NS2 PROJECT ABSTRACTS
(Wireless Sensor Network, Vanet, Ad-Hoc Network, Mesh Network, Parallel & Distributed System, Underwater Sensor Networks)

2016 IEEE WSN (Wireless Sensor Networks) PROJECT LIST BASED ON NS2

1. **Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks**
   Energy savings optimization becomes one of the major concerns in the wireless sensor network (WSN) routing protocol design,due to the fact that most sensor nodes are equipped with the limited nonrechargeable battery power. In this paper, we focus on minimizing energy consumption and maximizing network lifetime for data relay in one-dimensional (1-D) queue network. Following the principle of opportunistic routing theory, multihop relay decision to optimize the network energy efficiency is made based on the differences among sensor nodes, in terms of both the irdistance to sink and the residual energy of each other. Specifically,an Energy Saving via Opportunistic Routing (ENS_OR) algorithmis designed to ensure minimum power cost during data relay andprotect the nodes with relatively low residual energy. Extensivesimulations and real testbed results show that the proposed solutionENS_OR can significantly improve the network performanceon energy saving and wireless connectivity in comparison withother existingWSN routing schemes.

2. **Extending Wireless Sensor Network Lifetime With Global Energy Balance.**
   In this paper, a decentralized routing algorithm,called game theoretic energy balance routing protocol,is proposed to extend the network lifetime by balancing energyconsumption in a larger network area using geographical routingprotocols. The objective of the proposed protocol is to makesensor nodes deplete their energy at approximately the sametime, which is achieved by addressing the load balance problem atboth the region and node levels. In the region level, evolutionarygame theory (EGT) is used to balance the traffic load to availablesubregions. At the node level, classical game theory (CGT) isused to select the best node to balance the load in the selectedsubregion. This two-level approach is shown to be an effectivesolution for load balancing and extending network lifetime.This paper shows the use of EGT and CGT in designing arobust protocol that offers significant improvement over existingprotocols in extending network lifetime.

3. **Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks**
   Wireless sensor networks (WSNs) deployed in hostileenvironments are vulnerable to clone attacks. In such attack,an adversary compromises a few nodes, replicates them, andinserts arbitrary number of replicas into the network. Consequently,the adversary can carry out many internal attacks. Previoussolutions on detecting clone attacks have several drawbacks.First, some of them require a central control, which introducesseveral inherent limits. Second, some of them are deterministicand vulnerable to simple witness compromising attacks. Third,in some solutions the adversary can easily learn the criticalwitness nodes to start smart attacks and protect replicas frombeing detected. In this paper, we first show that in order toavoid existing drawbacks, replica-detection protocols must benon-deterministic and fully distributed (NDFD), and fulfill threesecurity requirements on witness selection. To our knowledge,only one existing protocol, Randomized Multicast, is NDFD andfulfills the requirements, but it has very high communicationoverhead. Then, based on random walk, we propose two newNDFD protocols, RAndomWaLk (RAWL) and Table-assistedRAndomWaLk (TRAWL), which fulfill the requirements whilehaving only moderate communication and memory overheads.The random walk strategy outperforms previous strategies becauseit distributes a core step, the witness selection, to everypassed node of random walks, and then the adversary cannoteasily find out the critical witness nodes. We theoretically analyzethe required number of walk steps for ensuring detection.Our simulation results show that our protocols outperform anexisting NDFD protocol with the lowest overheads in witnessselection, and TRAWL even has lower memory overhead thanthat protocol. The communication overheads of our protocols arehigher but are affordable considering their security benefits.

4. **Data Aggregation Techniques to Remove Redundancy in Wireless Sensor Networks.**
In Wireless Sensor Networks (WSN), some sensor nodes are mobile in nature. Due to mobility of nodes, there is no guarantee of reliable delivery of information. To ensure reliability, many sensor nodes are deployed in the monitoring environment. These sensor nodes sense the same kind of data and forward it to the sink node. This redundant information sustains the reliability; but at the same time, sink node wastes its energy in processing the redundant data. So there is a need to eliminate the redundancy in sensed data up to adequate level in order to maintain the tradeoff between energy conservation and reliability. There exist many data aggregation techniques that perform data redundancy removal in order to improve life time of sensor nodes. Data aggregation is a technique in which each intermediate node in the routing path receives multiple input packets, process them and transmits a single packet. In this paper we have studied different data aggregation strategies and focused on some data aggregation techniques based on these strategies. Further we havediscussed advantages and limitations of these techniques.

5. **QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks.**
QoS routing is an important research issue in wireless sensor networks (WSNs), especially for mission-critical monitoringand surveillance systems which requires timely and reliable data delivery. Existing work exploits multipath routing to guaranteeboth reliability and delay QoS constraints inWSNs. However, the multipath routing approach suffers from a significant energy cost. In this work, we exploit the geographic opportunistic routing (GOR) for QoS provisioning with both end-to-end reliability and delay constraints in WSNs. Existing GOR protocols are not efficient for QoS provisioning in WSNs, in terms of the energy efficiency and computation delay at each hop. To improve the efficiency of QoS routing in WSNs, we define the problem of efficient GOR for multiconstrainedQoS provisioning in WSNs, which can be formulated as a multiobjectivemulticonstraint optimization problem. Based on the analysis and observations of different routing metrics in GOR, we then propose an Efficient QoS-aware GOR (EQGOR) protocol for QoS provisioning in WSNs. EQGOR selects and prioritizes the forwarding candidate set in an efficient manner, which is suitable for WSNs in respect of energy efficiency, latency, and time complexity. We comprehensively evaluate EQGOR by comparing it with the multipath routing approach and other baseline protocols through ns-2 simulation and evaluate its time complexity through measurement on the MicaZ node. Evaluation results demonstrate the effectiveness of the GOR approach for QoS provisioning in WSNs. EQGOR significantly improves both the end-to-end energy efficiency and latency, and it is characterized by the low time complexity.

6. **Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks.**
We propose two novel energy-aware routing algorithms for wireless ad hoc networks, called reliable minimum energy costrouting (RMECR) and reliable minimum energy routing (RMER). RMECR addresses three important requirements of ad hoc networks: energy-efficiency, reliability, and prolonging network lifetime. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. RMER, on the other hand, is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. RMER and RMECR are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability. Simulation studies show that RMECR is able to find energy-efficient and reliable routes similar to RMER, while also extending the operational lifetime of the network. This makes RMECR an elegant solution to increase energy-efficiency, reliability, and lifetime of wireless ad hoc networks. In the design of RMECR, we consider minute details such as energy consumed by processing elements of transceivers, limited number of retransmissions allowed per packet, packet sizes, and the impact of acknowledgment packets. This adds to the novelty of this work compared to the existing studies.

7. **Using Mobile Sensors to Enhance Coverage in Linear Wireless Sensor Networks.**

One of the main challenges of using Linear Wireless Sensor Networks (LSN) is the reliability of the connections among the nodes. Faults in a few contiguous nodes may causethe creation of holes which will result in dividing the network in to multiple disconnected segments. As a result, sensor nodesthat are located between holes may not be able to deliver the ir sensed information which negativity affects the network sensing coverage. This paper develops two models to utilize mobile sensors to help recover from these faults and enhance coverage. The first model utilizes mobile sensors to cover theholes while the second model has the feature of reallocating previously deployed mobile sensors for best possible coverage.In both models, the added mobile nodes can provide additional sensing coverage as well as enable connectivity among disconnected segments in the LSN. Evaluations and comparisons between both models are provided. In addition, ananalytical model for finding the expected number of mobile sensors needed for maintaining high coverage in a LSN with specific configurations is developed and validated.

8. **An Efficient Cluster-Tree Based Data Collection Scheme for Large Mobile Wireless Sensor Networks.**

Wireless Sensor Networks (WSNs) play a vital role in today's real world applications. The effectiveness of WSNs purely depends on the data collection scheme. Numerous data collection schemes such as multipath, chain, tree, cluster andhybrid topologies are available in literature for collecting data in WSNs. However, the existing data collection schemes fail toprovide a guaranteed reliable network in terms of mobility, traffic, and end-to-end connection. In this paper, a Velocity Energy-efficient and Link-aware Cluster-Tree (VELCT) scheme for data collection in WSNs is proposed which would effectivelymitigate the problems of coverage distance, mobility, delay, traffic, tree intensity, and end-to-end connection. The proposedVELCT constructs the Data Collection Tree (DCT) based on the cluster head location. The data collection node in the DCTdoes not participate in sensing on this particular round, however, it simply collects the data packet from the cluster head anddelivers it to the sink. The designed VELCT scheme minimizes the energy exploitation, reduces the end-to-end delay and traffic in cluster head in WSNs by effective usage of the DCT. The strength of the VELCT algorithm is to construct a simple treestructure, thereby reducing the energy consumption of the cluster head and avoids frequent cluster formation. It also maintainsthe cluster for a considerable amount of time. Simulation results have demonstrated that VELCT provides better QoS in terms of energy consumption, throughput, end-to-end delay, and network lifetime for mobility-based WSNs.

9. **A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in WSN.**

Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used indecisionmaking for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this paper, we propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

10. **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.

11. **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.

12. **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.

13. **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.

14. **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 itsdynamic 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.

15. **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.

16. **An Improvement On LEACH Protocol.**
Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for SN monitoring and recording the physical conditions of the environment and organizing 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. Routing protocols are most important for the network while resources are limited. LEACH is one of the first hierarchical 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.

17. **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.

18. **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 befailed 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.

19. **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.

20. **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.

21. **Intrusion Detection System for Power-Aware OLSR.**
Optimized Link State Routing (OLSR) is a standard proactive routing protocol for Wireless Sensor Network (WSN). OLSR uses two kinds of the control messages: Hello and Topology Control (TC). As these messages are un-authenticated, OLSR is prone to several attacks namely, blackhole, wormhole, grayhole etc. This paper is focused at Sleep Deprivation Torture Attack on OLSR. Sleep deprivation attack is one of the most interesting attack in layer 2 where the attacker tries to use a low energy node until all its energy is exhausted and the node goes into permanent sleep. This attack is also possible in routing level. In OLSR low energy node declare their status through willingness property of HELLO message. Using this information an attacker node can choose that low energy node deliberately and forward all traffic through that node. This leads to low energy node in a permanent sleep mode. In this paper we propose a specification based Intrusion Detection System (IDS) for that type of attack. The performance of the propose algorithm is studied by Network Simulator (NS2) and effectiveness of the propose scheme, along with a comparison with existing techniques is demonstrated.

22. **SPIN With Cluster for Data Centric Wireless.**
Routing Algorithms are driving the growth of the data transmission in wireless sensor networks. Contextually, many algorithms considered the data gathering and data aggregation. This paper uses the scenario of clustering and its impact over the SPIN protocol and also finds out the effect over the energy consumption in SPIN after uses of clustering. The proposed scheme is implemented using TCL/C++ programming language and evaluated using Ns2.34 simulator and compare with LEACH. Simulation shows proposed protocol exhibits significant performance gains over the LEACH for lifetime of network and guaranteed data transmission India

23. **Secure-SPIN with cluster for Data Centric Wireless sensor network**
Routing Algorithms are driving the growth of the data transmission in wireless sensor network. Contextually, many algorithms proposed for efficient data transferring. This paper uses the scenario and node distribution across the Battle field in India. This Paper uses clustering algorithms to send the data over different geographic region. During the Battle, data gathering and data aggregation to base station is important and critical task. Based onevent, clustering algorithm used. This paper assumes that sensor node uniformly distributed and coordinates of the base station and nodes are known. This paper is essential to enable the cluster head based selection scheme used in battle field and the performance of proposed protocol compute intensive and can significantly benefit over the others scheme. Proposed scheme having better data gathering, stability period and lifetime than the LECH scheme. The proposed scheme is implemented and simulated with LEACH in NS2.34. Simulation shows proposed protocol performance gains is better over the LEACH for

lifetime of network and guaranteed data transmission.

24. **Section of node density with cluster in SPIN for data centric wireless sensor network.**
Routing algorithm are driving the growth of the data transmission in wireless sensor networks. Contextually many algorithm considered the data gathering and data aggregation scenario like battle field, it is important and critical task in data transmission. Therefore through this paper handles the event generated by sensor nodes and provide the guaranteed transmission to sink using clustering process and node density with SPIN. Proposed scheme having better data gathering stability period and lifetie than the LEACH scheme. The proposed scheme is implemented usng TCL / C++ programming language and evaluated using Ns2.34 simulator with LEACH. Simulation shows proposed protocol exhibits significant performance gains over the LEACH for lifetime of network and guaranteed data transmissions.

25. **Breath: An Adaptive Protocol for Industrial Control Applications Using Wireless Sensor Networks.**
Opportunistic data forwarding has drawn much attention in the research community of multihop wireless networking, with most research conducted for stationary wireless networks. One of the reasons why opportunistic data forwarding has not been widely utilized in mobile ad hoc networks (MANETs) is the lack of an efficient lightweight proactive routing scheme with strong source routing capability. In this paper, we propose a lightweight proactive source routing (PSR) protocol. PSR can maintain more network topology information than distance vector (DV) routing to facilitate source routing, although it has much smaller overhead than traditional DV-based protocols [e.g., destination-sequenced DV (DSDV)], link state (LS)-based routing [e.g., optimized link state routing (OLSR)], and reactive source routing [e.g., dynamic source routing (DSR)]. Our tests using computer simulation in Network Simulator 2 (ns-2) indicate that the overhead in PSR is only a fraction of the overhead of these baseline protocols, and PSR yields similar or better data transportation performance than these baseline protocols.

26. **Grouping of Clusters for Efficient Data Aggregation (GCEDA) in Wireless Sensor Network.**
In the application based WSN environment, energy and bandwidth of the sensor are valuable resources and need to utilize efficiently. Data aggregation at the sink by individual node causes flooding of the data which results in maximum energy consumption. To minimize this problem we propose and evaluate the group based data aggregation method, where grouping of nodes based on available data and correlation in the intra-cluster and grouping of cluster heads at the network level help to reduce the energy consumption. In addition, proposed method uses additive and divisible data aggregation function at cluster head (CH) as in-network processing to reduce energy consumption. Cluster head transmits aggregated information to remote sink and cluster head nodes transmit data to CH. Simulation result shows, proposed algorithm provides an improvement of 14.94% in energy consumption as compared with primary cluster based protocol LEACH which uses only one CH, it also improves the network stability.

27. **By-Passing Infected Areas in Wireless Sensor Networks using BPR.**
Abnormalities in sensed data streams indicate the spread of malicious attacks, hardware failure and software corruption among the different nodes in a Wireless Sensor Network. These factors of node infection can affect generated and incoming data streams resulting in high chances of inaccurate data, misleading packet translation, wrong decision making and severe communication disruption. This problem is detrimental to real-

time applications having stringent Quality-of-Service (QoS) requirements. The sensed data from other uninfected regions might also get stuck in an infected region should no prior alternative arrangements are made. Although several existing methods (BOUNDHOLE and GAR) can be used to mitigate these issues, their performance is bounded by some limitations, mainly due to the high risk of falling into routing loops and involvement in unnecessary transmissions. This paper provides a solution to by-pass the infected nodes dynamically using twin rolling balls technique and also divert the packets that are trapped inside the identified area. The identification of infected nodes is done by adapting a Fuzzy data clustering approach which classifies the nodes based on the fraction of anomalous data that is detected in individual data streams. This information is then used in the proposed By-Passed Routing (BPR) which rotates the balls in two directions simultaneously: clockwise and counter-clockwise. The first node that hits any ball in any direction and is uninfected, is selected as the next hop. We are also concerned with the incoming packets or the packets-on-the-fly that may be affected when this problem occurs. Besides solving both of the problems in the existing methods, the proposed BPR technique has greatly improved the studied QoS parameters as shown by almost 40% increase in the overall performance.

28. **A Novel Cluster-based Energy Efficient Routing in Wireless Sensor Networks.**
Recent development in electronics and wireless communications has enabled the improvement of low-power and lowcost wireless sensors networks. Wireless Sensor Networks(WSNs) are a combination of autonomous devices transmitting locally gathered information to a so-called sink node by using multihop wireless routing. One of the most important challenges in WSNs is to design energy efficient routing mechanism to increase the network lifetime due to the limited energy capacity of the network nodes. Furthermore, hot spots in a WSNs emerge as locations under heavy traffic load. Nodes in such areas quickly drain energy resources, leading to disconnection in network services. Cluster based routing algorithms in WSNs have recently gained increased interest, and energy efficiency is of particular interest. A cluster head (CH) represents all nodes in the cluster and collects data values from them. To balance the energy consumption and the traffic load in the network, the CH should be rotated among all nodes and the cluster size should be carefully determined at different parts of the WSNs. In this paper, we proposed an cluster based energy efficient routing algorithm (CBER), CBER elects CH based on nodes near to the optimal cluster head distance and residual energy of the nodes. In WSNs energy is mostly consumed for transmission and reception, it is a non linear function of transmission range.In this paper, the optimal cluster head distance which links to optimal energy consumption is derived. In addition, residual energy is considered in the CH election in order to increase the network lifetime. Furthermore, the energy consumption of being a CH is equally spread among the cluster members. Performance results show CBER scheme reduces the end to end energy consumption and prolong the network lifetime of multi hop network compared to the well-known clustering algorithms LEACH and HEED.

29. **EgyHet: An Energy-Saving Routing Protocol for Wireless Heterogeneous Sensor Networks.**
Due to different requirements in application environment, wireless heterogeneous sensor networks (WHSNs) formed by sensors with various capacities are built. Data routing in WHSNs poses special challenges: First, it should be redesigned because the existing ones may not be directly used due to asymmetric links caused by diverse sensor transmission ranges. Second, it should guarantee an assured delivery rate because data is routed through lossy links. Third, it should be energyefficient due to the limitation of sensor batteries and the difficulty of replacing them after deployment. To address these issues, we propose *EgyHet*: an Energy-saving routing protocol for Heterogeneous sensor networks. EgyHat deals with asymmetric links by establishing reverse paths. It saves energy by taking the shortest path, considering the remaining energy in sensors and reducing the number of forwarding nodes while guarantees an assured delivery rate. Simulation results show that EgyHat can save more energy yet keep the similar delivery ratio and latency to those of the existing

routing protocol for WHSNs.

30. **Overlapped Schedules with Centralized Clustering for Wireless Sensor Networks.**
The main attributes that have been used to conserve the energy in wireless sensor networks (WSNs) are clustering, synchronization and low-duty-cycle operation. Clustering is an energy efficient mechanism that divides sensor nodes into many clusters. Clustering is a standard approach for achieving energy efficient and hence extending the network lifetime. Synchronize the schedules of these clusters is one of theprimary challenges in WSNs. Several factors cause the synchronization errors. Among them, clock drift that is accommodated at each hop over the time. Synchronization by means of scheduling allows the nodes to cooperate and transmit data in a scheduled manner under the duty cycle mechanism. Duty cycle is the approach to efficiently utilize the limited energy supplies for the sensors. This concept is used to reduce idle listening. Duty cycle, nodes clustering and schedules synchronization are the main attributes we have considered for designing a new medium access control (MAC) protocol. The proposed OLS-MAC protocol designed with the target of making the schedules of the clusters to be overlapped with introducing a small shift time between the adjacent clusters schedules to compensate the clock drift. The OLSMAC algorithm is simulated in NS-2 and compared to some SMAC derived protocols. We verified that our proposed algorithm outperform these protocols in number of performance matrix.

31. **Low-Latency Asynchronous Duty-Cycle MAC Protocol for Burst Traffic in Wireless Sensor Networks.**
Many energy-efficient asynchronous duty-cycle media access control (MAC) protocols for wireless sensor networks (WSNs) have been proposed in recent years. However, for burst traffic, most of them suffer from significant performance degradation due to randomly waking up to communicate with each other. In this paper, we propose a new asynchronous duty-cycle receiver-initiated MAC protocol called HKMAC. In proposed HKMAC, by adaptively adjusting beacon time of the receiver and scheduling the sender's listening time during scheduled period, it can achieve low end-to-end packet delivery latency and high energy efficiency under burst traffic. We have evaluated the performance of HKMAC through detailed ns-2 simulation. The simulation results show that HKMAC can always reduce end-to-end packet delivery latency and energy consumption under various data rates in different topologies compared with RI-MAC - a state-of-the-art MAC protocol in WSNs.

32. **Impact of Multipath Routing on WSN Security Attacks.**
Multipath routing does not minimize the consequences of security attacks. Due to this many WSNs are still in danger of most security attacks even when multipath routing is used. In critical situations, for example, in military and health applications this may lead to undesired, harmful and disastrous effects. These applications need to get their data communicated efficiently and in a secure manner. In this paper, we show the results of a series of security attacks on a multipath extension to the ad hoc on-demand distance vector AODV protocol, AOMDV. It is proved that many security parameters are negatively affected by security attacks on AOMDV, which is contradictory to research claims. This means that alternative refinements have to be made to present multipath routing protocols in order to make them more effective against network security attacks.

33. **Defending against vampire attacks in wireless sensor networks.**
Wireless Sensor Networks in today's world are the basic means of communication. The limitations of system are resources like battery power, communication range and processing capabilities. One of the major challenges in Wireless Sensor Networks is the security concerns. The attacks affecting these systems are increasing as they progress. One of the resource depletion attacks called vampire attacks are the major concern. They not only affect a single node but they bring down the entire system draining the power i.e.

Battery power. In this paper, the system proposed overcomes this challenge by using the Energy Weight Monitoring Algorithm (EWMA) and the energy consumption is reduced to a great-extend.

34. **Efficient Cluster Head Election For Detection And Prevention Of Misdirection Attack In Wireless Sensor Network.**

Wireless sensor networks are gaining their popularity in application like consumer, defense, industrial sectors monitoring and collecting environmental data. Wireless Sensor networks are in areas which are not having any human monitoring. Being unmonitored, wireless sensor networks are vulnerable to different kinds of the attack. Misdirection attack in one the Denial of Service Attack, which causes the nodes to route information on long paths and ultimately creates situations of network jam.Misdirection attack that reduces throughput, network life time and increases the delay. There is only one solution to misdirection attack is third party monitoring. The work here in this dissertation proposes third party monitoring by cluster head and also monitoring of cluster head by source and destination transmission. Furthermore the work also improves the cluster head election procedure for security, so that initially intruder should not be selected as a cluster head.

35. **Energy Efficient Data Aggregation Techniques in Wireless Sensor Networks.**

The data in wireless sensor networks is organized in an efficient manner using data aggregation and data dissemination protocols. Due to the energy constraints in sensor nodes, energy-efficient data aggregation protocols are used to save the node energy and enhance the network life cycle. Deploying additional sensor nodes in the network reduce the resource constraints but increase the rate of data redundancy. This limitation is addressed by the data aggregation protocols in sensor networks. Data aggregation protocols use cluster head node to collect the data, aggregate the data and forward the data to the base station. The primary attributes considered in the design of data aggregation protocols are energy, latency, cluster size and data rate. In this article, we present a novel approach to classify the energy-efficient data aggregation protocols based on structure, search-based and time-based approaches. Analysis for structure-free, structure-based, distance and time-based data aggregation protocols are given in detail. Simulation results indicate that the energy and throughput rate are improved in the cluster-based data aggregation protocols as compared to the structure-free, time-based or search-based data aggregation protocols.

36. **Efficient Multilevel Data Aggregation Technique for Wireless Sensor Networks.**

Wireless sensor network (WSN) is one of the most emerging technology which consists of large number of sensor nodes with each having the capacity to sense, compute and communicate the data. WSN has great deal of applications in various fields like military, agriculture, industry healthcare etc. Sensor nodes are randomly and densely deployed. This kind of deployment creates large number of redundant sensor data. Routing of such redundant data not only saturates network resources, but also consumes more energy. Data aggregation is the effective technique which reduces the number of transmissions to sink node by aggregating the similar packets in an energy efficient manner to enhance the lifetime of network. There exists different data aggregation techniques which perform aggregation in single level or two levels. In this paper we are proposing multilevel hierarchical data aggregation technique which handles the redundancy in sensor data very efficiently.

37. **Secured Clustering and Multipath Routing in Wireless Sensor Networks.**

Secure data transmission is a critical issue for wireless sensor networks (WSNs).Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-

Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to] illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

38. **Achieving Efficient Flooding by Utilizing Link Correlation in WSN.**

Although existing flooding protocols can provideefficient and reliable communication in wireless sensor networkson some level, further performance improvement has been hampered by the assumption of link independence, which requires costly acknowledgments (ACKs) from every receiver. In this paper, we present collective flooding (CF), which exploits the link correlation to achieve flooding reliability using the concept of collective ACKs. CF requires only 1-hop information at each node, making the design highly distributed and scalable with low complexity. We evaluate CF extensively in real-world settings, using three different types of testbeds: a single-hop network with 20 MICAz nodes, a multihop network with 37 nodes, and a linear outdoor network with 48 nodes along a 326-m-long bridge. System evaluation and extensive simulation show that CF achieves the same reliability as state-of-the-art solutions while reducing the total number of packet transmission and the dissemination delay by 30%–50% and 35%–50%, respectively.

39. **Efficient multicast QOS Approach for localized clustered based wireless sensor network.**

Limited resources in Wireless Sensor Networks (WSNs) are the key concern that needs to be given a careful consideration when studying virtually any aspect of a sensor network. Therefore, energy demands and radio bandwidth utilization should be addressed, especially in one-to-many communication.To define the problem, this article presents and categorizes he most common WSN multicast procedures depending on the way a target group is identified by the means of geographic position. It is evident that a need for centralized network-wide topology knowledge can jeopardize scarce energy resources of a sensor network. The term multicasting means “Point-to-multipoint" or “one to many”. In multicasting there is one source and multiple receivers, means copy of same data can be transmit to multiple receivers at a same time Multicasting is one of the major communication technologies primarily designed for bandwidth conservation and an efficient way of transferring data to a group of receivers in wireless sensor networks. Providing QoS support in wireless sensor networks is an emerging area of research.Due to resource constraints like processing power, memory, bandwidth and power sources in sensor networks, QoS support in WSNs is a challenging task. In this paper, we discuss the QoS requirements in WSNs and present a survey of some of the QoS aware routing techniques in WSNs

40. **Energy efficient reliable routing approach considering residual energy in Mobile WSN.**

We propose two novel energy-aware routing algorithms for wireless ad hoc networks, called reliable minimum energy cost routing and reliable minimum energy routing .Reliable minimum energy cost routing addresses three important requirements of ad hoc networks: energy-efficiency, reliability, and prolonging network lifetime. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. Reliable minimum energy routing, on the other hand, is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. Reliable minimum energy routing and RELIABLE MINIMUM ENERGY COST ROUTING are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability. Simulation studies show that RELIABLE MINIMUM ENERGY COST

ROUTING is able to find energy-efficient and reliable routes similar to Reliable minimum energy routing, while also extending the operational lifetime of the network. This makes RELIABLE MINIMUM ENERGY COST ROUTING an elegant solution to increase energy-efficiency, reliability, and lifetime of wireless ad hoc networks. In the design of RELIABLE MINIMUM ENERGY COST ROUTING, we consider minute details such as energy consumed by processing elements of transceivers, limited number of retransmissions allowed per packet, packet sizes, and the impact of acknowledgment packets. This adds to the novelty of this work compared to the existing studies.

41. **ALBA-R: Load-Balancing Geographic Routing Around Connectivity Holes in Wireless Sensor Networks**

This paper presents ALBA-R, a protocol for convergecasting in wireless sensor networks. ALBA-R features the cross-layer integration of geographic routing with contention-based MAC for relay selection and load balancing (ALBA), as well as a mechanism to detect and route around connectivity holes (Rainbow). ALBA and Rainbow (ALBA-R) together solve the problem of routing around a dead end without overhead-intensive techniques such as graph planarization and face routing. The protocol is localized and distributed, and adapts efficiently to varying traffic and node deployments. Through extensive ns2-based simulations, we show that ALBA-R significantly outperforms other convergecasting protocols and solutions for dealing with connectivity holes, especially in critical traffic conditions and low-density networks. The performance of ALBA-R is also evaluated through experiments in an outdoor testbed of TinyOS motes. Our results show that ALBA-R is an energy-efficient protocol that achieves remarkable performance in terms of packet delivery ratio and end-to-end latency in different scenarios, thus being suitable for real network deployments.

42. **PEPPDA: Power Efficient Privacy Preserving Data Aggregation for Wireless Sensor Networks**

Energy efficient privacy preserving data aggregation is important in power constrained wireless sensor etworks. Existing hop by hop encrypted privacy preserving data aggregation protocols does not provide efficient solutions for energy constrained and security required WSNs due to the overhead of performing power consuming decryption and encryption at the aggregator node for the data aggregation and the increased number of transmissions for achieving data privacy. The decryption of data at the aggregator node will increase the frequency of node compromise attack. Thereby aggregator node reveals large amounts of data to adversaries. The proposed privacy homomorphism based privacy preservation protocol achieves non delayed data aggregation by performing aggregation on encrypted data. Thereby decreases the node compromise attack frequency. So high chance to get accurate aggregated results at the sink with reduced communication and computation overhead. The PEPPDA technique is best suited for time critical, secure applications such as military application, since it achieves privacy, authenticity, accuracy, end to end confidentiality, data freshness and energy efficiency during data aggregation. Our main aim is to provide a secure data aggregation schemewhich guarantees the privacy, authenticity and freshness of individual sensed data as well as the accuracy and confidentiality of the aggregated data without introducing a significant overhead on the battery limited sensors.

43. **R3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks.**

Providing reliable and efficient communication under fading channels is one of the major technical challenges in wireless sensor networks (WSNs), especially in industrial WSNs (IWSNs) with dynamic and harsh environments. In this work,we present the Reliable Reactive Routing Enhancement (R3E) to increase the resilience to link dynamics for WSNs/IWSNs. R3E is designed to enhance existing reactive routing protocols to provide reliable and energy- efficient packet delivery against the unreliable wireless links by utilizing the local path diversity. Specifically, we introduce a biased backoff scheme during the route-discovery phase to find a robust guide path, which can provide more cooperative forwarding opportunities. Along this guide path, data

packets are greedily progressed toward the destination through nodes' cooperationwithout utilizing the location information. Through extensive simulations, we demonstrate that compared to other protocols, R3E remarkably improves the packet delivery ratio, while maintaining high energy efficiency and low delivery latency

44. **Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs.**

In recent years, applications of wireless sensor networks (WSNs) have been increased due to its vast potential to connect the physical world to the virtual world. Also, an advance in microelectronic fabrication technology reduces the cost of manufacturing portable wireless sensor nodes. It becomes a trend to deploy the large numbers of portable wireless sensors in WSNs to increase the quality of service (QoS). The QoS of such WSNs is mainly affected by the failure of sensor nodes. Probability of sensor node failure increases with increase in number of sensors. In order to maintain the better QoS under failure conditions, identifying and detaching such faults are essential. In the proposed method, faulty sensor node is detected by measuring the round trip delay (RTD) time of discrete round trip paths and comparing them with threshold value. Initially, the suggested method is experimented on WSNs with six sensor nodes designed using microcontroller and ZigBee. Scalability of proposed method is verified by simulating the WSNs with large numbers of sensor nodes in NS2. The RTD time results derived in hardware and software implementations are almost equal, justifying the real time applicability of the investigated method. Necessity of received signal strength measurement in cluster head variation and assigning separate wavelength for each link in other fault detection techniques are overcome here.

45. **An Efficient Reactive Routing Security Scheme Based on RSA Algorithm for Preventing False Data Injection Attack in WSN.**

Wireless sensor networks are vulnerable to various attacks. Injecting false data attack is one of the serious threats to wireless sensor network. In this attack adversary reports bogus information to the sink which causes error decision at upper level and energy waste in en-route nodes. Several authentication techniques using enroute filtering and cryptographic techniques are used for preventing such attacks. This paper focuses on the design of RSA based security scheme with on demand routing. On- demand routing protocol is used in this scheme to lower the energy consumption. This work evaluates and compares the performance of the network system using RSA algorithm and authentication algorithm. Study and implementation of these security schemes are been carried out using network simulator (ns2) and metrics such as Packet Delivery Ratio, Energy, Throughput. Results are presented as a function of these metrics and the graphs generated show that RSA based security scheme with on-demand routing performs better than the security schemes using authentication algorithms.