IEEE 2014 papers

1) 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.

2) Clustering of Mobile Ad Hoc Networks: An Approach for Black Hole Prevention

This paper addresses security and performance issues of MANET. A novel cluster-oriented concept is proposed to enhance security and efficiency of the network. Proposed strategy insures the optimum performance of MANET in presence of black hole attack. The simulation of the proposed methodology is carried out using NS2 network simulator and the simulation results reflects the performance of scheme for detection and prevention of the black hole.

3) Comparative Study Of Proactive and Reactive AdHoc Routing Protocols Using Ns2

A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point or administration. MANET protocols have to face high challenges due to dynamically changing topologies, low transmission power and asymmetric links of network. An attempt has been made to compare the performance of two On-demand reactive routing protocols namely AODV and DSR which works on gateway discovery algorithms and a proactive routing protocol namely DSDV which works on an algorithm to constantly update network topology information available to all nodes for MANETs on different scenarios. In this paper comparison is made on the basis of performance metrics such as throughput, packet loss and end-to-end delay, and the simulator used is NS-2 in Ubuntu operating system (Linux). The simulations are carried out by varying the packet size, number of connecting nodes at a time and pause time and the results are analyzed.

4) Effect of Number of Active Nodes and Inter-node Distance on the Performance of Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are used to monitor different ambient conditions. These networks can be used for constant environment and habitat monitoring applications such as sensing of humidity, temperature, soil moisture and fire. All these applications have certain desired network performance and lifetime requirements. In this paper, we present our findings about variation in network performance and energy efficiency with varying number of active nodes and inter-node distance in WSNs. Change of network behavior with changing network conditions is studied through simulations carried out in ns2.34.

5) Re-Organizable Wireless Mesh Network Using ARS

In recent years wireless communication is most widely used, but there is also traffic in surrounding environment, while transferring the data from source to destination. This can be possible due to channel interference, various obstacles, which result in link failure causes poor performance, require expensive network management for their recovery. To maintain the network performance Autonomous network reconfiguration system (ARS) is used which autonomously reconfigure and recover from local link failure. Through NS2 based simulation ARS has been implemented and evaluated. ARS improves the channel efficiency better than other recovery methods for example reroute and greedy channel.

6) 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.

7) Transmission Energy Management for Wireless Ad-hoc Network

Remaining energy is the energy of the nodes after transreceiving data in network. This energy of nodes is the main parameter to control the energy consumption of wireless mobile ad-hoc networks. An optimum remaining energy is required to maintain life of network. In this paper, transmission energy management is proposed to optimize energy consumption of nodes in network. Transmission energy consumption is inversely proportional to remaining energy of node in network. NS2 simulation model is used to analysis energy consumption of nodes in network and results show that varying the transition and receiving energy affects the remaining energy of nodes in network.

8) 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.

9) 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.

10) 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.

11) 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.

12) 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.

13) 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.

14) 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 scheme
which 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.

15) Passive cluster-based multipath routing protocol for wireless sensor networks
Energy efficiency and quality of service (QoS) are both essential issues in the applications of wireless sensor networks (WSNs) all along, which are mainly reflected in the development of routing and MAC protocols. However, there is little design for achieving the dual performances simultaneously. In this paper, we develop a practical passive cluster-based node-disjoint many to one multipath routing protocol to satisfy the requirements of energy efficiency and QoS in practical WSNs. Passive clustering approach is put to use in the first round, while active clustering technique is taken in the other rounds. Implementation of smart delay strategy makes the cluster distribute uniformly, as well as lessen the number of nodes that have taken part in routing. Among cluster heads, a node-disjoint many to one multipath routing discovery algorithm, which is composed of the optimal path searching process and multipath expansion process, is implemented to find multiple paths at the minimum cost. The simulation results show the proposed protocol achieved very good performance both in energy efficiency and QoS.

16) A hybrid multi-path routing algorithm for industrial wireless mesh networks
Multi-path routing, a routing technique that enables data transmission over multiple paths, is an effective strategy in achieving reliability in wireless sensor networks. However, multi-path routing does not guarantee deterministic transmission. This is because more than one path is available for transferring data from the source node to the destination node. A hybrid multi-path routing algorithm is proposed for industrial wireless mesh networks for improving reliability and determinacy of data transmission, as well as to effectively deal with link failures. The proposed algorithm adopts the enhanced Dijkstra's algorithm for searching the shortest route from the gateway to each end node for first route setup. A virtual pheromone distinct from the regular pheromone is introduced to realize pheromone diffusion and updating. In this way, multiple routes are searched based on the ant colony optimization algorithm. The routes used for data transmission are selected based on their regular pheromone values, facilitating the delivery of data through better routes. Link failures are then handled using route maintenance mechanism. Simulation results demonstrate that the proposed algorithm outperforms traditional algorithms in terms of average end-to-end delay, packet delivery ratio, and routing overhead; moreover, it has a strong capacity to cope with topological changes, thereby making it more suitable for industrial wireless mesh networks.

17) Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks
Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These “Vampire” attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of $O(N)$, where $N$ in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

18) ELBAR: Efficient Load Balanced Routing Scheme for Wireless Sensor Networks with Holes
A critical issue in designing efficient routing algorithms for wireless sensor networks (WSN) is dealing with holes which do occur due to several reasons, including cases caused by natural obstacles or disaster suffered areas. Traditional solutions utilize perimeter routing techniques that however lead to traffic concentration on the nodes on the hole boundary, which can make these nodes getting energy exhausted and the hole enlarging, consequently. Several recent proposals attempt to fix this by deploying a special, forbidding area around the hole, which helps to improve path length but still causes significant load unbalancing due to the fixed shape of this forbidding area. We introduce a novel approach in dealing with routing holes where the packet forwarder node notices early enough about the occurrence of a hole in the direction to the destination.
and hence, can bend the path around this hole efficiently. This can be done by deploying a hole aware area around the hole where each node maintains an angle of its view to this hole. We achieve this hole awareness mechanism by using an economical learn-and-disseminate strategy where the nodes on a hole's boundary learn and create a core shape of the hole and then economically disseminate this information piece to the surrounding neighborhood of a controlled size wherein each node then compute and store its holeview angle. To the best of our knowledge, our proposed routing scheme is the first one that targets and achieves both the two requirements of energy efficiency and load balancing in dealing with the occurrence of holes. Our simulation experiments show that our scheme strongly outperforms several important existing schemes in several performance factors, including route length, efficient use of energy and load balancing.

19) A Zone-Based Node Replica Detection Scheme for Wireless Sensor Networks
Wireless sensor networks (WSNs) are susceptible to various kinds of attack, and node replication attack is one of them. It is considered to be one of the most serious attacks in WSN. In this type of attack, an adversary deploys clones of a legitimate node. These clones participate in all network activities and behave identically same as the legitimate node. Therefore, detection of clones in the network is a challenging task. Most of the work reported in the literature for clone detection is location dependent. In this paper, we have proposed a location independent zone-based node replica detection technique. In the proposed scheme, the network is dynamically divided into a number of zones. Each zone has a zone-leader, and they share their membership list among themselves. It is the responsibility of the zoneleader to detect the clone. The proposed technique is a deterministic one. We have compared our scheme with LSM, RED, and P-MPC and observed that it has a higher clone detection probability and a lower communication cost.

20) STARS: A Statistical Traffic Pattern Discovery System for MANETs
Many anonymity enhancing techniques have been proposed based on packet encryption to protect the communication anonymity of mobile ad hoc networks (MANETs). However, in this paper, we show that MANETs are still vulnerable under passive statistical traffic analysis attacks. To demonstrate how to discover the communication patterns without decrypting the captured packets, we present a novel statistical traffic pattern discovery system (STARS). STARS works passively to perform traffic analysis based on statistical characteristics of captured raw traffic. STARS is capable of discovering the sources, the destinations, and the end-to-end communication relations. Empirical studies demonstrate that STARS achieves good accuracy in disclosing the hidden traffic patterns.

21) 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 improve 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’ cooperation without 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.

22) Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks
Mobile ad hoc networks (MANET) refers to a network designed for special applications for which it is difficult to use a backbone network. In MANETs, applications are mostly involved with sensitive and secret information. Since MANET assumes a trusted environment for routing, security is a major issue. In this paper, we analyze the vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR) against a specific type of denial-of-service (DOS) attack called node isolation attack. Analyzing the attack, we propose a mechanism called enhanced OLSR (EOLSR) protocol which is a trust based technique to secure the OLSR nodes against the attack. Our technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks. The experiment results show that our protocol is able to achieve routing security with 45% increase in packet delivery ratio and 44% reduction in packet loss rate when compared to standard OLSR under node isolation attack. Our technique is light.
Data communication in mobile ad hoc cognitive networks (MACNets) significantly suffers from link instability and channel interference. The availability and stability of each link in MACNets highly depends on not only the relative movement of neighbor nodes but also the adjacent communication among primary nodes and among cognitive nodes. In multihop and multilow MACNets, this problem becomes even worse because multiple links potentially interfere with each other. In this paper, we propose a cross-layer distributed approach, called mobility-prediction-based joint stable routing and channel assignment (MP-JSRCA), to maximize the network throughput by jointly selecting stable routes and assigning channels avoiding inter- and intra-flow interferences based on mobility prediction. To quantitatively measure the communication quality of links, we propose a new metric data transmission cost (DTC) that captures node mobility, impact to primary nodes, and channel interference. The availability and stability of each link in MACNets highly depends on not only the relative movement of neighbor nodes but also the adjacent communication among primary nodes and among cognitive nodes. In multihop and multilow MACNets, this problem becomes even worse because multiple links potentially interfere with each other. In this paper, we propose a cross-layer distributed approach, called mobility-prediction-based joint stable routing and channel assignment (MP-JSRCA), to maximize the network throughput by jointly selecting stable routes and assigning channels avoiding inter- and intra-flow interferences based on mobility prediction. To quantitatively measure the communication quality of links, we propose a new metric data transmission cost (DTC) that captures node mobility, impact to primary nodes, and channel interference. The availability and stability of each link in MACNets highly depends on not only the relative movement of neighbor nodes but also the adjacent communication among primary nodes and among cognitive nodes. In multihop and multilow MACNets, this problem becomes even worse because multiple links potentially interfere with each other. In this paper, we propose a cross-layer distributed approach, called mobility-prediction-based joint stable routing and channel assignment (MP-JSRCA), to maximize the network throughput by jointly selecting stable routes and assigning channels avoiding inter- and intra-flow interferences based on mobility prediction. To quantitatively measure the communication quality of links, we propose a new metric data transmission cost (DTC) that captures node mobility, impact to primary nodes, and channel interference.
conflict among cognitive nodes. In our MP-JSRCA, each relay node selects the best link with the smallest DTC as the next hop, within a specified sector region towards the destination. NS2-based simulation results demonstrate that our MP-JSRCA algorithm significantly improves network throughput, and the higher degree of interference MACNets experience, the more improvement can be achieved.

27) Distributed Multipath Routing for Data Center Networks based on Stochastic Traffic Modeling
Modern data center networks often adopt multi path topologies for greater bisection bandwidth and better fault tolerance. However, traditional distributed routing algorithms make routing decisions based on only packet destinations, and cannot readily utilize the multi path feature. In this paper, we study distributed multi path routing for data center networks. First, to capture the time varying and non-deterministic nature of data center network traffic, we present a stochastic traffic model based on the log normal distribution. Then, we formulate the stochastic load-balanced multi path routing problem, and prove that it is NP hard for typical data center network topologies, including the fat tree, VL2, DCell, and BCube. Next, we propose our distributed multi path routing algorithm, which balances traffic among multiple links by minimizing the probability of each link to face congestion. Finally, we implement the proposed algorithm in the NS2 simulator, and provide simulation results to demonstrate the effectiveness of our design.

28) EEFA: Energy Efficiency Frame Aggregation Scheduling Algorithm for IEEE 802.11 Wireless Network
Packet size is restricted due to the error-prone wireless channel which drops the network energy utilization. Furthermore, the frequent packet retransmissions also lead to energy waste. In order to improve the energy efficiency of wireless networks and save the energy of wireless devices, EEFA (Energy Efficiency Frame Aggregation), a frame aggregation based energy-efficient scheduling algorithm for IEEE 802.11 wireless network, is proposed. EEFA changes the size of aggregated frame dynamically according to the frame error rate, so as to ensure the data transmission and retransmissions completed during the TXOP and reduce energy consumption of channel contention. NS2 simulation results show that EEFA algorithm achieves better performance than the original frame-aggregation algorithm.

29) Energy Efficient Cluster Head Selection Algorithm in Mobile Wireless Sensor Networks
In Wireless sensor networks, existing energy efficient routing algorithms assumed that the sensor nodes are stationary. Some of the applications in WSN must combine with both mobile sensor nodes and fixed sensor nodes in the same networks. When mobility is functioned there should be performance degradation. Because these nodes are equipped with a lesser amount of memory, restricted battery power, little computation capability, and small range of communication. So there is a need for energy efficient routing protocol to forward the incoming packet. In this paper, we propose Energy Efficient Cluster Head Selection Protocol in Mobile Wireless Sensor Network (EECHS-MWSN). The cluster-head nodes are selected from the residual energy, lowest mobility factor and density of the node. It is also used that the Gateway nodes are act as an intermediate node to transfer the data to the Base station. Simulation results show that the EECHS-MWSN protocol has more Energy consumption, network lifetime and throughput than the existing LEACH-Mobile protocol.

30) Genetically derived secure cluster-based data aggregation in wireless sensor networks
In wireless sensor networks (WSNs), the current cluster-based data aggregation technique consumes more energy. Also the secured data transmission are vital for enhancing the data authentication and confidentiality. In order to overcome these issues, in this study, the authors propose a genetically derived secure cluster-based data aggregation in WSN. Initially the cluster heads are selected based on the node connectivity, which acts as a data aggregator. Then, the clustering process is executed using the genetic algorithm. When a cluster member wants to transmit the data to aggregator, a data encryption technique are utilised that offers authenticity, confidentiality and integrity. By simulation results, the authors show that the proposed technique minimizes the energy consumption, ensures data security and reduces the transmission overhead.

31) Path Load Balanced Adaptive Gateway Discovery in Integrated Internet-MANET
An interconnection of mobile ad hoc network and wired Internet is called Integrated Internet-MANET. This interconnection is achieved through gateways. There are two very important issues in Integrated Internet-MANET. First, path load balancing in the communication of mobile nodes with gateways. Second, mobile nodes register with a gateway before communication begins. This registration is achieved through agent advertisement
messages. The issue is, for how many hops these gateway advertisement messages must be forwarded. In this paper we propose a gateway discovery algorithm which addresses the above issues. Simulation results show that our approach outperforms the existing approach.

32) An Evaluation of the TPGF Protocol Implementation over NS-2

Wireless multimedia sensor networks (WMSNs) is one of the hottest topic nowadays which attracts more and more researchers as being an interdisciplinary research interest. Its cost decreases continously due to advances in micro-electromechanical systems, and the proliferation and progression of wireless communications. However, the transmission of multimedia information must satisfy QoS criteria which increases energy consumption. This issue should be taken into consideration in the protocol design for WMSNs. In this paper, we propose an implementation and an evaluation of the TPGF routing protocol (Two Phase geographical Greedy Forwarding) over the network simulator NS2. The TPGF module over NS-2 is available for the research community. In this evaluation, we compare the TPGF performances with two other protocols: the well known AODV protocol and the EA-TPGF protocol (our previous work on an extension of the TPGF protocol which takes into account the remaining energy of nodes during the process of path identification). The performance metrics measured to evaluate the QoS of each protocol are: delay, PDR, remaining energy of each node at the end of the communication and the standard deviation of remaining energy. Simulations show promising results in terms of network life extension when TPGF is used.

33) Distributed and Fast Detection of Mobile Replica Node Capture Attacks Using Sequential Hypothesis Testing For WSN

Security is important for many sensor network applications. Wireless Sensor Networks (WSN) are often deployed in hostile environments as static or mobile, where an adversary collects all the credentials like keys and identity. The attacker can reprogram it and replicate the node in order to eavesdrop the transmitted messages or compromise the functionality of the network. A harmful attack against sensor networks where one or more nodes illegitimately claims an identity as replicas is known as the node replication attack. This paper detects the node replication attack using Efficient Distributed Detection, Scheme and Game theoretic approach to improve the performance.