2016-2017 NS2 PROJECTS LIST

S.NO	Project Code	IEEE 2016-17 NS2 Project Titles	Domain	Lang/Year
1	N1601	A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks	MANET	NS2/2016
2	N1602	D2D: Delay-Aware Distributed Dynamic Adaptation of Contention Window in Wireless Networks	MANET	NS2/2016
3	N1603	Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks	MANET	NS2/2016
4	N1604	Distance-Based Location Management Utilizing Initial Position for Mobile Communication Networks	MANET	NS2/2016
5	N1605	Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes	MANET	NS2/2016
6	N1606	Opportunistic Routing With Congestion Diversity in Wireless Ad Hoc Networks	MANET	NS2/2016
7	N1607	Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs	MANET	NS2/2016
8	JPN1608	Resisting Blackhole Attacks on MANETs	MANET (IEEE CONFERENCE)	NS2/2016
9	JPN1609	A Kautz-Based Wireless Sensor and Actuator Network for Real-Time, Fault-Tolerant and Energy-Efficient Transmission	WSN (Routing)	NS2/2016
10	JPN1610	CANS: Towards Congestion-Adaptive and Small Stretch Emergency Navigation with Wireless Sensor Networks	WSN (Routing)	NS2/2016

11	JPN1611	Cluster-Based Routing for the Mobile Sink in Wireless Sensor Networks With Obstacles	WSN (Routing)	NS2/2016
12	JPN1612	Code-Based Neighbor Discovery Protocols in Mobile Wireless Networks	WSN (Routing)	NS2/2016
13	JPN1613	DaGCM: A Concurrent Data Uploading Framework for Mobile Data Gathering in Wireless Sensor Networks	WSN (Routing)	NS2/2016
14	JPN1614	Dictionary Based Secure Provenance Compression for Wireless Sensor Networks	WSN (Routing)	NS2/2016
15	JPN1615	Distributed Emergency Guiding with Evacuation Time Optimization Based on Wireless Sensor Networks	WSN (Routing)	NS2/2016
16	JPN1616	Duplicate Detectable Opportunistic Forwarding in Duty-Cycled Wireless Sensor Networks	WSN (Routing)	NS2/2016
17	JPN1617	Fair Routing for Overlapped Cooperative Heterogeneous Wireless Sensor Networks	WSN (Routing)	NS2/2016
18	JPN1618	Geographic and Opportunistic Routing for Underwater Sensor Networks	WSN (Routing)	NS2/2016
19	JPN1619	iPath: Path Inference in Wireless Sensor Networks	WSN (Routing)	NS2/2016
20	JPN1620	Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks	WSN (Routing)	NS2/2016
21	JPN1621	Location aware sensor routing protocol for mobile wireless sensor networks	WSN (Routing)	NS2/2016
22	JPN1622	Maximizing Data Collection Throughput on a Path in Energy Harvesting Sensor Networks Using a Mobile Sink	WSN (Routing)	NS2/2016
23	JPN1623	Maximum Data Collection Rate in Rechargeable Wireless Sensor Networks with Multiple Sinks	WSN (Routing)	NS2/2016

24	JPN1624	Mobile Coordinated Wireless Sensor Network: An Energy Efficient Scheme for Real-Time Transmissions	WSN (Routing)	NS2/2016
25	JPN1625	NACRP: A Connectivity Protocol for Star Topology Wireless Sensor Networks	WSN (Routing)	NS2/2016
26	JPN1626	Privacy-Preserving Data Aggregation in Mobile Phone Sensing	WSN (Routing)	NS2/2016
27	JPN1627	RSSI-based Localization through Uncertain Data Mapping for Wireless Sensor Networks	WSN (Routing)	NS2/2016
28	JPN1628	Towards Distributed Optimal Movement Strategy for Data Gathering in Wireless Sensor Networks	WSN (Routing)	NS2/2016
29	JPN1629	DTMAC: A Delay Tolerant MAC Protocol for Underwater Wireless Sensor Networks	UWSN (Routing)	NS2/2016
30	JPN1630	A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks	WSN (Security)	NS2/2016
31	JPN1631	ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks	WSN (Security)	NS2/2016
32	JPN1632	Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks	WSN (Security)	NS2/2016
33	JPN1633	Analysis of One-Time Random Projections for Privacy Preserving Compressed Sensing	WSN (Security)	NS2/2016
34	JPN1634	Energy and Memory Efficient Clone Detection in Wireless Sensor Networks	WSN (Security)	NS2/2016
35	JPN1635	PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks	WSN (Security)	NS2/2016
36	JPN1636	Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes	WSN (Security)	NS2/2016

37	JPN1637	Traffic Decorrelation Techniques for Countering a Global Eavesdropper in WSNs	WSN (Security)	NS2/2016
38	JPN1638	A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks	VANET	NS2/2016
39	JPN1639	A Threshold Anonymous Authentication Protocol for VANETs	VANET	NS2/2016
40	JPN1640	ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks	VANET	NS2/2016
41	JPN1641	Coalition Formation for Cooperative Service-Based Message Sharing in Vehicular Ad Hoc Networks	VANET	NS2/2016
42	JPN1642	Contact-Aware Data Replication in Roadside Unit Aided Vehicular Delay Tolerant Networks	VANET	NS2/2016
43	JPN1643	DIVERT: A Distributed Vehicular Traffic Re-routing System for Congestion Avoidance	VANET	NS2/2016
44	JPN1644	Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks	VANET	NS2/2016
45	JPN1645	LORA: Loss Differentiation Rate Adaptation Scheme for Vehicle-to-Vehicle Safety Communications	VANET	NS2/2016
46	JPN1646	SCRP: Stable CDS-Based Routing Protocol for Urban Vehicular Ad Hoc Networks	VANET	NS2/2016
47	JPN1647	Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETs	VANET	NS2/2016
48	JPN1648	A Hop-by-Hop Routing Mechanism for Green Internet	WIRELESS COMMUNICATIONS	NS2/2016
49	JPN1649	Achieving Optimal Traffic Engineering Using a Generalized Routing Framework	WIRELESS COMMUNICATIONS	NS2/2016

50	JPN1650	Assessing Performance Gains Through Global Resource Control of Heterogeneous Wireless Networks	WIRELESS COMMUNICATIONS	NS2/2016
51	JPN1651	Contact Duration Aware Data Replication in DTNs with Licensed and Unlicensed Spectrum	WIRELESS COMMUNICATIONS	NS2/2016
52	JPN1652	Cost-Aware Caching: Caching More (Costly Items) for Less (ISPs Operational Expenditures)	WIRELESS COMMUNICATIONS	NS2/2016
53	JPN1653	Design of Scheduling Algorithms for End-to-End Backlog Minimization in Wireless Multi-Hop Networks Under -Hop Interference Models	WIRELESS COMMUNICATIONS	NS2/2016
54	JPN1654	DSearching: Using Floating Mobility Information for Distributed Node Searching in DTNs	WIRELESS COMMUNICATIONS	NS2/2016
55	JPN1655	Dynamic Network Control for Confidential Multi-Hop Communications	WIRELESS COMMUNICATIONS	NS2/2016
56	JPN1656	Embedding IP Unique Shortest Path Topology on a Wavelength-Routed Network: Normal and Survivable Design	WIRELESS COMMUNICATIONS	NS2/2016
57	JPN1657	Ghost-in-ZigBee: Energy Depletion Attack on ZigBee based Wireless Networks	Internet of Things (IoT)	NS2/2016
58	JPN1658	Improving Access Point Association Protocols Through Channel Utilization and Adaptive Probing	WIRELESS COMMUNICATIONS	NS2/2016
59	JPN1659	LAAEM: A Method to Enhance LDoS Attack	SECURE COMPUTING	NS2/2016
60	JPN1660	Mimicry Attacks Against Wireless Link Signature and New Defense Using Time-Synched Link Signature	SECURE COMPUTING	NS2/2016
61	JPN1661	PROVEST: Provenance-based Trust Model for Delay Tolerant Networks	SECURE COMPUTING	NS2/2016
62	JPN1662	Routing Protocol for Heterogeneous Wireless Mesh Networks	Mesh Networks	NS2/2016

63	JPN1663	Opportunistic Piggyback Marking for IP Traceback	SECURE COMPUTING	NS2/2016
64	JPN1664	Secure Transmission Against Pilot Spoofing Attack: A Two-Way Training-Based Scheme	SECURE COMPUTING	NS2/2016
65	JPN1665	Security Analysis and Improvements on Two Homomorphic Authentication Schemes for Network Coding	SECURE COMPUTING	NS2/2016
66	JPN1666	Thwarting Selfish Behavior in 802.11 WLANs	NETWORKING	NS2/2016
67	JPN1667	Mobility Prediction Based Joint Stable Routing and Channel Assignment for Mobile Ad Hoc Cognitive Networks	COGNITIVE NETWORK	NS2/2016
68	JPN1668	Detecting Node Failures in Mobile Wireless Networks: A Probabilistic Approach	MOBILE COMPUTING	NS2/2016
69	JPN1669	Local Anchor Schemes for Seamless and Low-Cost Handover in Coordinated Small Cells	MOBILE COMPUTING	NS2/2016
70	JPN1670	Robotic Message Ferrying for Wireless Networks using Coarse-Grained Backpressure Control	MOBILE COMPUTING	NS2/2016
71	JPN1671	TCP-Aware Backpressure Routing and Scheduling	MOBILE COMPUTING	NS2/2016
72	JPN1672	Virtual Multipath Attack and Defense for Location Distinction in Wireless Networks	MOBILE COMPUTING	NS2/2016

PROJECT SUPPORT TO REGISTERED STUDENTS:

1) IEEE Base paper.

2) Abstract Document.

3) Future Enhancement (based on Requirement).

4) Modified Title / Modified Abstract (based on Requirement).

5) Complete Source Code.

6) Final Report / Document

(Document consists of basic contents of about Abstract, Bibilography, Conclusion, Implementation, I/P & O/P Design, Introduction, Literature Survey, Organisation Profile, Screen Shots, Software Environment, System Analysis, System Design, System Specification, System Study, System Testing)

(The chapter System Design consists of 5 diagrams: Data Flow, Use Case, Sequence, Class, Activity Diagram)

7) Review PPTs and Documents.

8) How to Run execution help file.

9) NS2 Software Package (Cygwin, NS2.28, How to install help file).

10) International Conference / International Journal Publication based on your project.

WSN(Wireless Sensor Network)

1. **Effects of mobility on latency in a WSN that accommodates mobile nodes.**

Several applications have been proposed for mobile wireless sensor networks. Some of these applications require the transfer of a large amount of data in a short period of time. This is challenging, since mobility can lead to a deterioration in the quality of an established link. Frequent link disconnection may in turn require a mobile node to repeatedly establish new links with the surrounding relay nodes to proceed with the data transfer. The new link establishment may cause extra data communication latency and make most of the applications delay sensitive. To evaluate the effect of mobility on latency, this paper first sets up a mathematical model based on a hybrid medium access control (MAC) protocol in mobile scenarios. It then uses NS2 simulation to further analyze the latency associated with mobility. Both results show that the latency increases with an increment in the network density and the duty cycle.

2. **Leveraging SDN to Conserve Energy in WSN-An Analysis.**

Energy conservation is one of the serious problems faced by WSN as the sensor nodes have limited battery power and are expected to perform data aggregation and actuation functions in addition to sensing data. Literature has plenty of solutions proposed to reduce energy consumption and usage .With the recent upcoming technology of introducing network programmability that centralizes network management tasks using softwaredefined architecture (SDN), network trafficking is a prominent domain for applicability of SDN. Inherent traffic issues in WSN like data forwarding, aggregation of the data, path break and energy consumption can be efficiently handled by SDN, which provides a platform in which the data plane and the control plane are separated . By integrating SDN in WSN, the sensor nodes perform only forwarding and don't take any routing decision, due to which energy usage will be reduced. We propose a general framework for a software-defined wireless sensor network where the controller will be implemented at the base station, centre nodes in the cluster acts as switches and communication between the switch and the controller is via OpenFlow protocol. We realize the energy saving in the proposed architecture with the results obtained using NS2 and mininet emulator environments.

3. **A Fault Tolerant Approach to Extend Network Life Time of Wireless Sensor Network.**

In a wireless sensor network the delivery of the data packet from source to destination may be failed for various reasons and major due to failure-prone environment of networks. This may happen due to the topology changes, node failure due to battery, exhaust or breakdown of the communication module in the wireless node and results in the link failure. This paper addressed the major problem of link failure due to the failure of the nodes in the WSN and with the aim of providing robust solutions to satisfy the QoS-based stern end-to-end requirements of communication networks. In this paper, we propose the new solution by modifying the existing extended fully distributed cluster-based routing algorithm (EFDCB). In this proposed algorithm the faulty nodes or nodes that are more prone to failure in the every cluster of the network get identified by exchanging data and mutually testing among neighbor nodes. When we established the path between source and destination these faulty nodes get excluded in the path selection process and more stable, less prone to failure path will be formed. The performance of this new modified fault-tolerant fully distributed cluster-based routing algorithm is evaluated by simulating it in NS2 environment. Simulation results show that it performs better than the existing algorithm and provide novel solution for fault detection and fault management along the QoS paths and achieves a high degree of fault tolerance.

4. **An Autonomic in-Network Query Processing for Urban Sensor Networks.**

The sensing of urban environments usually takes into account the deployment of a large number of devices to measure their environmental attributes, such as temperature, pressure, humidity,

luminosity and pollution. In such applications, nearby sensors usually produce similar readings due to their spatial and temporal correlation. In the era of big data, management of collected data requires autonomous and scalable Wireless Sensor Network (WSN) structures. In this paper, we propose an in-network data storage model, called AQPM, that provides efficient processing of both spatial and value-based queries. AQPM is autonomous and scalable. That is, it does not rely on any central entity for neither managing data storage on sensor devices nor for processing queries. Scalability is achieved by grouping sensors with similar readings into clusters, while efficient query processing relies on the concept of repositories. Repositories are sensors that store readings of a set of clusters, and are the only ones that have to be contacted for answering queries. AQPM has been implemented on NS2 simulator and experimental results show that it is more effective than existing approaches.

5. **Efficient Route Update and Maintenance for Reliable Routing in Large-Scale Sensor Networks**

Reliable data transmissions are challenging in industrial wireless sensor networks (WSNs) as channel conditions change over time. Rapid changes in channel conditions require accurate estimation of the routing path performance and timely update of the routing information. However, this is not well fulfilled in existing routing approaches. Addressing this problem, this paper presents combined global and local update processes for efficient route update and maintenance and incorporates them with a hierarchical proactive routing framework. While the global process updates the routing path with a relatively long period, the local process with a shorter period checks potential routing path problems. A theoretical modelling is developed to describe the processes. Through simulations, the presented approach is shown to reduce end-to-end delay up to 30 times for large networks while improving packet reception ratio (PRR) in comparison with hierarchical and proactive routing protocols ROL/NDC, DSDV and DSDV with RPL's Trickle algorithm. Compared with reactive routing protocols AODV and AOMDV, it provides similar PRR while reducing end-to-end delay over 15 times.

6. **An Improvement On LEACH Protocol.**

Wireless sensor network (Wsn) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and orginizing the collected data at a central location.WSNs measure environmental conditions like temperature sound,pollution levels humidity,wind speed,direction,pressure..etc. Sensors are usually attached to microcontrollers and are powered by battery. Energy consideration is a critical issue for designing the routing protocols. Routig protocols are most important for the network while resources are limited. LEACH is one of the first heirerachical approaches for sensor networks. Most of the clustering algorithms are derived from this algorithm. In this paper we propose on the improvement on LEACH protocol. In our proposed algorithm ,network is logically divided into 4 zone. In first select the CH the node that close to center of every zone forward its location to BS. Then BS select node that are very closer than other node to center of regions. In addition residual energy of each node is also considered. We have evaluate LEACH ,PR-LEACH and Energy-zone LEACH (EZ-LEACH) through simulation using ns2 simulator which shows that LR-LEACH performs better than LEACH and PR-LEACH protocols.

7. **A Trust Based Secured Coordination Mechanism for WSAN.**

Wireless sensor-actor networks (WSAN) consist of a vast number of sensors and few actors. Generally, these networks are deployed in an unprotected environment to sense the physical world, and perform reliable actions on it. Hence, these networks are always susceptible to various kinds of passive and active attacks by malicious nodes. The back hole and gray hole attacks are part of active attacks. These attacks degrade the network efficiency and performance. In this paper, an efficient trust based secured coordination mechanism is proposed to counter the black hole and gray hole attacks on the delay and energy efficient routing protocol in sensor-actor networks. In the proposed

mechanism, each
sensor analyzes the trust level of its 1 − hop sensors based on the experience, recommendation, and knowledge. The analyzed trust value is transferred to the actor. The actor analyzes these values to identify the malicious nodes in its cluster region. The proposed trust based secured coordination mechanism (TBSC) is simulated using NS2. The performance is analyzed with respect to packet delivery
ratio, average energy dissipation in the network, and average end-to-end delay. The simulation results reveal that TBSC mechanism performs well for the delay and energy efficient routing protocol compared to the existing security mechanisms.

8. **Implementing Energy Efficient Technique for Defens against Gray-Hole and Black-Hole Attacks in Wireless Sensor Networks.**

In a Wireless Sensor Networks (WSNs), energy consumption is a key challenge due to its dynamic topology, highly decentralized infrastructure and resource constraint sensors. These entities make WSNs easily compromised by various denials of service attacks resulting in disastrous consequences. In the development of various cluster basedenergy efficient protocols to improve the lifetime of WSNs compromised with some malicious nodes, a challenging problem is how to adopt the most effective energy efficient cluster head selection approach to extend lifetime of WSNs. Gray-Hole and Black-Hole attack are those denial of service attacks that reduces the performance of WSNs. In order to achieve energy efficiency in WSNs, an efficient and trust based secure protocol is proposed to defend against single and cooperative Gray-Hole and Black Hole attacks. A proposed protocol incorporates efficient estimation to determine honest nodes during packets transmission phase. A proposed energy efficient technique is builds to evaluate in detecting and preventing compromised node to become cluster head. Besides, NS2 simulation result compare proposed protocol with LEACH proves that proposed system is efficiently reduces possibility of compromised node to be a part of network communication process and achieves better packet delivery ratio, throughput , less end-to-end delay and extend the lifetime of network significantly.

9. **Constructing A Shortest Path Overhearing Tree With Maximum Lifetime In WSNs**

Secure data collection is an important problem in wireless sensor networks. Different approaches have been proposed. One of them is overhearing. We investigate the problem of constructing a shortest path overhearing tree with the maximum lifetime. We propose three approaches. The first one is a polynomial-time heuristic. The second one uses ILP (Integer Linear Programming) to iteratively find a monitoring node and a parent for each sensor node. The last one optimally solves the problem by using MINLP (Mixed- Integer Non-Linear Programming). We have implemented the three approaches using MIDACO solver and MATLAB Intlinprog, and performed extensive simulations using NS2.35. The simulation results show that the average lifetime of all the network instances achieved by the heuristic approach is 85.69% of that achieved by the ILP-based approach and 81.05% of that obtained by the MINLP-based approach, and the performance of the ILP-based approach is almost equivalent to that of the MINLP-based approach.

10. **Energy Efficient Detection of Malicious Nodes Using Secure Clustering With Load Balance and Reliable Node Disjoint Multipath Routing in Wireless Sensor Networks**

In order to increase the network latency and resolve the security bottlenecks induced by the camouflaged malicious nodes in Wireless Sensor Networks, the residual energy and trust values are used to form a secured clustering, the network lifetime is increased by using the backup nodes in order to distribute theload among the secured clusters and reliable multipath node disjoint route discovery algorithm is proposed. The simulated experimental results in NS2 platform show that the

proposed method can minimize the effect of malicious nodes and improve the network lifetime for the sensor network by balancing the trust values and residual energy of sensor nodes.

11. New Hierarchical Stable Election Protocol for Wireless Sensor Networks

In wireless sensor networks energy is limited source. We must manage accurate use of energy for growing sensor lifetime. The hierarchy networks like Low-energy Adaptive Clustering Hierarchy (LEACH) choosing of cluster heads probability in some part of network haven't cluster head and other parts have cluster head with amount of density is high. Choosing of cluster heads in this algorithm done randomlyand it is probability low energy nodes was selected as cluster head. Thus fault has a high probability. This problem was solving by Stable Election Protocol (SEP). The New Hierarchical Stable Election Protocol (NHSEP) clustering is done symmetrically and the best node with respect to remained energy and distance of other nodes in comparing with each that selected as a cluster head. In this paper performance of the LEACH, SEP and NHSEP protocols have to evaluate and simulation results were carry out using NS2 simulator and compare with parameters Energy Consumed, Energy Remaining, Packet Delivery Fraction, End to End Delay and Dead Nodes.

12. Energy aware multicast routing in mobile ad-hocnetworks using NS-2

The nodes in MANET are constrained with limited power for their vital operations since the connectivity of the network will go down as soon as node energy gets exhausted. Node failures due to power constraints cause system failures and hence minimizes end-to-end connectivity in the network. In recent years, majority of research on multicast routing protocols in MANET focus upon the mechanisms to build energy efficient multicast routes based upon shortest paths and energy consumption for various transactions at node level. In this paper, we propose an Energy Aware Multicast Routing Protocol (EAMRP) which maximizes end-to-end connectivity in the network and minimizes faults at link or/and node level. A set of multiple paths are established from source to multicast destinations using energy efficient neighbor node selection mechanism. Our scheme operates in following phases. (1) Computation of residual energy of a node using node energy model. (2) Pruning the nodes having residual energy less than threshold value. (3) Discovery of multiple routes to the destination using request and reply packets, (4) Selection of stable routes by considering residual energy of the nodes. (5) Route maintenance for route breaks and node failures due to energy drain and (6) Simulation analysis for various parameters such as Packet Delivery Ratio (PDR), and end-to-end delay has been performed. We observe that EAMRP outperforms the energy efficient AODV and AOMDV protocols for various performance Parameters.

VANETS

13. SOLVING TRAFFIC CONGESTION –AN APPLICATION OF VANET

Vehicular Ad Hoc Network (VANET) is an evolving technology of today's world and is expected to be all pervasive in the near future. The vehicles in VANET possess mobility as well as computational processing power. The vehicles collaboratively form the ad-hoc network and are peers of each other. This paper discusses solving Traffic Congestion as an application of VANET. We have simulated the work of mobility on Network Simulator Tool(NS2),in which we have simulated the traffic roads with the help of SUMO(Simulation of urban mobility) using routing protocol AODV.

14. A novel mechanism for detecting DOS Attack in VANET using Enhanced

Attacked Packet Detection Algorithm (EAPDA)

Security is the major concern with respect to the critical information shared between the vehicles. Vehicular ad hoc network is a sub class of Mobile ad hoc network in which the vehicles move freely and communicate with each other and with the roadside unit (RSU) as well. Since the nodes are self organized, highly mobile and free to move therefore any nodes can interact with any other node which may or may not be trustworthy. This is the area of concern in the security horizon of VANETs. It is the responsibility of RSU to make the network available all the time to every node for secure communication of critical information. For this, network availability occurs as the major security requirement, which may be exposed to several threats or attacks. The vehicles and the RSU are prone to several security attacks such as masquerading, Sybil attack, alteration attack, Selfish driver attack, etc. Among these Denial of Service attack is the major threat to the availability of network. In order to shelter the VANET from DoS attack we have proposed Enhanced Attacked Packet Detection Algorithm which prohibits the deterioration of the network performance even under this attack. EAPDA not only verify the nodes and detect malicious nodes but also improves the throughput with minimized delay thus enhancing security. The simulation is done using NS2 and the results are compared with earlier done work.

15. **Performance Evaluation of an Enhanced Hybrid Wireless Mesh Protocol (E-HWMP) for VANET.**

In this paper we evaluate Enhanced Hybrid Wireless Mesh Protocol (E-HWMP), an enhanced version of HWMP based on IEEE802.11p and IEEE802.11s standards, especially created for Vehicular Ad-hoc Networks (V ANETs). An enhanced gateway selection algorithm for multi-hop relay in VA NET-LTE integration network is proposed. In the proposed algorithm the gateway selection is implemented using the E-HWMP protocol. The proposed gateway selection algorithm aims to improve the handoff efficiency and increasing the data rate while minimizing the average delay and overhead. Therefore, a multi-hop routing over the V ANET network is designed. NS2 simulator is used to evaluate the system performance of the proposed gateway selection algorithm (E-HWMP). The results show that, compared to conventional methods, the proposed algorithm significantly improves the system performance in terms of packets delivery ratio, overhead and average end-to-end delay.

16. **A Hybrid Model to Extend Vehicular intercommunication V2V through D2D Architecture.**

In the recent years, many solutions for Vehicle to Vehicle (V2V) communication were proposed to overcome failure problems (also known as ‘dead-ends’). This paper proposes a novel framework for V2V failure recovery using Device-to-Device (D2D) communications. Based on the unified Intelligent Transportation Systems (ITS) architecture, LTE-based D2D mechanisms can improve V2V ‘dead-ends’ failure recovery delays. This new paradigm of hybrid V2V-D2D communications overcomes the limitations of traditional V2V routing techniques. According to NS2 simulation results, the proposed hybrid model decreases the end to end delay (E2E) of messages delivery. A complete comparison of different D2D use cases (best & worst scenarios) is presented to show the enhancements brought by our solution compared to traditional V2V techniques.

17. **Performance Evaluation of Manet Using Quality of Service Metrics.**

An ad hoc network is a collection of mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Several routing protocols have been proposed for ad hoc networks and prominent among them are Ad hoc On Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR). Effort has been made to merge software Quality assurance parameters to adhoc networks to achieve desired results. This Paper analyses the performance of AODV and DSR routing protocols for the quality assurance metrics. The performance differentials of AODV and DSR protocols are analyzed using NS-2 simulator and compared in terms of quality assurance metrics applied.

18. **Power Aware and Topology Aware Ad-Hoc On-Demand Multipath Distance Vector Routing For Manet.**

The objective of this work is to improve the performance of a MANET multi-path routing protocol without increasing or decreasing its default transmission range of the nodes. The proposed work is to control the routing process and only allow hops with maximum possible distances in a route based on the received signal strength at each node. We propose topology aware and power aware ad hoc on-demand multipath distance vector routing protocol based on the maximum transmission range. We call this model as AOMDV_RR Range Routing and implemented it under ns2 by improving the standard AOMDV protocol. We studied the proposed AOMDV_RR and the standard AOMDV under different network densities and measured the performance for suitable metrics. Measurable difference in performance was realized and the proposed AOMDV_RR performed better than normal AOMDV with respect to metrics network overhead, throughput and energy consumption.

19. Quality of Service Routing for Multipath Manets.

Adhoc network design goal is to provide internet access anytime characterized by lack of infrastructure and absence of base station, mobility and heterogeneity which require a dynamic efficient routing protocol. We proposed a delay energy aware routing protocol called as reactive congestion aware multipath routing protocol-RCRP aim to select the route based on energy reduction rate and packet delivery time it address . Two important characteristics of mantes: # improving life time of networks and avoiding congestion. # It consider the node energy reduction rate(ERR) and packet delivery time(Pdt)
to compute the delay energy drain rate(d.e.d.r) optimistically with respect to current energy and traffic condition. The simulation result shows that this work is better than existing AOMDV and MM-AOMDV in
terms of networks life time and end to end delays by using NS2.

20. Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes

With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Over the years, emphasis has also been placed on improving the security of these networks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation, we demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable. Last, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

21. An Energy Management Framework For Smart Factory based on context-awareness.

In this paper,an Energy management framework for smart factory illustrated on context-awareness. The smart factory composed of three layers ,and IoT sensors are deployed in the smart factrories and used to collect many kinds of data including personnel, equipment, and environment. The first layer , data control and collection layer,colects and send environmental and control data to the second layer. And the second layer, Energy management based on context-awareness layer,analyses the data and infers the context from them. Finally ,the energy service layer provides Energy management service to users throug monitoring and controlling the status of Energy consumption. Using the protocol scheme ,users can monitor their Energy consumption, and control thier utilities and equipment to aviod energy leakage.

22. A Proposed Framework for Protection of Identity Based Attack in Zigbee.

ZigBee is used for emerging standard of lowpower, low-rate wireless communication which aims at interoperability and covers a full range of devices even including low- end battery-powered nodes. Zigbee is a specification for a suite of high-level communication protocols used to create personal area network built from small network. Zigbee network are vulnerable to Sybil attack in which a Sybil node send forges multiple identities to trick the system and conduct harmful attack. We propose a Sybil attack detection and prevention method using distance and address of node in Zigbee. In this technique, trusted node verifies other nodes and identifies the malicious node. We will implement this technique using NS2 with AODV protocol for mesh topology.

NS2 Project List

1. **A Global Approach for the Improvement of UHF RFID Safety and Security**

Radio Frequency Identification (RFID) devices are widely used in many domains such as tracking, marking and management of goods, smart houses (IoT), supply chains, etc. However, there is a big number of challenges which must still be overcome to ensure RFID security and privacy. In addition, due to the low cost and low consumption power of UHF RFID tags, communications between tags and readers are not robust. In this paper, we present our approach to evaluate at the same time the security and the safety of UHF RFID systems in order to improve them. First, this approach allows validating UHF RFID systems by simulation of the system behavior in presence of faults in a real environment. Secondly, evaluating the system robustness and the security of the used protocols, this approach will enable us to propose the development of new more reliable and secure protocols. Finally, it leads us to develop and validate new low cost and secure tag hardware architectures.

2. **A Novel Resource Scheduling Approach to Improve the Reliability of Shuffle-Exchange Networks**

Approaches such as increasing the number of intermediate stages are introduced to increase the reliability and throughput of Multistage Interconnection Networks (MINs). However, they mainly try to change the network architecture to achieve the goal of having more reliable network. When multiple sources in such a network try to send data, collision of packets and blocking problems are inevitable. Using existing networks, they cant be prevented completely and a multiple access protocol must be used to that end. Time division multiple access (TDMA) protocol can be used to overcome these problems. To improve the performance of this protocol, we propose an adaptive slot allocation approach using Monte Carlo random sampling method. This approach is applied to Shuffle-exchange network (SEN) and Shuffle-exchange network with one additional stage (SEN+). Results for 4000 simulation cycles using Network Simulator 2 (NS2) show that the new SENs perform better in terms of reliability and throughput compared to their regular types.

3. **Channel Selection Scheme for Cooperative Routing Protocols in Cognitive Radio Networks**

In this work, we propose CSCR, a channel selection scheme for cooperation-based routing protocols in cognitive radio networks. The proposed scheme increases the spectrum utilization through integrating the channels selection in the route discovery phase of the cooperation-based routing protocols. The best channels, that are less congested with primary users and that lead to minimum switching overhead, are chosen while constructing the cooperative group. Evaluating CSCR via NS2 simulations shows that it outperforms its counterparts in terms of goodput, end-to-end delay, and packet delivery ratio. The proposed scheme can enhance the network goodput, in some cases, by more than 150%, as compared to other related protocols.

4. **Network Delay Modeling in Mobile Wireless Mesh Networks using Network Tomography**

Network Tomography is a statistical inverse problem which estimates the traffic intensities in the network for a dynamic environment using a probabilistic approach. Wireless Mesh Networks (WMNs) is very strongly perceived as the future of wireless networking technology. The WMNs have a stable topology. However, Mobile Clients (MCs) in general are very active between Mobile Routers (MRs) which is referred as Mobile WMN (MWMN). It is the normal tendency of the nodes in WMNs to select the path with minimum number of hops or the shortest possible path to carry out

their transmissions but still it doesn't give full proof guarantee that the path being efficient and of good quality. In order to avoid this, we will require routing metric for choosing the most efficient path. Using Network Tomography which is a methodology for estimating the intensities of traffic for source-destination from link data to obtain end-to-end delay measurements with minimal or no co-operation from nodes is expected, we carry out NS2 simulations. These simulations gives the results of the proposed inverse problem approach that estimates the network performance parameter such as network delay and prefatory results for network tomography application in MWMN's in dynamic environment.

5. Performance analysis of Zigbee WDSN using clustering protocol and STR algorithm

In recent years, wireless networking plays a prominent role because of its easy installation and flexibility. Among the various wireless domains, Zigbee based Wireless Dynamic Sensor Networks (WDSN) pose a good support to the dynamics that arise when the nodes are induced with mobility. In the Zigbee based Wireless Dynamic Sensor Network (WDSN), major consideration is on utilizing the energy efficiently among the mobile nodes. Various techniques are used to attain energy efficiency in Zigbee WDSN. Among them, clustering the nodes is one of the best methods, since they aim at reducing the energy dissipation and increasing the life span of the network. Hence, in this paper, the performance of Zigbee WDSN using clustering scheme is done by considering the nodes with mobility and compared with performance of Zigbee WDSN using non clustering technique. The proposed work is summarized as follows: the network is deployed as clusters and the remaining energy of the node is determined by utilizing clustering protocol. In each cluster, the clustering protocol opts for the node with the maximum remaining energy as the head of that cluster. Then STR algorithm is utilized to route the sensed data from the member nodes to the cluster head. Hence, the clustering technique and STR, route the information through the shortest path paving the way for enhanced average residual energy and Packet Delivery Ratio (PDR). The simulations are done by using ns2 and performance metrics such as average residual energy and PDR are computed and analyzed for non clustered and clustered method.

6. Achieving High-Performance Cellular Data Services with Multi-Network Access

This paper presents the design and evaluation of a mobile data service which exploits parallel multi-path trans- mission over multiple cellular networks to achieve significant performance gains. Multi-network access is motivated by the fact that multi-radio mobile devices are fast becoming a real- ity, making it possible for end-users to increase their service speed and availability via network diversity. In contrast to previously proposed techniques at the application or transport layers, we propose a novel network assisted architecture for multi-homed (NAMH) cellular access. In the proposed system, network elements such as routers and base stations provide the necessary multihoming functionality including identification of a bifurcation router and dynamic splitting of the data stream corresponding to currently achievable bit-rates on the cellular base stations. A detailed evaluation is provided for the multi- network service with LTE base stations, using both ns3 simulation and trace-driven emulations. The results show that significant gains are achieved with multi-network access with bit-rates of 1.9x using two LTE networks in parallel. Comparison with the well-known MPTCP method is given, showing gains of about 40% with NAMH for the trace-driven two-network scenario.

7. Collision-Free Anycast Transmission Scheduling in UWSNs

Underwater Wireless Sensor Network (UWSNs) have been proposed to monitor underwater regions such as seas and oceans. A typical example of an UWSN consists of a set of underwater sensor nodes and a set of sink nodes that are deployed at the sea surface. Using acoustic transmission, the sensors send their collected data to at least one of the sinks in what is known as the anycast transmission problem. One of the major problems with underwater nodes is their limited power, which means that transmission collisions are very costly. In this paper, we propose a collision-free anycast transmission

scheduling algorithm for UWSNs. The proposed algorithm is a location-based routing algorithm that schedules transmissions between sensor nodes and sink nodes in order to minimize the energy consumption and possible collisions. We perform a set of experiments using the NS2 Aqua-Sim simulator to show that the proposed algorithm can provide up to 26% in energy savings compared with a simple greedy algorithm.

8. Design of transmission manager in heterogeneous WSNs

The current generation of sensor networks are designed to be application-specific, thus are exposed only to a limited set of users. The emerging concept of IoT is expected to house multiple applications with diverse delay requirements. A transmission manager provides an optimal transmission time for transmitting the buffered measurements. In the literature, solutions have been proposed optimizing mainly for single sensing infrastructures. In this work, we first propose an optimal transmission manager that supports multiple applications in a single-hop wireless sensor networks. Then, we extend our
solution into a distributed transmission manager to operate in multi-hop WSNs. Both transmission managers work in tandem, and determine the transmission time for every buffered measurement. We implement both solutions in ns3 and compare with other state of the art solutions. Our case studies show that our proposed solution reduces energy consumption by 75% compared to the state of the art approaches while having on average 12% less expired measurements.

9. Efficient Data Center Flow Scheduling without Starvation using Expansion Ratio

Existing data center transport protocols are usually based on the Processor Sharing (PS) policy and/or the Shortest Remaining Processing Time (SRPT) policy. PS divides link bandwidth equally between competing flows, thus it fails to achieve optimal average flow completion time (FCT). SRPT prioritizes flows that have the shortest remaining processing time and provides near-optimal average FCT, but it may cause long flows to suffer unfair delays, or even starve them. In fact, these two types of policies represent two directions in the design space: PS prefers fairness (in terms of starvation freedom) while SRPT favors efficiency (in terms of average FCT). In this paper, we propose a novel metric, expansion ratio, which enables us to strike a balance between SRPT and PS. We design MERP that achieves efficient flow scheduling without starvation. MERP takes care of both average and tail FCTs by minimizing the expansion ratio of competing flows in a lexicographically manner. MERP controls the sending rate of competing flows via synchronized virtual deadlines and routes flows in a downstream-aware manner that reacts quickly to link failures. We evaluate MERP using extensive NS2-based simulations. Results show that, under various traffic loads, MERP reduces the tail FCT significantly with a negligible increase of average FCT compared with pFabric, and MERP reduces the average FCT notably compared with ECMP and CONGA when link failures occur.

10. Issues and Attacks – A Security Threat to Wsn: An Analogy

Computer network is a group of computing devices like computers which are connected together and these devices communicate or exchange the information through links. One such type of network is wireless sensor networks. Wireless sensor networks consist of sensor nodes connected in some fashion. These nodes detect various environmental conditions such as temperature, sound and so on. Attacks have become serious security threats that wireless sensor networks have to overcome. These attacks lead to energy inefficiency. There are various types of security attacks that a wireless sensor network has to overcome. Blackhole attack and power consumption attack are also among the types of security attacks. This paper is a survey paper which consists of a survey on avoidance of the attacks mentioned above and an effort to reduce the power consumption and increase the energy efficiency.

11. **Research of the positioning of an improveed WSN particle swarm optimization in node ranging**

To order to know how to better solve the problem of node positioning in WSN, this paper mainly improves the particle swarm optimization of wireless sensor network node positioning in RSSI ranging. Aiming at the problem that local convergence exists in the algorithm, dynamic disturbance factors are introduced to reduce the speed of local convergence. And penalty function is introduced, thereby limiting the search range of feasible solutions and avoid consuming time in ineffective solution space. Compared with other algorithms, the improved algorithm has significant changes in the effects of convergence speed and stability analysis.

NS3 Projects

1. **A Distributed Prevention Scheme from Malicious Nodes in VANETs' Routing Protocols**

Vehicular environments are vulnerable to attacks because of the continuous interactions between vehicles despite authentication techniques deployed by communication standards. In fact, an authenticated node with a certificate could initiate an attack while complying with implemented protocols if it has malicious intentions and benefit from this always on connection to threaten the network accuracy. Several mechanisms to counter these attacks were proposed but none of them is able to anticipate the behavior of nodes. In the present work, we target this problem by proposing a preventive mechanism able to predict the behavior of vehicles and prevent from attacks. We use Kalman filter to predict the future behavior of vehicles and classify them into three categories (white, gray and black) based on their expected trustworthiness. The main concern of this work is to prevent from the denial of service (DoS) attack. Results, given by the implementation of the proposed mechanism over an intersectionbased routing protocol using ns3 simulator, prove its accuracy regarding the detection rate and a good impact on packets
delivery ratio and end-to-end delay.

2. **Mobility Quantification for MultiPoint Relays Selection Algorithm in Mobile Ad Hoc Networks**

In Mobile Ad hoc Networks (MANETs), with Optimized Link State Routing Protocol (OLSR) the mobility concept is an essential element which can result in the evolution of network performances. In this paper, the main objective is to develop an algorithm to improve the MultiPoint Relay (MPR) selection process in such networks. This algorithm is based on the Mobility Rate (MR) which in turn is relied on the relative velocity of nodes. Additionally, in this algorithm, each node keeps a mobility rate record of other nodes. Moreover, this mobility value will be exchanged between nodes using OLSR
messages (HELLO and Topology control (TC)). Furthermore, this value will be used as a criterion when a node chooses their MPR set. In addition, the simulation results using Network Simulator 3 (NS3) have shown that the mobility concept could improve network performances in terms of the throughput,
packet received, packet loss, packet delivery ratio and packet forwarded. Moreover, and through this paper the proposed algorithm can be used as a functional mobility mechanism to improve network performances in MANETs.

3. **Performance Analysis of Multicast Routing Protocols Using NS-3**

Mobility of users and enhancement of bandwidth have been characterizing factors for the global telecommunication development which also witnessed improvements in services. If user needs to

send some information over the prescribed bandwidth with dure reliability then the (QOS) Quality of services
becomes more critical and seeks expected performance. A Mobile Adhoc Network is self-possessed combination of mobile nodes. It has to be self-structured. These are mobility extensions into wireless domain and autonomous mobile dominion. In this set of specified nodes which form adhoc network with routing infrastructure too. Multicasting is responsible for transferring information efficiently from a source to any destination; duplication of messages and delivery takes place only once and that too at the branch points, due to splitting of the destination links. The authors have successfully been able to address several issues relating to MANET, especially multicasting, its routing protocols and qualitative comparisons. Further, in this paper, we particularly focused on implementation as well as performance
analysis of multicast routing protocols like AODV, MAODV using network simulator NS3.By using the performance parameter such as average end-to-end delay and packet delivery ratio (PDR) and routing-overhead.

4. Performance of The Routing Protocols AODV, DSDV and OLSR in Health Monitoring Using NS3

The complexity of health care and the increasing cost of health care in developing country such as Indonesia caused by the source of available funds and limited human resources, especially health professionals. Health monitoring through wireless body area network is one of the solution and which offers several advantages as inexpensive health services, better utilization from health care professional resource, mobility, and great experience for the patient. However, health monitoring has some challenges such as limited area coverage, mobility problem and attenuation from human body. In this paper, it describes how to research about utilization AODV, DSDV, and OLSR routing protocols from ad hoc network to improve health monitoring by using NS3 to face limited area coverage and mobility problem for static and mobile conditions. As simulation, the researcher compares the performance of AODV, DSDV, and OLSR. The researcher selected three performances of metrics: delay, throughput, and packet delivery ratio. As a result showed, OLSR has better performance for mobile and mobile has more than 50 nodes except delay, when througput, and packet delivery ratio of mobile condition OLSR show better than AODV . In static condition, throughput of AODV shows better than DSDV and OLSR, even though for mobile condition OLSR shows better than AODV and DSDV, but
in some cases the delay of AODV shows better than DSDV and OLSR. This is an indication for the possible implementation of OLSR routing protocols which node is bigger than 50 nodes.

An NS3 Implementation of physical layer based on 802.11 for utility maximization of WSN

Abstract:

A Technology require to meet customer demands and improve the performance in WLAN 802.11.Wireless is a scalable, reliable and cost effective technology which can be used to implement 802.11 for utility maximization of WSN. Integrate physical layer simulator for OFDM-based IEEE 802.11 communication in a network simulator. We implement OFDM-based IEEE 802.11 standard, more precisely, for the orthogonal frequency division multiplexing (OFDM) PHY specification for the 5 GHz band. PhySim-Wifi is a detailed and accurate implementation of the OFDM-based IEEE 802.11 standard, with higher fidelity at the physical layer than found in NS3. It can be used as replacement for the official YansWifiPhy implementation when higher simulation accuracy is required in NS3. Which will provide channel related access information in dynamic network scenario. This can lead to a programmable interface for management and control of physical layer and network layer resources in an optimal fashion.

Increasing network lifetime by energy-efficient routing scheme for OLSR protocol

Abstract:

One of the main considerations in designing routing protocols for Mobile Ad-Hoc Network (MANET) is to increase network lifetime by minimizing nodes' energy consumption, since nodes are typically battery powered. Many proposals have been addressed to this problem; however, few papers consider a proactive protocol like Optimized Link State Routing Protocol (OLSR) to better manage the energy consumption. Some of them have explored modifications to the MPRs selection mechanism, whereas others have investigated multiple cross layer parameters to increase the network lifetime. In this paper, we explored both modification to MPR selection and integrating appropriate routing metrics in the routing decision scheme to lessen effects of reason that lead to more energy consumption. Our power-aware version of OLSR is proven by simulations in NS3 under a range of different mobile scenarios. Significant performance gains of 20% are obtained in network lifetime for our modified OLSR and little to no performance gains in term of Packet Delivery Ratio (PDR).

Architecture and Implementation of An Information-Centric Device-to-Device Network

Today's mobile devices almost exclusively connect to infrastructures for communications and information access; but advances such as AirDrop andWiFi Direct are bringing deviceto-device communication to the forefront of mobile computing. Self-organizing ad hoc mobile networks have a wide range of applications in scenarios where infrastructure is not available or with limited bandwidth, such as communications in the aftermath of natural disasters, censorship resistant communications, and battlefield communications. In this paper, we propose an information-centric device-to-device network, called ICD2D. The network is distributed and requires no centralized coordination. For each published item

of data, the system creates a metatdata; a publish-subscribe mechanism disseminates the metadata and facilitates filtering information in a distributed

fashion. We implemented a full-featured system on NS3. Evaluations show significant improvement in successful information retrieval compared with OLSR (Optimized Link State Routing), a common approach to ad hoc routing.

DETERMINING THE NETWORK THROUGHPUT AND FLOW RATE USING GSR AND AAL2R

ABSTRACT

In multi-radio wireless mesh networks, one node is eligible to transmit packets over multiple channels to different destination nodes simultaneously. This feature of multi-radio wireless mesh network makes high throughput for the network and increase the chance for multi path routing. This is because the multiple channel availability for transmission decreases the probability of the most elegant problem called as interference problem which is either of interflow and intraflow type. For avoiding the problem like interference and maintaining the constant network performance or increasing the performance the WMN need to consider the packet aggregation and packet forwarding. Packet aggregation is process of collecting several packets ready for transmission and sending them to the intended recipient through the channel, while the packet forwarding holds the hop-by-hop routing. But choosing the correct path among different available multiple paths is most the important factor in the both case for a routing algorithm. Hence the most challenging factor is to determine a forwarding strategy which will provide the schedule for each node for transmission within the channel. In this research work we have tried to implement two forwarding strategies for the multi path multi radio WMN as the approximate solution for the above said problem. We have implemented Global State Routing (GSR) which will consider the packet forwarding concept and Aggregation Aware Layer 2 Routing (AAL2R) which considers the both concept i.e. both packet forwarding and packet aggregation. After the successful implementation the network performance has been measured by means of simulation study.

A Comparative Performance Analysis of Routing

Protocols in MANET using NS3 Simulator

Abstract—Due to frequent topology changes and routing overhead, selection of routing protocol in Mobile Ad-hoc Network (MANET) is a great challenge. A design issue for an efficient and effective routing protocol is to achieve optimum values of performance parameters under network scenarios. There are various routing

protocols available for MANET. This paper involves study of four routing protocols (Ad-hoc On Demand Distance Vector Routing, Optimized Link State Routing, Dynamic Source Routing and Distance Sequenced Distance Vector), and performance comparisons between these routing protocols on the basis of performance

metrics (throughput, packet delivery ratio, Packet dropped, jitter and end to end delay measured after simulation of network) with the help of NS3 Simulator.