOSED SYSTEM,** we implementing congestion control algorithm for avoiding packet loss in TCP with wireless network. Based on that source node sends packet to destination via router and user centric network. Although source node fix the time for packet transmission and receiving ACK. In the **MODIFICATION PROCESS,** we will provide threshold value for each node. Although source node sends packet to the destination node of the duration time means we will give a chance to increase the source node packet size transmission doubly in the Network.

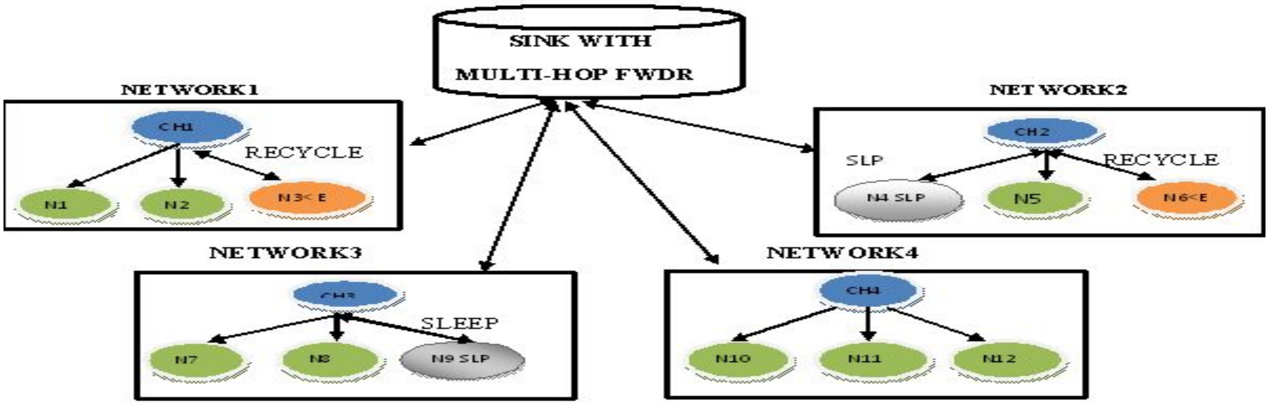
ALGORITHM / METHODOLOGY: CONGESTION CONTROL ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Networking, 2014

NS 026: LIFETIME MAXIMIZATION IN HETEROGENEOUS WIRELESS SENSOR NETWORKS USING MULTIPATH ROUTING TECHNIQUE

ARCHITECTURE DIAGRAM



DESCRIPTION: In **EXISTING SYSTEMS,** for delay in supporting real-time monitoring of every point of a region at all times and early detection of sensor node threats. However, sensor networks face serious obstacles like limited energy resources and high vulnerability to harsh environmental conditions that have to be considered carefully. A comprehensive framework for the use of wireless sensor networks for fault tolerant detection and monitoring. The framework is to detect a fault tolerant threat as early as possible and yet consider the energy consumption of the sensor nodes and the environmental conditions that may affect the required activity level of the network. In **PROPOSED SYSTEM,** it introduce threshold based TTL (time to live) for identifying energy level is less than approximate value. It is used to recycling energy level of the node. Through, it shows that how can recover fast fault while also consuming energy efficiently.

ALGORITHM / METHODOLOGY: MULTI-HOP FORWARDING ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Paper on IJSRP, 2014

BMQR
ISO/IEC 20000-1 CERTIFIED
ASCB(E) Accrediting Certifying Bodies
ISO / IEC 20000 CERTIFIED

INDIAN ECONOMIC DEVELOPMENT & RESEARCH ASSOCIATION
IEDRA
BHARTIYA UDYOG RATAN - AWARDED

BITS PILANI PRACTICE SCHOOL

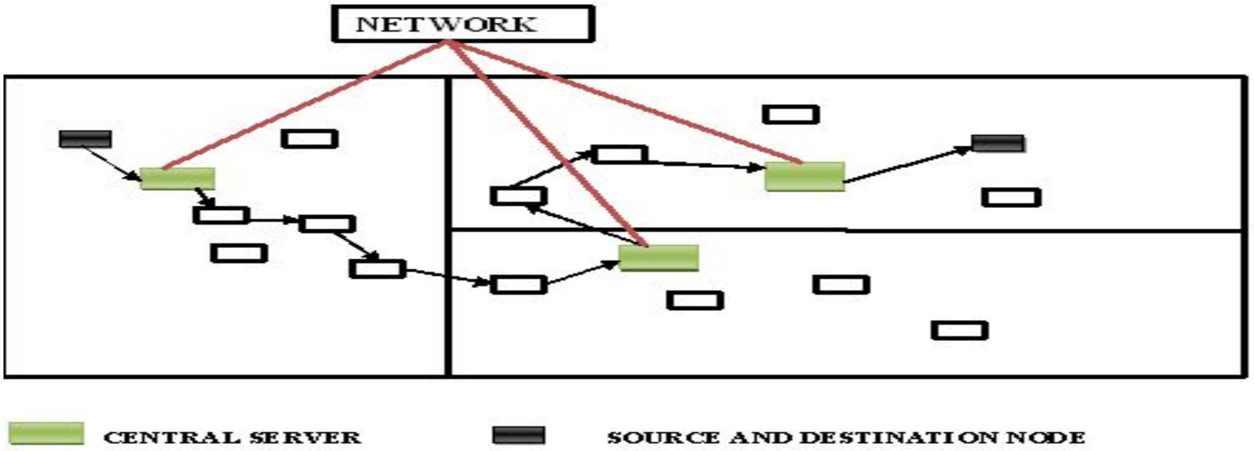
ISO AMERICAN GLOBAL STANDARDS 9001 CERTIFIED
AIAO-BAR QMS ACCREDITED
ISO 9001 : 2008 CERTIFIED

Page 26 of 38

77/2,HABIBULLAH ROAD, T. NAGAR, CH – 17. PH : 2834 2821 / 2822 / 2823

NS 027: ALERT: AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL IN MANETS

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM,** anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic, either generates high cost or cannot provide full anonymity protection to data sources, destinations, and routes. In the **PROPOSED SYSTEM,** we propose an Anonymous Location-based Efficient Routing protocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route using neighbor statistical trust table algorithm. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. In the **MODIFICATION PROCESS,** we will give threshold value for each node for avoiding reuse path many times. So it is used to avoid traffic network.

.

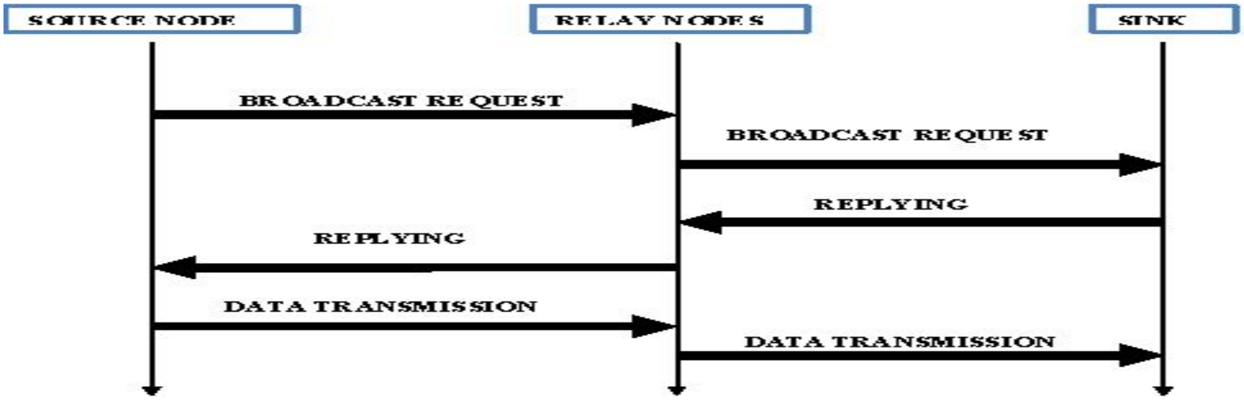
ALGORITHM / METHODOLOGY: ALERT PROTOCOL

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on mobile computing, 2013

NS 028: LIFETIME MAXIMIZING DYNAMIC ENERGY EFFICIENT ROUTING PROTOCOL FOR MULTI HOP WIRELESS NETWORKS

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, an unbalanced distribution of energy among the nodes may cause early death of nodes as well as network. Hence, balancing the energy distribution is a challenging area of research in wireless networks. In the **PROPOSED SYSTEM,** we propose an energy efficient scheme that considers the node cost of nodes for relaying the data packets to the sink. Source node sends request to all intermediate nodes based on energy aware routing algorithm for identifying node cost and relay node selection using centralized load balanced algorithm. Based on node reply source node selects the shortest path using spanning tree based routing algorithm. In the **MODIFICATION PROCESS,** we will provide low latency and energy saving based on neighbor table checking before broadcast the request.

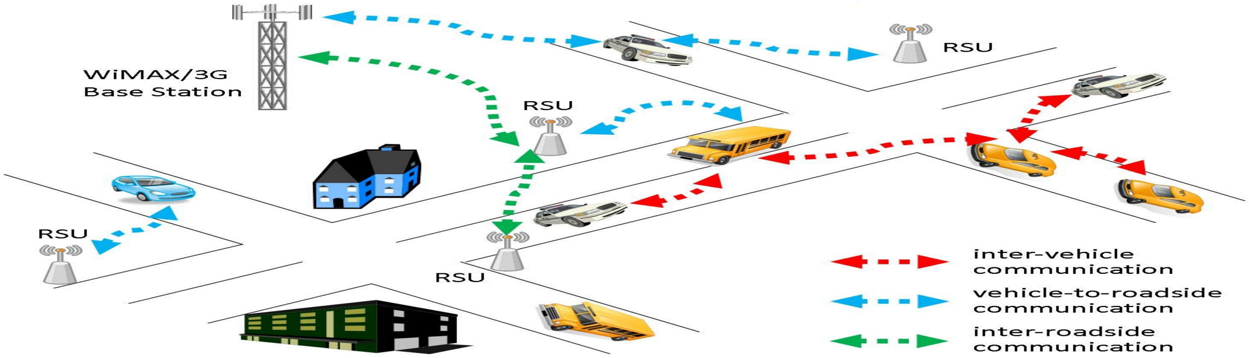
ALGORITHM / METHODOLOGY: ENERGY EFFICIENT ROUTING ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Journal on SIMPAT, 2013

NS 029: ADAPTIVE TRAFFIC SIGNAL CONTROL WITH VEHICULAR AD HOC NETWORKS

ARCHITECTURE DIAGRAM


WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

DESCRIPTION: In the **EXISTING SYSTEM,** the Vehicular Ad Hoc Network (VANET) applications work on the principle of periodic exchange of messages between each vehicle. However, a malicious vehicle can disseminate false traffic information in order to force other vehicles and vehicular authorities to take incorrect decisions by creating multiple virtual identities using different forged positions. In the **PROPOSED SYSTEM,** now the intelligent adaptive traffic control system is proposed in such a way that a traffic signal controller with wireless sensor receives the information from OBU vehicles such as position and speed. By using this information, it optimizes the traffic signal scheduling at the intersection. The traffic signal controller reduces the waiting time of the vehicle from the RSU and also it detects the position forging attacks occurring on VANET thereby providing security to passengers by using secret key. In the **MODIFICATION PROCESS,** we will randomly changes secret key of each vehicles while entering from one network to other network. Also find the alternate path due to traffic jam occurred, the RSU can get the best path chosen for vehicle can enter to the best path by sending request to specific network.

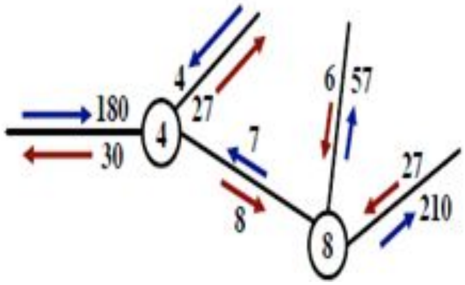
ALGORITHM / METHODOLOGY: OAF ALGORITHM

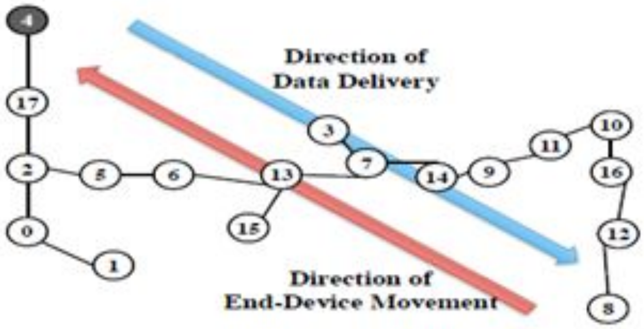
DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Vanet, 2013

NS 030: DESIGN OF ASSURED DATA DELIVERY USING INDEGREE AND CAPACITY CALCULATION

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.

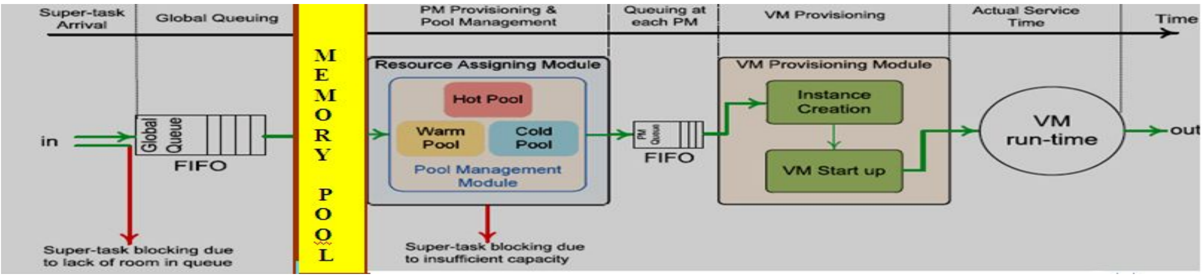
ALGORITHM / METHODOLOGY: ZND, ZTC, ZCD

DOMAIN: **Networking**

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

NS 031: GREEN COMPUTING BASED OPTIMIZED RESOURCE UTILIZATION IN CLOUD COMPUTING

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).

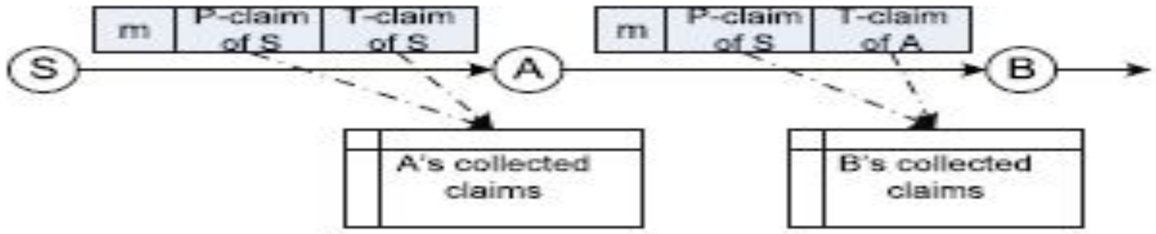
ALGORITHM / METHODOLOGY: Successive Substitution Method

DOMAIN: Cloud Computing, Green Computing

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

NS 032: DETECTION OF FLOODING ATTACKS AND CONTENT ANALYSIS IN DTN

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.

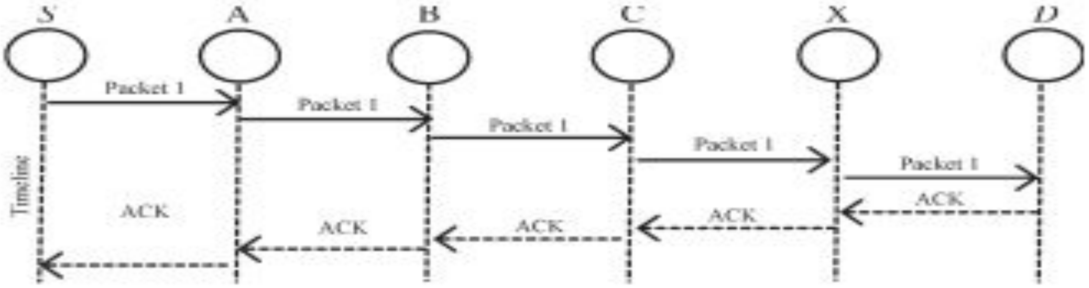
ALGORITHM / METHODOLOGY: PACKET FORWARDING SCHEME ALGORITHM

DOMAIN: Network Security

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

NS 033: IDENTIFICATION OF MISBEHAVIOUR AND PACKET LOSS ACTIVITIES IN MOBILE ADHOC NETWORKS.

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,** network assigns buffer level, TTL and key. Suppose anyone node it didn't send acknowledgement to previous node means network identify that misbehavior node based on key and intimates to source node.

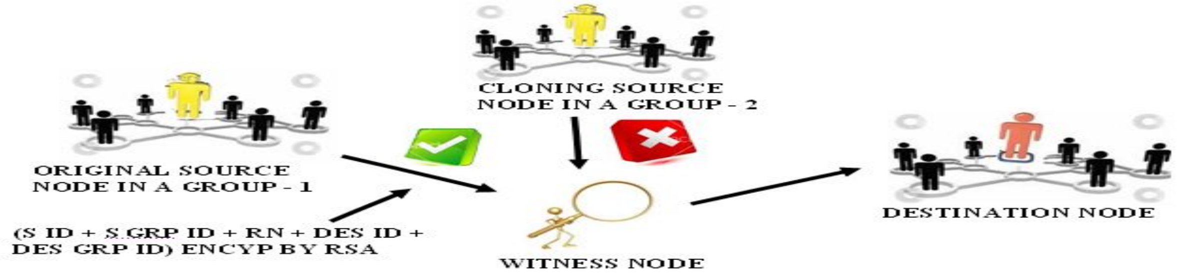
ALGORITHM / METHODOLOGY: RSA ALGORITHM

DOMAIN: Mobile Computing

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

NS 034: IDENTIFICATION OF CLONE NODES USING RDE AND CHORD ALOGORITHM WITH ENCRYPTION

ARCHITECTURE DIAGRAM



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.

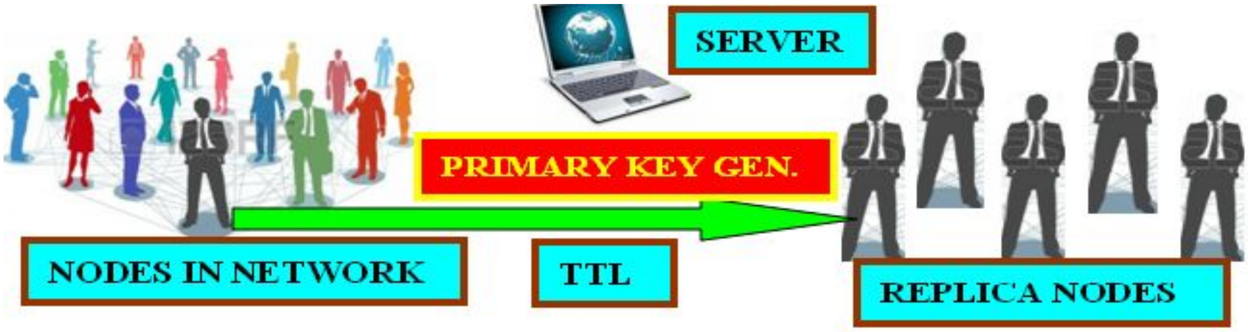
ALGORITHM / METHODOLOGY: CHORD ALGORITHM

DOMAIN: Network Security

IEEE REFERENCE: *IEEE Transactions* on Networking, 2013

NS 035: DETECTION OF REPLICATION ATTACKS WITH ALTERED PRIMARY KEY USING LOCALIZATION APPROACH & PRIORITY STATUS OF DELIVERY

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, Defending against Node Replication is not achieved in the Present System, only few methods are deployed. In the **PROPOSED SYSTEM**, using Localization Algorithm to identify the exact place of the original node which is verified and compared with the requested node to detect whether it is Replica or original node. We are monitoring Primary Key for every Node. In the **MODIFICATION**, this Primary Key will be changed on Random basis with Tine Stamp & as attack occurs. Source node will specify Time to Live (TTL) for every data Transmission, based on the TTL value Priority of the Packet is identified and transmitted accordingly.

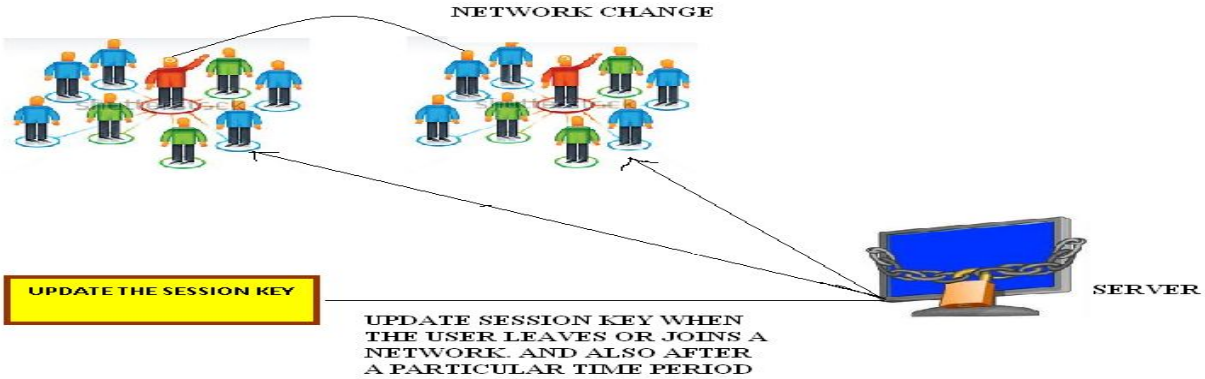
ALGORITHM / METHODOLOGY: LOCALIZATION ALGORITHM

DOMAIN: Network Security

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

NS 036: DYNAMIC KEY FOR SECURED COMMUNICATION AMONG THE FLEXIBLE NODES

ARCHITECTURE DIAGRAM


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

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.

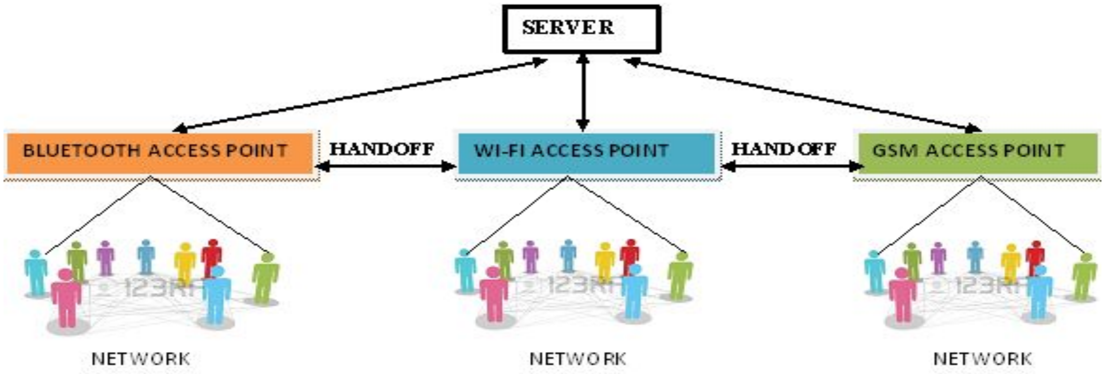
ALGORITHM / METHODOLOGY: **AES, RSA**

DOMAIN: **Wireless Ad-hoc Networks**

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

NS 037: MISSION-CRITICAL MANAGEMENT USING MEDIA INDEPENDENT HANDOVER

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM,** Natural disasters are an unexpected fact of life that may occur during unpredictable times and in unpredictable ways. Inefficiencies in the technology during rescue operation made the communication problematic. In the **PROPOSED SYSTEM,** we are implementing an adaptive network for media independent handover through multiple networks such as cellular network, GSM, Wi-Fi, Bluetooth for effective communication. We suggest Vertical Handoff among existing network to provide seamless communication. We propose Vertical Handoff Algorithm as an effective algorithm to choose the best network using a method Markov Decision Process, during Vertical Handoff for seamless communication. MDP chooses the best attributes (bandwidth, delay, packet loss, cost) to suggest the Vertical Handoff to decide the network for effective communication.

ALGORITHM / METHODOLOGY: VERTICAL HANDOFF ALGORITHM

DOMAIN: Networking

IEEE REFERENCE: IEEE Journal on CAIES, 2013

YOUR OWN IDEAS ALSO