Nxtlogic
SOFTWARE SOLUTIONS
We inspire the next

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

Project Code	NS2 IEEE PAPERS-2016 PROJECT TITLES WITH ABSTRACT
	WIRELESS SENSOR NETWORKS
NXT01NS2	**TITLE: Analysis of PKF: A Communication Cost Reduction Scheme for Wireless Sensor Networks.** **ABSTRACT:** Energy efficiency is a primary concern for wireless sensor networks (WSNs). One of its most energy-intensive processes is the radio communication. This work uses a predictor combined with a Kalman filter (KF) to reduce the communication energy cost for cluster-based WSNs. The technique, called PKF, is suitable for typical WSN applications with adjustable data quality and tens of picojoule computation cost. However, it is challenging to precisely quantify its underlying process from a mathematical point of view. Through an in-depth mathematical analysis, we formulate the tradeoff between energy efficiency and reconstruction quality of PKF. One of our prominent results for that is the explicit expression for the covariance of the doubly truncated multivariate normal distribution; it improves the previous methods and has generality. The validity and accuracy of the analysis are verified with both artificial and real signals. The simulation results, using real temperature values, demonstrate the efficiency of PKF: without additional data degradation, it reduces the communication cost by more than 88%. Compared to previous works based on KF, PKF requires less computational effort while improving the reconstruction quality; compared with the techniques without KF, the advantages of PKF are even more significant. It reduces the transmission rate of them by at least 29%. Besides, it can be integrated into network level techniques to further extend the whole network lifetime.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT02NS2	**TITLE: Online Packet Dispatching for Delay Optimal Concurrent Transmissions in Heterogeneous Multi-RAT Networks** **ABSTRACT:** In this paper, we consider the problem of concurrent transmissions in a wireless network consisting of multiple radio access technologies (multi-RATs). That is, a single flow of packets is dispatched over multiple RATs so that the complementary advantages of different RATs can be exploited. One of the challenging issues arising in concurrent transmissions is the packet outof- order problem due to diverse wireless channel states and scheduling policies of different RATs, leading to substantial performance degradation to delay sensitive applications. To address this problem, we firstly propose a state-independent packet dispatching (SIPD) policy, which attempts to find the traffic dispatching ratios over multiple RATs to minimize the maximum average delay across different RATs in the long run. We further propose a state-dependent packet dispatching (SDPD) policy, which achieves fine-grained packet dispatching in the short-term. We use the value function as a measure of the admittance cost for packet dispatching given the current queueing states, and formulate the SDPD problem as a convex programming problem. We derive the close-form solutions for both problems for the special case of two RATs, and adopt the dual decomposition technique as the solution for the general cases. Simulation results are presented to compare the performance of the proposed schemes with existing solutions.
NXT03NS2	**TITLE: Toward Optimal Adaptive Wireless Communications in Unknown Environments** **ABSTRACT:** Designing efficient channel access schemes for wireless communications without any prior knowledge about the nature of environments has been a very challenging issue, in which the channel state distribution of all spectrum resources could be entirely or partially stochastic or adversarial at different times and locations. In this paper, we propose an online learning algorithm for adaptive channel access of wireless communications in

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	unknown environments based on the theory of multiarmed bandits (MAB) problems. By automatically tuning two control parameters, i.e., learning rate and exploration probability, our algorithms could find the optimal channel access strategies and achieve the almost optimal learning performance over time in different scenarios. The quantitative performance studies indicate the superior throughput gain when compared with previous solutions and the flexibility of our algorithm in practice, which is resilient to both oblivious and adaptive jamming attacks with different intelligence and attacking strength that ranges from no-attack to the full-attack of all spectrum resources. We conduct extensive simulations to validate our theoretical analysis.
NXT04NS2	**TITLE: Adaptive Pilot Clustering in Heterogeneous Massive MIMO Networks** **ABSTRACT:** We consider the uplink of a cellular massive MIMO network. Acquiring channel state information at the base stations (BSs) requires uplink pilot signaling. Since the number of orthogonal pilot sequences is limited by the channel coherence, pilot reuse across cells is necessary to achieve high spectral efficiency. However, finding efficient pilot reuse patterns is nontrivial especially in practical asymmetric BS deployments. We approach this problem using coalitional game theory. Each BS has a few unique pilots and can form coalitions with other BSs to gain access to more pilots. The BSs in a coalition thus benefit from serving more users in their cells, at the expense of higher pilot contamination and interference. Given that a cell's average spectral efficiency depends on the overall pilot reuse pattern, the suitable coalitional game model is in partition form. We develop a low-complexity distributed coalition formation based on individual stability. By incorporating a base station intercommunication budget constraint, we are able to control the overhead in message exchange between the base stations and ensure the algorithm's convergence to a solution of the game called individually stable coalition structure. Simulation results reveal fast algorithmic convergence and substantial performance gains over the baseline schemes with no pilot reuse,

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	full pilot reuse, or random pilot reuse pattern.
NXT05NS2	**TITLE: Data Aggregation and Principal Component Analysis in WSNs** **ABSTRACT:** Data aggregation plays an important role inWireless Sensor Networks (WSNs) as far as it reduces power consumption and boosts the scalability of the network, specially in topologies that are prone to bottlenecks (e.g. cluster-trees). Existing works in the literature use clustering approaches, Principal Component Analysis (PCA) and/or Compressed Sensing (CS) strategies. Our contribution is aligned with PCA and explores whether a projection basis that is not the eigenvectors basis may be valid to sustain a Normalized Mean Squared Error (NMSE) threshold in signal reconstruction and reduce the energy consumption. We derivate first the NSME achieved with the new basis and elaborate then on the Jacobi eigenvalue decomposition ideas to propose a new subspace-based data aggregation method. The proposed solution reduces transmissions among the sink and one or more Data Aggregation Nodes (DANs) in the network. In our simulations we consider without loss of generality a single cluster network and results show that the new technique succeeds in satisfying the NMSE requirement and gets close in terms of energy consumption to the best possible solution employing subspace representations. Additionally the proposed method alleviates the computational load with respect to an eigenvector-based strategy (by a factor of six in our simulations).
NXT06NS2	**TITLE: A New cost-effective approach for Battlefield Surveillance in Wireless Sensor Networks** **ABSTRACT:** Assuring security (in the form of attacking mode as well as in safeguard mode) and at the same time keeping strong eye on the opposition's status (position, quantity, availability) is the key responsibility of a commander in the battlefield. Battlefield surveillance is one of the strong applications of Wireless Sensor Networks (WSNs). A commander is not only liable to his above responsibilities, but also to manage his duties in an efficient way. For this

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	reason, ensuring maximum destruction with minimum resources is a major concern of a commander in the battlefield. This paper focuses on the maximum destruction problem in military affairs. In the work of Jaigirdar and Islam (2012), the authors proposed two novel algorithms (Maximum degree analysis and Maximum clique analysis) that ensure the efficiency and cost-effectiveness of the above problem. A comparative study explaining the number of resources required for commencing required level of destruction made to the opponents has been provided in the paper. In this paper the authors have come forward with another algorithm for the same problem. With the simulation studies and comparative analysis of the same example set the authors in this paper demonstrate the effectiveness (in both the quality and quantity) of the new method to be best among the three.
NXT07NS2	**TITLE: Energy-Efficient Cooperative Relaying for Unmanned Aerial Vehicles** **ABSTRACT:** Airborne relaying can extend wireless sensor networks (WSNs) to remote human-unfriendly terrains. However, lossy airborne channels and limited battery of unmanned aerial vehicles (UAVs) are critical issues, adversely affecting success rate and network lifetime, especially in real-time applications. We propose an energy-efficient cooperative relaying scheme which extends network lifetime while guaranteeing the success rate. The optimal transmission schedule of the UAVs is formulated to minimize the maximum (min-max) energy consumption under guaranteed bit error rates, and can be judiciously reformulated and solved using standard optimisation techniques. We also propose a computationally efficient suboptimal algorithm to reduce the scheduling complexity, where energy balancing and rate adaptation are decoupled and carried out in a recursive alternating manner. Simulation results confirm that the suboptimal algorithm cuts off the complexity by orders of magnitude with marginal loss of the optimal network yield (throughput) and lifetime. The proposed suboptimal algorithm can also save energy by 50

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	percent, increase network yield by 15 percent, and extend network lifetime by 33 percent, compared to the prior art.
NXT08NS2	**TITLE: CANS: Towards Congestion-Adaptive and Small Stretch Emergency Navigation with Wireless Sensor Networks** **ABSTRACT:** One of the major applications of wireless sensor networks (WSNs) is the navigation service for emergency evacuation, the goal of which is to assist people in escaping from a hazardous region safely and quickly when an emergency occurs. Most existing solutions focus on finding the safest path for each person, while ignoring possible large detours and congestions caused by plenty of people rushing to the exit. In this paper, we present CANS, a C ongestion-Adaptive and small stretch emergency Navigation algorithm with WSNs. Specifically, CANS leverages the idea of level set method to track the evolution of the exit and the boundary of the hazardous area, so that people nearby the hazardous area achieve a mild congestion at the cost of a slight detour, while people distant from the danger avoid unnecessary detours. CANS also considers the situation in the event of emergency dynamics by incorporating a local yet simple status updating scheme. To the best of our knowledge, CANS is the first WSN-assisted emergency navigation algorithm achieving both mild congestion and small stretch, where all operations are in-situ carri ed out by cyber-physical interactions among people and sensor nodes. CANS does not require location information, nor the reliance on any particular communication model. It is also distributed and scalable to the size of the network with limited storage on each node. Both experiments and simulations validate the effectiveness and efficiency of CANS.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT09NS2	**TITLE: A Traffic Adaptive Multi-Channel MAC Protocol with Dynamic Slot Allocation for WSNs** **ABSTRACT:** Using low duty-cycle is the most common technique to extend the system lifetime in WSNs. However, it also implies limited throughput and long delay and the penalty is even higher under variable traffic patterns. In this paper, we present iQueue-MAC, a hybrid CSMA/TDMA MAC that adapts to variable/bursty traffic. With light load, iQueue-MAC uses a contention-based CSMA mechanism that provides low delay with scattered transmissions. When traffic increases, detected by a forming backlog in the sender, iQueue-MAC changes to a contention-free TDMA mechanism allocating transmission slots. Thus, iQueue-MAC mitigates packet buffering and reduces packet delay, combining the best of TDMA and CSMA. In this paper we also show how iQueue-MAC can operate in both single and multi channel modes. We implemented it on SIM32W108 chips together with other reference WSN protocols for comparison. iQueue-MAC exhibits similar figures during light traffic. However, with bursty traffic its throughput can be five times that of CoSenS and Ri-MAC-MC and its delay 20 times lower. Finally, iQueue-MAC is able to effectively use multiple channels, duplicating its throughput when compared to single channel operation.
NXT10NS2	**TITLE: Distributed Workload Dissemination for Makespan Minimization in Disruption Tolerant Networks** **ABSTRACT:** Mobile devices are undergoing explosive proliferation today. Although they are gaining more and more capabilities, they still fall short to execute complex applications. One possible solution to alleviate this limitation is offloading tasks to remote clouds. However, it may require persistent connectivity to the Internet and thus is not always available or affordable. An alternative solution is taking advantage of pervasive mobile devices and their pairwise encounters. In this paradigm, complex tasks from mobile devices are

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	processed in a distributed and collaborative fashion on all mobile devices that are loosely-connected. Working towards this vision, this paper studies the following problem: given a task that originates at some node in a Disruption Tolerant Network (DTN), how are we to disseminate the task's workload during the pairwise contacts among mobile devices to achieve makespan minimization? We first imagine access to an oracle that has global and future knowledge of node mobility, and we design a provably-optimal centralized polynomial-time solution as the benchmark for comparison. With the insights obtained from the centralized solution, we then develop a distributed dissemination algorithm, D2, which maintains certain neighborhood information at individual nodes. D2 makes dissemination decisions based on the estimations of the potential computational capacities and the future workloads of mobile nodes. Extensive trace-driven simulations confirm the effectiveness of D2.
NXT11NS2	**TITLE: Joint Optimization of Transmission Power Level and Packet Size for WSN Lifetime Maximization** **ABSTRACT:** In pursuit of better energy efficiency and enhanced network lifetime in wireless sensor networks (WSNs), two crucial factors are data packet size and transmission power level. On one hand, smaller packet size reduces the overall impact of bit error rates on packet loss. However, the consequence of smaller packet size is fragmentation into more data packets and thereby dissipation of increased energy. Hence, there emerges a delicate engineering tradeoff in deciding the data packet size, where both low and high data packet size decisions lead to certain energy inefficiency issues. On the other hand, increasing transmission power level decreases packet loss probability, which is another decision variable to optimize for maximizing network lifetime. Joint consideration of these two factors exacerbates the complexity of the optimization problem for the objective of the network lifetime maximization. In

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	this paper, we develop a realistic WSN link layer model built on top of the empirically verified energy dissipation characteristics of Mica2 motes and WSN channel models. We make use of the aforementioned link layer model to design a novel mixed integer programming (MIP) framework for the joint optimization of transmission power level and data packet size to take up the challenge introduced above. Numerical evaluations of the MIP framework with the analysis of the results over a large parameter space are performed to characterize the effects of joint optimization of packet size and power level on WSN lifetime.
NXT12NS2	**TITLE: Improving Energy Efficiency of Mobile WSN Using Reconfigurable Directional Antennas** **ABSTRACT:** Reconfigurable directional antennas (RDA) bring new opportunities to reduce data collision in wireless sensor networks (WSN). In this letter, a new reconfigurable directional antenna-based receiver-Initiated cycled receiver (RDA-RICER) medium access control (MAC) protocol is proposed for WSN nodes equipped with switched antennas. A low complexity and energy efficient scanning process is embedded in RDA-RICER to identify the direction providing the highest received signal strength Indicator between two nodes. OMNeT++ simulation results for a single hop network show that data collision rate can be drastically reduced compared with related MAC protocols, leading to a significant decrease in energy consumption. Our approach is also validated in the field using WSN platforms equipped with a four-direction RDA, and powered by solar cells.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT13NS2	**TITLE: RAEED-EA: A formally analysed energy efficient WSN routing protocol** **ABSTRACT:** The operational efficiency and lifetime of Wireless Sensor Network (WSNs) suffers from several factors among which the security and energy consumption are the most important. Most of the WSN routing protocols are designed either from the perspective of security or energy. In this paper, the network lifetime of Robust Formally Analysed Protocol for Wireless Sensor Networks Deployment (RAEED) is improved by introducing a new version of RAEED called RAEED with energy-aware-routing (RAEED-EA). Energy aware routing requires introducing suitable changes in the third and final phase i.e. Data Forwarding Phase of RAEED. In RAEED the decision of selecting the next node was entirely based on the throughput of the target nodes, whereas in RAEED-EA the decision is taken based upon residual energy and throughput of the target nodes. For performance evaluation formal verification is used and these protocols are compared in terms of minimum network lifetime. Results show that by changing the network topology the gain in network lifetime of a network using RAEED-EA over RAEED ranges from 3 percent to 40 percent.
NXT14NS2	**TITLE: Design and performance evaluation of an energy efficient routing protocol for Wireless Sensor Networks** **ABSTRACT:** In recent years, the advancements in wireless communications and electronics have enabled the development of low-cost, low-power and multi-functional Wireless Sensor Networks (WSNs). As nodes in sensor networks are equipped with a limited power source, efficient utilization of power is a very important issue in order to extend the network lifetime. In this paper, a routing protocol namely GAICH (Genetic Algorithm Inspired Clustering Hierarchy) that provide efficient energy management for WSNs is proposed. This protocol makes use of Genetic Algorithm(GA) to create optimum clusters in terms of energy consumption. Using a standard radio energy dissipation model that is used for the simulation of WSNs, the performance of this algorithm is

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	simulated and compared with an already existing LEACH routing protocol for WSNs.
NXT15NS2	**TITLE: Evaluation of the Energy Consumption and the Packet Loss in WSNs Using Deterministic Stochastic Petri Nets** **ABSTRACT:** When developing critical and complex systems, the analysis and the performance evaluation of the designed system is a challenging task. Wireless Sensor Networks (WSNs) are examples of such systems. A WSN consists of a large amount of distributed nodes which monitor physical or environmental conditions. In this paper, we address the problem of how WSNs must be designed to have good performances in particular the energy consumption and the packet loss ratio. To do so, we use an expressive kind of Petri Nets called Deterministic Stochastic Petri Nets. To show the applicability of the proposed model, one of routing techniques dedicated for WSNs is presented.
NXT16NS2	**TITLE: Cost-Aware Activity Scheduling for Compressive Sleeping Wireless Sensor Networks** **ABSTRACT:** In this paper, we consider a compressive sleeping wireless sensor network (WSN) for monitoring parameters in the sensor field, where only a fraction of sensor nodes (SNs) are activated to perform the sensing task and their data are gathered at a fusion center (FC) to estimate all the other SNs' data using the compressive sensing (CS) principle. Typically, research published concerning CS implicitly assume the sampling costs for all samples are equal and suggest random sampling as an appropriate approach to achieve good reconstruction accuracy. However, this assumption does not hold for compressive sleeping WSNs, which have significant variability in sampling cost owing to the different physical conditions at particular SNs. To exploit this sampling cost nonuniformity, we propose a cost-aware activity scheduling approach that minimizes the sampling cost with constraints on the regularized

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	mutual coherence of the equivalent sensing matrix. In addition, for the case with prior information about the signal support, we extend the proposed approach to incorporate the prior information by considering an additional constraint on the mean square error (MSE) of the oracle estimator for sparse recovery. Our numerical experiments demonstrate that, in comparison with other designs in the literature, the proposed activity scheduling approaches lead to improved tradeoffs between reconstruction accuracy and sampling cost for compressive sleeping WSNs.
NXT17NS2	**TITLE: A Kautz-Based Wireless Sensor and Actuator Network for Real-Time, Fault-Tolerant and Energy-Efficient Transmission** **ABSTRACT:** Wireless sensor and actuator networks (WSANs) are composed of sensors and actuators to perform distributed sensing and actuating tasks. Most WSAN applications (e.g., fire detection) demand that actuators rapidly respond to observed events. Therefore, real-time (i.e., fast) and fault-tolerant transmission is a critical requirement in WSANs to enable sensed data to reach actuators reliably and quickly. Due to limited power resources, energy-efficiency is another crucial requirement. Such requirements become formidably challenging in large-scale WSANs. However, existing WSANs fall short in meeting these requirements. To this end, we first theoretically study the Kautz graph for its applicability in WSANs to meet these requirements. We then propose a Kautz-based REal-time, Fault-tolerant and EneRgy-efficient WSAN (REFER). REFER embeds Kautz graphs into the physical topology of a WSAN for real-time communication and connects the Kautz graphs using distributed hash table (DHT) for high scalability. We also theoretically study routing paths in the Kautz graph, based on which we develop an efficient fault-tolerant routing protocol. It enables a relay node to quickly and efficiently identify the next shortest path from itself to the destination based only on node IDs upon routing failure, rather than relying on retransmission from the

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	source. REFER is advantageous over previous Kautz graph based works in that it does not need an energy-consuming protocol to find the next shortest path and it preserves the consistency between the overlay and physical topology. We further improve routing in REFER by multi-path based routing and energy-efficient multicasting within and between Kautz graph cells, respectively. Extensive experimental results demonstrate the superior performance of REFER in comparison with existing WSAN systems in terms of real-time communication, energy-efficiency, fault-tolerance and scalability.
NXT18NS2	**TITLE: Cluster-Based Routing for the Mobile Sink inWireless Sensor Networks With Obstacles** **ABSTRACT:** In wireless sensor networks (WSNs), the bene_ts of exploiting the sink mobility to prolongnetwork lifetime have been well recognized. In physical environments, all kinds of obstacles could exit inthe sensing _eld. Therefore, a research challenge is how to ef_ciently dispatch the mobile sink to _nd anobstacle-avoiding shortest route. This paper presents an energy-ef_cient routing mechanism based on thecluster-based method for the mobile sink in WSNs with obstacles. According to the cluster-based method,the nodes selected as cluster heads collect data from their cluster members and transfer the data collectedto the mobile sink. In this paper, the mobile sink starts the data-gathering route periodically from thestarting site, then directly collects data from these cluster heads in a single-hop range, and _nally returnsto the starting site. However, due to the complexity of the scheduling problem in WSNs with obstacles, theconventional algorithms are dif_cult to resolve. To remedy this issue, we propose an ef_cient schedulingmechanism based on spanning graphs in this paper. Based on the spanning graph, we present a heuristictour-planning algorithm for the mobile sink to _nd the obstacle-avoiding shortest route. Simulation resultsverify the effectiveness of our method.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT19NS2	**TITLE: Code-Based Neighbor Discovery Protocols in Mobile Wireless Networks** **ABSTRACT:** In mobile wireless networks, the emerging proximity-based applications have led to the need for highly effective and energy-efficient neighbor discovery protocols. However, existing works cannot realize the optimal worst-case latency in the symmetric case, and their performances with asymmetric duty cycles can still be improved. In this paper, we investigate asynchronous neighbor discovery through a code-based approach, including the symmetric and asymmetric cases. We derive the tight worst-case latency bound in the case of symmetric duty cycle. We design a novel class of symmetric patterns called Diff-Codes, which is optimal when the Diff-Code can be extended from a perfect difference set. We further consider the asymmetric case and design ADiff-Codes. To evaluate (A)Diff-Codes, we conduct both simulations and testbed experiments. Both simulation and experiment results show that (A)Diff-Codes significantly outperform existing neighbor discovery protocols in both the median case and worst case. Specifically, in the symmetric case, the maximum worst-case improvement is up to 50%; in both symmetric and asymmetric cases, the median case gain is as high as 30%.
NXT20NS2	**TITLE: DaGCM: A Concurrent Data Uploading Framework for Mobile Data Gathering in Wireless Sensor Networks** **ABSTRACT:** Data uploading time constitutes a large portion of mobile data gathering time in wireless sensor networks. By equipping multiple antennas on the mobile collector, data uploading time can be greatly shortened. However, previous works only treated wireless link capacity as a constant and ignored power control on sensors, which would significantly deviate from the real wireless environments. To overcome this problem, in this paper we propose a new data gathering cost minimization framework for mobile data gathering in wireless sensor networks by considering dynamic wireless link capacity and power control jointly. Our new framework not only allows concurrent data

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	uploading from sensors to the mobile collector, but also determines transmission power under elastic link capacities. We study the problem under constraints of flow conservation, energy consumption, elastic link capacity, transmission compatibility, and Sojourn time. We employ the subgradient iteration algorithm to solve the minimization problem. We first relax the problem with Lagrangian dualization, then decompose the original problem into several subproblems, and present distributed algorithms to derive data rate, link flow and routing, power control, and transmission compatibility. For the mobile collector, we also propose a sub-algorithm to determine sojourn time at different stopping locations. Finally, we provide extensive simulation results to demonstrate the convergence and robustness of proposed algorithms. The results reveal 20 percent shorter data collection latency on average with lower energy consumptions compared to previous works as well as lower data gathering cost and robustness in case of node failures.
NXT21NS2	**TITLE: Dictionary Based Secure Provenance Compression for Wireless Sensor Networks** **ABSTRACT:** Due to energy and bandwidth limitations of wireless sensor networks (WSNs), it is crucial that data provenance for these networks be as compact as possible. Even if lossy compression techniques are used for encoding provenance information, the size of the provenance increases with the number of nodes traversed by the network packets. To address such issues, we propose a dictionary based provenance scheme. In our approach, each sensor node in the network stores a packet path dictionary. With the support of this dictionary, a path index instead of the path itself is enclosed with each packet. Since the packet path index is a code word of a dictionary, its size is independent of the number of nodes present in the packet's path. Furthermore, as our scheme binds the packet and its provenance through an AM-FM sketch and uses a secure packet sequence number generation

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	technique, it can defend against most of the known provenance attacks. Through simulation and experimental results, we show that our scheme outperforms other compact provenance schemes with respect to provenance size, robustness, and energy consumption.
NXT22NS2	**TITLE: Distributed Emergency Guiding with Evacuation Time Optimization Based on Wireless Sensor Networks** **ABSTRACT:** This paper proposes a load-balancing framework for distributed emergency guiding based on wireless sensor networks. A load-balancing guiding scheme is designed and an analytical model is derived to reduce the total evacuation time of people indoors. The guiding scheme can provide the fastest path for people to reach an exit according to the evacuation time estimated using the analytical model. Based on thorough research, this is the first distributed solution in which corridor capacity and length, exit capacity, and the concurrent movement and distribution of people are considered in estimating the evacuation time and planning escape paths. Using the proposed framework, congestion in corridors and at exits can be eased to substantially reduce the total evacuation time. Analytical and simulation results show that this approach outperforms existing schemes and can prevent people from following localoptimal guiding directions that increase the evacuation time. A prototype called the Load-balancing Emergency Guiding System (LEGS) is implemented; this system can be used to compare the evacuation times and guiding directions provided by existing schemes and the proposed scheme for various distributions of people.
NXT23NS2	**TITLE: Duplicate Detectable Opportunistic Forwarding in Duty-Cycled Wireless Sensor Networks** **ABSTRACT:** Opportunistic routing, offering relatively efficient and adaptive forwarding in low-duty-cycled sensor networks, generally allows multiple nodes to forward the same packet simultaneously, especially in networks with

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	intensive traffic. Uncoordinated transmissions often incur a number of duplicate packets, which are further forwarded in the network, occupy the limited network resource, and hinder the packet delivery performance. Existing solutions to this issue, e.g., overhearing or coordination based approaches, either cannot scale up with the system size, or suffer high control overhead. We present Duplicate-Detectable Opportunistic Forwarding (DOF), a duplicate-free opportunistic forwarding protocol for low-duty-cycled wireless sensor networks. DOF enables senders to obtain the information of all potential forwarders via a slotted acknowledgment scheme, so the data packets can be sent to the deterministic next-hop forwarder. Based on light-weight coordination, DOF explores the opportunities as many as possible and removes duplicate packets from the forwarding process. We implement DOF and evaluate its performance on an indoor testbed with 20 TelosB nodes. The experimental results show that DOF reduces the average duplicate ratio by 90%, compared to state-of-the-art opportunistic protocols, and achieves 61.5% enhancement in network yield and 51.4% saving in energy consumption.
NXT24NS2	**TITLE: Fair Routing for Overlapped Cooperative Heterogeneous Wireless Sensor Networks** **ABSTRACT: I**n recent years, as wireless sensor networks (WSNs) are widely diffused, multiple overlapping WSNs constructed on the same area become more common. In such a situation, their lifetime is expected to be extended by cooperative packet forwarding. Although some researchers have studied about cooperation in multiple WSNs, most of them do not consider the heterogeneity in the characteristics of each WSN such as battery capacity, operation start time, the number of nodes, nodes locations, energy consumption, packet size and/or data transmission timing, and so on. In a heterogeneous environment, naive lifetime improvement with cooperation may not be fair. In this paper, we propose a fair cooperative routing method for heterogeneous overlapped

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	WSNs. It introduces an energy pool to maintain the total amount of energy consumption by cooperative forwarding. The energy pool plays a role of broker for fair cooperation. Finally, simulation results show the excellent performance of the proposed method.
NXT25NS2	**TITLE: Geographic and Opportunistic Routing for Underwater Sensor Networks** **ABSTRACT:** Underwater wireless sensor networks (UWSNs) have been showed as a promising technology to monitor and explore the oceans in lieu of traditional undersea wireline instruments. Nevertheless, the data gathering of UWSNs is still severely limited because of the acoustic channel communication characteristics. One way to improve the data collection in UWSNs is through the design of routing protocols considering the unique characteristics of the underwater acoustic communication and the highly dynamic network topology. In this paper, we propose the GEDAR routing protocol for UWSNs. GEDAR is an anycast, geographic and opportunistic routing protocol that routes data packets from sensor nodes to multiple sonobuoys (sinks) at the sea's surface. When the node is in a communication void region, GEDAR switches to the recovery mode procedure which is based on topology control through the depth adjustment of the void nodes, instead of the traditional approaches using control messages to discover and maintain routing paths along void regions. Simulation results show that GEDAR significantly improves the network performance when compared with the baseline solutions, even in hard and difficult mobile scenarios of very sparse and very dense networks and for high network traffic loads.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	MANETS
NXT26NS2	**TITLE: Mitigating Denial Of Service Attacks In Olsr Protocol Using Fictitious Nodes** **ABSTRACT:** With The Main Focus Of Research In Routing Protocols For Mobile Ad-Hoc Networks (Manet) Geared Towards Routing Efficiency, The Resulting Protocols Tend To Be Vulnerable To Various Attacks. Over The Years, Emphasis Has Also Been Placed On Improving The Security Of These Networks. Different Solutions Have Been Proposed For Different Types Of Attacks, However, These Solutions Often Compromise Routing Efficiency Or Network Overload. One Major Dos Attack Against The Optimized Link State Routing Protocol (Olsr) Known As The Node Isolation Attack Occurs When Topological Knowledge Of The Network Is Exploited By An Attacker Who Is Able To Isolate The Victim From The Rest Of The Network And Subsequently Deny Communication Services To The Victim. In This Paper, We Suggest A Novel Solution To Defend The Olsr Protocol From Node Isolation Attack By Employing The Same Tactics Used By The Attack Itself. Through Extensive Experimentation, We Demonstrate That 1) The Proposed Protection Prevents More Than 95 Percent Of Attacks, And 2) The Overhead Required Drastically Decreases As The Network Size Increases Until It Is Non-Discernable. Last, We Suggest That This Type Of Solution Can Be Extended To Other Similar Dos Attacks On Olsr.
NXT27NS2	**TITLE: Trust Management using Probabilistic Energy-Aware Monitoring for Intrusion Detection in Mobile Ad-Hoc Networks** **ABSTRACT:** The security is a key aspect in Mobile Ad-hoc Networks (MANETs), because the communication between the nodes is obtained using the wireless transmission, and the network setup is done without an infrastructure. In this scenario it is possible to perform internal and external attacks compromising the network functions. Moreover, the adoption of Intrusion Detection System (IDS) to discover internal attacks is often energy consuming highly reducing the

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	network lifetime. At this purpose, our proposal is the design and adoption of an energy-aware probabilistic monitoring module useful to IDS, to better perform in a MANET scenario where not only security but also energy constraints need to be accounted. The proposed scheme has been analyzed by an energy point of view and considering also its efficacy to discover malicious nodes under different network conditions.
NXT28NS2	**TITLE: Secure and Energy Efficient MANET Routing Incorporating Trust Values using Hybrid ACO** **ABSTRACT:** Routing in a MANET varies considerably from the other networks due to the fact that MANET, being an ad-hoc network does not follow a specific topology and the nodes are dynamic. Further, power consumption is another major aspect, which needs to be kept in check, as the depleted nodes tend to become selfish. This paper presents a Hybrid Ant Colony Optimization based routing algorithm that generates routes dynamically, following the concept of equal load distribution in the network. The local search component of ACO is modified using Simulated Annealing to provide an effective and energy efficient node selection mechanism. Experiments show that the algorithm exhibits effective load distributions and also provides dynamic random paths.
NXT29NS2	**TITLE: Fuzzy-Based Trust Model for Detection of Selfish Nodes in MANETs** **ABSTRACT:** Cooperation among nodes is mandatory for smooth operation of Mobile Ad Hoc Networks (MANETs) in terms of data routing. A participating node may refuse to deplete its resources for the benefit of others because of not getting any direct advantage for its service. Nodes showing such behavior are called selfish or non-cooperative nodes. Non-cooperative nodes can severely affect the performance of MANETs. Non-cooperative behavior of nodes in the MANETs may lead to network partitioning. In this paper, we address the issue of non-cooperative behavior by incorporating the concept of fuzzy logic closely coupled with the concept of trust. Fuzzy-based analyzer is

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	used to distinguish between the non-cooperative behavior nodes and trustworthy nodes. We propose a fuzzy-based scheme to detect and isolate non-cooperative nodes in MANETs. In the proposed scheme, every node in the network constantly monitors its one-hop neighbors for their actions. Every node computes the trust of the observed neighbors. These trust values are passed on to a fuzzy function which is mapped into different classes. The resulting classes show the trust levels of the observed nodes. On the basis of the calculated trust value, the non-cooperative nodes are detected and isolated from the active routes of the MANET. Proposed fuzzy-based scheme is robust enough in terms of detecting packet drop attack in the network. Results show that proposed scheme detects non-cooperative nodes effectively with low false positives rate. Moreover, proposed scheme increases the packet delivery ratio and throughput in the presence of non-cooperative nodes in the network.
NXT30NS2	**TITLE: A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks** **ABSTRACT:** Mobile Ad hoc Networks (MANET) are selfconfiguring, infrastructureless, dynamic wireless networks in which the nodes are resource constrained. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the otherwise vulnerable network. In this paper, we present efficient schemes for analyzing and optimizing the time duration for which the intrusion detection systems need to remain active in a mobile ad hoc network. A probabilistic model is proposed that makes use of cooperation between IDSs among neighborhood nodes to reduce their individual active time. Usually, an IDS has to run all the time on every node to oversee the network behavior. This can turn out to be a costly overhead for a battery-powered mobile device in terms of power and computational resources. Hence, in this work our aim is to reduce the duration of active time

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	of the IDSs without compromising on their effectiveness. To validate our proposed approach, we model the interactions between IDSs as a multi-player cooperative game in which the players have partially cooperative and partially conflicting goals. We theoretically analyze this game and support it with simulation results.
NXT31NS2	**TITLE: D2D: Delay-Aware Distributed Dynamic Adaptation of Contention Window in Wireless Networks** **ABSTRACT:** The IEEE 802.11e enhanced distributed channel access (EDCA) protocol follows class-based service differentiation for providing differentiated quality-of-service (QoS). However, its collision avoidance mechanism using backoff algorithm can be inefficient for providing improved performance with respect to throughput and channel access delay, especially in a high network configuration (i.e. number of stations) with imperfect wireless channel. The existing and emerging works have devoted considerable attention on tuning the backoff parameters for achieving optimal throughput only. The prior works do not consider the channel access delay and throughput metrics altogether for performance improvement. Additionally, in most of the cases, the optimal configuration of backoff parameters are performed by a centralized controller. In this paper, we propose a delay-aware distributed dynamic adaptation of contention window scheme, namely D2D, for the cumulative improvement of both the throughput and the channel access delay at runtime. The D2D scheme requires two ad-hoc, distributed, and easy-to-obtain estimates-delay deviation ratio and channel busyness ratio-of the present delay level and channel congestion status of the network, respectively. A key advantage of the D2D scheme is that it is compliant with the IEEE 802.11 standard, and, thus, can be seamlessly integrable with the existing wireless card. We show the integrated model of the medium access control protocol, namely D2D Channel Access (D2DCA), for the IEEE 802.11e networks. We further propose a two-

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	dimensional Markov chain model of the D2DCA protocol for analyzing.
NXT32NS2	**TITLE: Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks** **ABSTRACT:** Delay Tolerant Network (DTN) is developed to cope with intermittent connectivity and long delay in wireless networks. Due to the limited connectivity, DTN is vulnerable to blackhole and greyhole attacks in which malicious nodes intentionally drop all or part of the received messages. Although existing proposals could accurately detect the attack launched by individuals, they fail to tackle the case that malicious nodes cooperate with each other to cheat the defense system. In this paper, we suggest a scheme called Statistical-based Detection of Blackhole and Greyhole attackers (SDBG) to address both individual and collusion attacks. Nodes are required to exchange their encounter record histories, based on which other nodes can evaluate their forwarding behaviors. To detect the individual misbehavior, we define forwarding ratio metrics that can distinguish the behavious of attackers from normal nodes. Malicious nodes might avoid being detected by colluding to manipulate their forwarding ratio metrics. To continuously drop messages and promote the metrics at the same time, attackers need to create fake encounter records frequently and with high forged numbers of sent messages. We exploit the abnormal pattern of appearance frequency and number of sent messages in fake encounters to design a robust algorithm to detect colluding attackers. Extensive simulation shows that our solution can work with various dropping probabilities and different number of attackers per collusion at high accuracy and low false positive.
NXT33NS2	**TITLE: Distance-Based Location Management Utilizing Initial Position for Mobile Communication Networks** **ABSTRACT:** This paper aims at improving the distance-based location management scheme for mobile communication networks. In location

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	management, a mobile terminal (MT) is tracked based on its location-update area (LA). The improvement is brought about by joint optimization of LA center and LA size. For LA center optimization (LCO), we determine the optimal center position of the LA given the initial position of the MT upon each location update. The investigation of optimal LA center has eluded research to date. Based on the popular continuous-time random walk (CTRW) mobility model, we propose an analytical framework that uses a diffusion equation to determine the optimal LA center that minimizes the total cost of location management, consisting of the location update cost and terminal paging cost. This framework allows us to easily model the non-Markovian movement of the MT and evaluate the impact of various measurable physical parameters (such as length of road section, angle between road sections, and road section crossing time) and LA center. In particular, we show that proper LA center can significantly reduce the total cost. For example, for the circular LA and low Poisson call-arrival rate, optimizing the LA center alone has the potential of reducing the cost by up to 37 percent. Joint optimization of the LA center and terminal paging scheme can reduce the cost even further. Simulations results match the theoretical analysis to a gap within 3 percent, indicating that our theoretical model is very accurate.
NXT34NS2	**TITLE: Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs** **ABSTRACT:** In mobile ad hoc networks (MANETs), it is effective to retrieve data items using top-k query. However, accurate results may not be acquired in environments when malicious nodes are present. In this paper, we assume that malicious nodes attempt to replace necessary data items with unnecessary ones (we call these data replacement attacks), and propose methods for top-k query processing and malicious node identification based on node grouping in MANETs. In order to maintain the accuracy of the query result, nodes reply

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	with k data items with the highest score along multiple routes, and the query-issuing node tries to detect attacks from the information attached to the reply messages. After detecting attacks, the query-issuing node tries to identify the malicious nodes through message exchanges with other nodes. When multiple malicious nodes are present, the query-issuing node may not be able to identify all malicious nodes at a single query. It is effective for a node to share information about the identified malicious nodes with other nodes. In our method, each node divides all nodes into groups by using the similarity of the information about the identified malicious nodes. Then, it identifies malicious nodes based on the information on the groups. We conduct simulation experiments by using a network simulator, QualNet5.2, to verify that our method achieves high accuracy of the query result and identifies malicious nodes.
NXT35NS2	**TITLE: Resisting Blackhole Attacks on MANETs** **ABSTRACT:** MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the routing protocol. AODV is a reactive MANET routing protocol that is vulnerable to a dramatic collapse of network performance in the presence of blackhole attack. The paper introduces a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal protocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior. We present a Blackhole Resisting Mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol. It does not require expensive cryptography or authentication mechanisms, but relies on locally applied timers and thresholds to classify nodes as malicious. No modifications to the packet formats are needed, so the overhead is a small amount of calculation at nodes, and no extra communication. Using NS2 simulation, we compare the performance of

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	networks using AODV under blackhole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a blackhole attack.
NXT36NS2	**TITLE: Impact of trust-based security association and mobility on the delay metric in MANET** **ABSTRACT:** Trust models in the literature of MANETs commonly assume that packets have different security requirements. Before a node forwards a packet, if the recipient's trust level does not meet the packet's requirement level, then the recipient must perform certain security association procedures, such as re-authentication. We present in this paper an analysis of the epidemic broadcast delay in such context. The network, mobility and trust models presented in this paper are quite generic and allow us to obtain the delay component induced only by the security associations along a path. Numerical results obtained by simulations also confirm the accuracy of the analysis. In particular, we can observe from both simulation's and analysis results that, for large and sparsely connected networks, the delay caused by security associations is very small compared to the total delay of a packet. This also means that parameters like network density and nodes' velocity, rather than any trust model parameter, have more impact on the overall delay.

Nxtlogic
SOFTWARE SOLUTIONS
We inspire the next

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT37NS2	**TITLE: ZigBee Wireless Dynamic Sensor Networks: Feasibility Analysis and Implementation Guide** **ABSTRACT:** The wireless sensor network (WSN) technology has attracted increasing attention considering its potential in many application fields. In most studies on WSNs, the network is assumed to cover several static devices over a fixed coverage area. As an extension of WSN capabilities, the devices mobility and the network dynamism provide a new chain of interesting applications defined as wireless dynamic sensor network (WDSN). The initial challenge in the WDSN is to investigate whether this dynamic imposed on the network will be supported, once the used network protocol must meet the requirements for WDSN applications, such as network formation and self-organization, route discovery and communication management with the input and output of devices on the network. In order to overcome these issues, specific wireless protocols have been developed to meet the applications with device mobility in the WSN. However, these specific protocols limit the development of the WSDN since, they are isolated and proprietary solutions, instead of using a standardized protocol for interoperability. This paper presents a feasibility analysis of the ZigBee protocol for the WDSN applications. A survey of application features and requirements, as well as a discussion of advantages and limitations, regarding the adoption of the ZigBee protocol in the WDSN is presented. An implementation guide for the ZigBee WDSN is proposed in order to assist a new application of this technology. Furthermore, a proof of concept using ZigBee devices validates the implementation guide and proves the ZigBee WDSN feasibility.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT38NS2	**TITLE: Distributed and Adaptive Medium Access Control for Internet-of-Things-Enabled Mobile Networks** **ABSTRACT:** In this paper, we propose a distributed and adaptive hybrid medium access control (DAH-MAC) scheme for a singlehop Internet-of-Things (IoT)-enabled mobile ad hoc network (MANET) supporting voice and data services. A hybrid superframe structure is designed to accommodate packet transmissions from a varying number of mobile nodes generating either delay-sensitive voice traffic or best-effort data traffic. Within each superframe, voice nodes with packets to transmit access the channel in a contention-free period using distributed time division multiple access (TDMA), while data nodes contend for channel access in a contention period using truncated carrier sense multiple access with collision avoidance (T-CSMA/CA). In the contention-free period, by adaptively allocating time slots according to instantaneous voice traffic load, the MAC exploits voice traffic multiplexing to increase the voice capacity. In the contention period, a throughput optimization framework is proposed for the DAH-MAC, which maximizes the aggregate data throughput by adjusting the optimal contention window size according to voice and data traffic load variations. Numerical results show that the proposed MAC scheme outperforms existing QoS-aware MAC schemes for voice and data traffic in the presence of heterogeneous traffic load dynamics.
NXT39NS2	**TITLE: A role-based approach to secure routing in wireless ad-hoc networks** **ABSTRACT:** The paper presents a brief overview of routing protocols in wireless ad-hoc networks. The main focus is on solving security issues. We conclude that the concept of trust is fundamental in the design of secure routing protocols today. Based on SAR (Security-Aware Ad-hoc Routing) protocol, we propose a role-based approach to secure routing. This approach enhances the flexibility and security of information flows in wireless ad-hoc networks. Some algorithmic solutions presented in order to apply this approach in other routing

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	protocols. In the final part, the proposed approach and related algorithms were demonstrated by an example.
NXT40NS2	**TITLE: Secure routing protocols for mobile ad hoc networks** **ABSTRACT:** Mobile Ad hoc NETwork (MANET) is a collection of self-organizing mobile nodes without any help of centralized administration or established infrastructure. Due to this characteristic, MANETs are particularly vulnerable to various security threats. In addition, the design of most MANET routing protocols assumes that there is no malicious node in the network. Hence, several efforts and researches have been made toward the design of a secure and robust routing protocol for ad hoc networks. In this paper, we discuss the major attacks that can target the operation of ad hoc routing protocol. A detailed survey of the well-known secured ad hoc routing protocols for mobile ad hoc networks is presented. In order to analyze the existent solutions for securing ad hoc routing protocols in a structured manner, we have classified them into three categories: solutions based on cryptography, solutions based on one-way hash chain and hybrid solutions. This paper also gives a brief summary and comparison of various protocols available for secured routing in MANET.

Nxtlogic
SOFTWARE SOLUTIONS
We inspire the next

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT41NS2	**TITLE: Securely-entrusted multi-topology routing for community networks** **ABSTRACT:** Routing in open and decentralized networks relies on cooperation despite the participation of unknown nodes and node administrators pursuing heterogeneous trust and security goals. Living use cases for such environments are given by community mesh networks due to their open structure and decentralized management and ownership. However, despite many active work in the field of routing security for mesh and MANET networks, practical solutions enabling a secured but decentralized trust management are still missing, leaving nowadays existing community networks vulnerable to various attacks and seriously challenged by the obligation to find consensus on the trustability of participants within an increasing user size and diversity. This work presents the design, implementation and analysis of a routing protocol that enables cryptographically secured negotiation and establishment of concurrent and individually trusted routing topologies for infrastructure-less networks without relying on any central management. Benchmarking results, based on our initial implementation and tested on real and very cheap (10 Euro, Linux SoC) embedded routers, quantify the scalability of our approach supporting networks with hundreds of nodes and despite being based on supposedly CPU-expensive asymmetric cryptography.

Nxtlogic
SOFTWARE SOLUTIONS
We inspire the next

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT42NS2	**TITLE: Securing Mobile Ad Hoc Networks using distributed firewall with PKI** **ABSTRACT:** The MANETs (Mobile Ad Hoc Networks) are increasing on popularity due to their dynamic nature, minimal infrastructure requirements, deployment cost and their self-configuring attributes. Advances in low power computing and communications and increase of transfer rates makes MANETs even more desired in different real world applications. These properties make them ideal for employment in tactical military and civil rapid-deployment networks, including emergency rescue operations and ad hoc disaster-relief networks. Every MANET node acts as a router, thus expanding communications range and creating even larger network. However, decentralized nature of MANETs makes them susceptible to insider and outsider attacks. In this paper, we define security model for MANETs using PKI (Public Key Infrastructure), Firewall and aspects of IPS (Intrusion Prevention System). Our model denies all communication by default. Nodes can access only other nodes and services they are authorized to. Every node contains same security model, which protects it against routing, network and surveillance attacks. Model helps mitigate and prevent against most common attacks. This approach helps nodes to protect against insider and outsider attackers and allows them to withstand security threats which would otherwise damage or cripple whole network.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT43NS2	**TITLE: Group based analysis of AODV related protocols in MANET** **ABSTRACT:** With an objective of study and analysis of power efficient routing protocols in Mobile Adhoc Network(MANET), this paper presents a report on performance of Adhoc On Demand Distant Vector (AODV) oriented MANET routing protocols which are founded on power aware techniques and also support quality of service parameters and resource reservation strategies. The comparison is based on the type and extent of delay management techniques, Quality of service conditions and resource reservation methods used by these important protocols while minimizing the end to end delay during transmission. Secondly the paper also presents a complete analysis on the mechanism of routing , advantages and scope for further improvement for research in these protocols which will provide sufficient information and scope for further research in this magnificent area of MANET.
NXT44NS2	**TITLE: Simulation comparison and analysis of DSR and DYMO protocols in MANETs** **ABSTRACT:** Ad-hoc network has opened a new dimension in wireless networks. It allows wireless nodes to communicate with each other in the absence of centralized support. It does not follow any fixed infrastructure because of the mobility of nodes and multi-path propagations. Link instability and node mobility make routing a core issue in MANETs. A suitable and effective routing mechanism helps to extend the successful deployment of MANETs. In this paper, we have simulated and analyzed two routing protocols: DSR (Dynamic Source Routing Protocol) and DYMO (Dynamic MANET On-demand Routing). Our simulations were conducted using the OMNET simulation tool. Simulation results showed a better performance of DYMO over DSR in terms of throughput, packet delay, packet dropping, and collision ratio.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT45NS2	**TITLE: QoS Routing for MANET and Satellite Hybrid Network to Support Disaster Relives and Management** **ABSTRACT:** Communication technologies are very important for disaster management. Satellite network's advantage of large coverage and Mobile Ad hoc Network's (MANET) advantage of high flexibility could be ideal for disaster management. In this paper, the authors propose a novel scheme for providing reliable wireless communications in disaster sites with a hybrid network of terrestrial MANET and satellite network. In comparison with normal wireless routing approaches, i.e. AODV and AOMDV, the proposed scheme could achieve higher packet delivery ratio, higher throughput and lower delay; meanwhile it could also balance traffic loads at gateways to maximum satellite links' utilization.
NXT46NS2	**TITLE: Network security risk assessment method based on HMM and attack graph model** **ABSTRACT:** The ever-increasing complexity of computer network and various new types of bugs make the network security become an ever-growing serious challenge. In the evaluation of network security risk, the cause-and-effect relationship between multiple attack steps can be described well in an attack graph model. However, its test result is uncertain. Focused on this issue, the method of fusing attack graph model and Hidden Markov model (HMM) was proposed. Firstly, the network environment and attacker's aggressive behavior were abstracted by the attack graph model; Secondly, the probabilistic mapping that was between network observation and attack status was established by the HMM; Finally, the Viterbi algorithm was used to calculate the maximum probability state transition sequence. Experimental results show that the maximum probability of the state transition sequence can be effectively calculated and then the attack intention can be accurately inferred by this dual model. This method provides a good configuration for network

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	security administrators.
NXT47NS2	**TITLE: Cooperation via Spectrum Sharing for Physical Layer Security in Device-to-Device Communications Underlaying Cellular Networks** **ABSTRACT:** In this paper, we investigate the cooperation issue via spectrum sharing when employing physical layer security concept into the Device-to-Device (D2D) communications underlaying cellular networks. First, we derive the optimal joint power control solutions of the cellular communication links and D2D pairs in terms of the secrecy capacity under a simple cooperation case and further propose a secrecy-based access control scheme with best D2D pair selection mechanism. Then, we consider a more general case that multiple D2D pairs can access the same resource block (RB) and one D2D pair is also permitted to access multiple RBs, and provide a novel cooperation mechanism in the investigated network. Furthermore, we formulate the provided cooperation mechanism among cellular communication links and D2D pairs as a coalitional game. Then, based on a newly defined Max- Coalition order in the constructed game, we further propose a merge-and-split based coalition formation algorithm for cellular communication links and D2D pairs to achieve efficient and effective cooperation, leading to improved system secrecy rate and social welfare. Simulation results indicate the efficiency of the proposed secrecy-based access control scheme and the proposed merge-and-split based coalition formation algorithm.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT48NS2	**TITLE: Physical Layer Security in Heterogeneous Cellular Networks** **ABSTRACT:** The heterogeneous cellular network (HCN) is a promising approach to the deployment of 5G cellular networks. This paper comprehensively studies physical layer security in a multitier HCN where base stations (BSs), authorized users, and eavesdroppers are all randomly located. We first propose an access threshold-based secrecy mobile association policy that associates each user with the BS providing the maximum truncated average received signal power beyond a threshold. Under the proposed policy, we investigate the connection probability and secrecy probability of a randomly located user and provide tractable expressions for the two metrics. Asymptotic analysis reveals that setting a larger access threshold increases the connection probability while decreases the secrecy probability. We further evaluate the network-wide secrecy throughput and the minimum secrecy throughput per user with both connection and secrecy probability constraints. We show that introducing a properly chosen access threshold significantly enhances the secrecy throughput performance of a HCN.
NXT49NS2	**TITLE: Public key cryptography: Feasible for security in modern personal area sensor networks?** **ABSTRACT:** Public key cryptography has been considered too expensive, in terms of resource requirements, for applications within personal area networks and larger wireless sensor networks. Approaches based on public key cryptography for encryption/decryption and key generation respectively have been overlooked as the devices have been considered too low power or resource scarce. In recent times with the explosion of interest in the Internet of Things a range of new devices have been created that are low cost, powerful and could easily be applied within the wireless sensor network/personal area network domain. In this work we create a public key library suite based in selected approached from IEEE 1363 to test two of these new devices and

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	confirm the capabilities of these new devices.
NXT50NS2	**TITLE: Wireless network virtualization for enhancing security: Status, challenges and perspectives** **ABSTRACT:** Virtualization is emerging as an efficient resource utilization method that eliminates dedicated physical devices. Virtualization has been widely used in computer systems such as virtual memory, virtual storage access network and wired networks - and most recently in cloud computing - to enhance the network performance, resource utilization and energy efficiency, and to achieve performance isolation between different parties. Inspired by this, several techniques for network and wireless virtualization have been proposed in the literature in order to improve the network performance and security. In this paper, we provide a comprehensive study of network and wireless virtualization for enhancing overall network security. We also outline current state of the research and future perspectives. With this paper, readers can have a more thorough understanding of wireless virtualization for network security and the research trends in this area.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	VANETS
NXT51NS2	**TITLE: Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETs** **ABSTRACT:** Secure QoS routing algorithms are a fundamental part of wireless networks that aim to provide services with QoS and security guarantees. In vehicular ad hoc networks (VANETs), vehicles perform routing functions, and at the same time act as end-systems thus routing control messages are transmitted unprotected over wireless channels. The QoS of the entire network could be degraded by an attack on the routing process, and manipulation of the routing control messages. In this paper, we propose a novel secure and reliable multi-constrained QoS aware routing algorithm for VANETs. We employ the ant colony optimisation (ACO) technique to compute feasible routes in VANETs subject to multiple QoS constraints determined by the data traffic type. Moreover, we extend the VANET-oriented evolving graph (VoEG) model to perform plausibility checks on the routing control messages exchanged among vehicles. Simulation results show that the QoS can be guaranteed while applying security mechanisms to ensure a reliable and robust routing service.
NXT52NS2	**TITLE: A Graph Coloring Resource Sharing Scheme for Full-Duplex Cellular-VANET Heterogeneous Networks** **ABSTRACT:** Recently, the vehicular ad hoc networks (VANETs) and full-duplex (FD) cellular networks have both attracted much research interest. Considering the trend of integrated networks in the future, in this paper, we focus on the FD cellular-VANET heterogeneous networks, where cellular uplinks, downlinks, and vehicle-to-vehicle (V2V) communication links co-exist and are permitted to reuse the same spectrum resources. This also leads to a more complicated interference scenario. In such a scenario, we for the first time study the joint resource blocks assignment and transmit power allocation problem.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	Specifically, we construct a graph to model the system, and further propose a graph coloring based resource sharing scheme to solve the problem, in order to achieve a relatively good trade-off between the network throughput and the computational complexity. The simulation results demonstrate the efficiency of our proposed algorithm.
NXT53NS2	**TITLE: A Cluster Based Multicast Routing Protocol for Autonomous Unmanned Military Vehicles (AUMVs) Communication in VANET** **ABSTRACT:** Autonomous Unmanned Military Vehicles (AUMVs) became part of numerous military combat operations to meet the challenges of modern warfare techniques and strategies. Hence, there is a need to develop an ad hoc network among AUMVs to perform the military tasks collectively within a war field where infrastructure installation is not possible. Therefore, in this paper a novel AUMVs protocol is proposed to develop a Vehicular Ad Hoc Network (VANET) among unmanned Military Vehicles (MVs). The proposed protocol performs cluster based multicast communication among AUMVs by considering real time and dynamic war field scenario. The AUMVs protocol develops stable clusters and becomes adaptable according to the military environment by using a proposed Priority Based Cluster Head Election Scheme (PCHE) during cluster formation which reduces the network overhead and delay. Additionally, the AUMVs protocol achieves high throughput by combining the multicast approach with a cluster based scheme. The simulation results illustrate that the proposed protocol has achieved the goal of stable and efficient communication among unmanned MVs.
NXT54NS2	**TITLE: A Street-Centric Opportunistic Routing Protocol Based on Link Correlation for Urban VANETs** **ABSTRACT:** In urban vehicular ad hoc networks (VANETs), due to the high mobility and uneven distribution of vehicles, how to select an optimal relaying node in an intra-street and how to determine a street selection at the

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	intersection are two challenging issues in designing an efficient routing protocol in complex urban environments. In this paper, we build a link model with a Wiener process to predict the probability of link availability, which considers the stable and unstable vehicle states according to the behavior of vehicles. We introduce a novel concept called the link correlation which represents the influence of different link combinations in network topology to transmit a packet with less network resource consumption and higher goodput. Based on this concept, we design an opportunistic routing metric called the expected transmission cost over a multi-hop path (ETCoP) implemented with our link model as the selection guidance of a relaying node in intra-streets. This metric can also provide assistance for the next street selection at an intersection. Finally, we propose a street-centric opportunistic routing protocol based on ETCoP for VANETs (SRPE). Simulation results show that our proposed SRPE outperforms the conventional protocols in terms of packet delivery ratio, average end-to-end delay, and network yield.
NXT55NS2	**TITLE: TIBCRPH: Traffic Infrastructure Based Cluster Routing Protocol with Handoff in VANET** **ABSTRACT:** Vehicular Ad Hoc network (VANET), is a hot topic that applying mobile Ad Hoc network (MANET) to ITS in recent years. Special environments and applications cause difficulties to the design of the routing protocols of VANET which can not use the exiting protocols well. Firstly, this paper introduces some concepts of VANET briefly, analyzes and compares some different kinds of existing routing protocols inVANET. Then, basing on the characteristics of the VANET, and utilizing the idea of cluster and handoff, a more efficient protocol is developed in this paper, which is dubbed Traffic Infrastructure Based Cluster Routing Protocol with Handoff (TIBCRPH). Finally, TIBCRPH is compared with other six typical routing protocols on node density and speed respectively by NS2. The results show that TIBCRPH performs better

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	than some traditional routing protocols.
NXT56NS2	**TITLE: A two level privacy preserving pseudonymous authentication protocol for VANET** **ABSTRACT:** Vehicular ad hoc network (VANET) is gaining significant popularity due to their role in improving traffic efficiency and safety. However, communication in VANET needs to be secure as well as authenticated. The vehicles in the VANET not only broadcast traffic messages known as beacons but also broadcast safety critical messages such as electronic emergency brake light (EEBL). Due to the openness of the network, a malicious vehicles can join the network and broadcast bogus messages that could result in accident. On one hand, a vehicle needs to be authenticated while on the other hand, its private data such as location and identity information must be prevented from misuse. In this paper, we propose an efficient pseudonymous authentication protocol with conditional privacy preservation to enhance the security of VANET. Most of the current protocols either utilize pseudonym based approaches with certificate revocation list (CRL) that causes significant communicational and storage overhead or group signature based approaches that are computationally expensive. Another inherent disadvantage is to have full trust on certification authorities, as these entities have complete user profiles. We present a new protocol that only requires honest-but-curious behavior from certification authority. We utilize a mechanism for providing a user with two levels of pseudonyms named as base pseudonym and short time pseudonyms to achieve conditional privacy. However, in case of revocation, there is no need to maintain the revocation list of pseudonyms. The inherent mechanism assures the receiver of the message about the authenticity of the pseudonym. In the end of the paper, we analyze our protocol by giving the communication cost as well as various attack scenarios to show that our approach is efficient and robust.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT57NS2	**TITLE: P2P Computing in Design of VANET Routing Protocol** **ABSTRACT:** The study of peer-to-peer network and vehicle ad hoc network (VANET) are currently two hotspots in distributed computing and mobile communication researching domain. By building up a P2P overlay network on top of VANET's physical infrastructure, we effectively integrated P2P network's advantage on sustaining highly dynamic network into the design of VANET routing protocol. By deploying passiveVANET routing algorithms with innovative P2P routing mechanisms, we propose a new kind of VANETrouting protocol named Peer Computing based Ad hoc On Demand Vector (PAV). A detailed description of the P2P decentralized naming, route discovering, route querying and updating algorithm used in PAV is presented in this paper. The simulation results indicate that PAV has an improved routing performance in comparison with the popularly used AODV protocol.
NXT58NS2	**TITLE: Scalable VANET content routing using hierarchical bloom filters** **ABSTRACT:** In this paper, we discuss scalable content-oriented routing that enables storing, sharing and searching data totally within the VANET. We introduce a proactive content discovery scheme, Hierarchical Bloom-Filter Routing (HBFR), to tackle mobility, large population and rich content challenges of VANETs. HBFR is compared to the popular ICN reactive content discovery scheme in practical VANETscenarios. The results show that HBFR suits non-sharable data services, while reactive ICN inspired content discovery works well with popular sharable data. We suggest a hybrid approach that adaptively utilizes proactive and reactive schemes for time-sensitive data in ICN VANET.
NXT59NS2	**TITLE: Performance evaluation of reactive routing protocols in VANET** **ABSTRACT:** Node movement feature of Vehicular ad hoc network (VANET) closely resembles with that of mobile ad hoc network (MANET) but its high speed mobility and unpredictable movement characteristics are the key

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	contrasting feature from that of MANET. The similarity nature suggests that the prevailing routing protocol of MANET is very much applicable to VANET. However, on the same line, the dissimilarity characteristics result in frequent loss of connectivity. This necessitates upgradation of the existing routing protocols to adapt itself into VANET scenario. The key parameter that needs to be fed into these protocols is a realistic mobility model which contains criterion linked to speed, road intersections, traffic light effect etc. In this paper, we compare performances of reactive routing protocols named Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) and Ad hoc On Demand Multipath Distance Vector (AOMDV) in VANET using different Mobility Models provided in VanetMobiSim framework. The performances are evaluated by varying mobility, number of sources and node speed while packet delivery fraction, end to end delay and normalized routing load are used as performance metrics. The simulations have shown that AOMDV performs comparatively better than DSR and AODV in different mobility models in terms of end to end delay as performance metric.
NXT60NS2	**TITLE: VANET-Challenges in Selection of Vehicular Mobility Model** **ABSTRACT:** Vehicular Adhoc Network (VANET) is wireless communication between vehicle to vehicle and vehicle to roadside infrastructure. The VANET has different challenges if we compare it with MANET. VANEThas traffic, safety and user application based challenges which have some specific design requirements. To evaluate any VANET design, simulator with vehicular mobility model is required. Vehicular mobility model play a significant role in evaluating different challenges. It is found that different models are for different purposes. In fact Proper design with proper model is required for getting better results. A classification is made between different Vehicular mobility model on the basis of type, sub type, interaction level, and evaluation purpose with their examples.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT61NS2	**TITLE: MAZACORNET: Mobility aware zone based ant colony optimization routing for VANET** **ABSTRACT:** Vehicular Ad hoc Networks (VANET) exhibit highly dynamic behavior with high mobility and random network topologies. The performance of Transmission Control Protocols (TCP) in such wireless ad hoc networks is plagued by a number of problems: frequent link failures, scalability, multi-hop data transmission and data loss. In this work, we make use of the vehicle's movement pattern, vehicle density, vehicle velocity and vehicle fading conditions to develop a hybrid, multi-path ant colony based routing algorithm, Mobility Aware Zone based Ant Colony Optimization Routing for VANET(MAZACORNET). that exhibits locality and scalability. We use ACO to find multiple routes between nodes in the network to aid in link failures. To achieve scalability we partition the network into multiple zones. We use proactive approach to find a route within a zone and reactive approach to find routes between zones using the local information stored in each zone thereby trying to reduce broadcasting and congestion. Our proposed algorithm makes effective use of the network bandwidth, is scalable and is robust to link failures. The results show that the algorithm works well for dense networks. The algorithm produces better delivery ratio and is scalable for zones beyond four. When compared to other existing VANET algorithms, the hybrid algorithm proved to be more efficient in terms of packet delivery ratio and end to end delay. To our knowledge this is the first ant based routing algorithm for VANET that uses the concept of zones.
NXT62NS2	**TITLE: AODV routing protocol modification with dqueue(dqAODV) for VANET in city scenarios** **ABSTRACT:** Vehicular ad hoc network (VANET) is considered as a sub-set of mobile ad hoc network (MANET). It provides smart Transport System i.e., wireless ad-hoc communication in between vehicles and vehicle to roadside

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	equipments. Based on this technology road network is classified into two types 1. vehicle to vehicle interaction, 2. vehicle to infrastructure interaction. The objective of VANET is to provide safe, secure and automated traffic system. For this automated traffic technique several types of routing protocols have been developed. But routing protocols of MANET are not directly applicable to VANET. In this study, we proposed a modified AODV routing protocol in the context of VANET with the help of dqueue introduction into the RREQ header in the C++ code of built-in AODV protocol in NCTUns-6.0 simulator. Recently Saha et al [1] has reported the results showing the nature of modified AODV obtained from the rudimentary version of their simulation code. It is mainly based on packed delivery throughput. It shows greater In-throughput information of packet transmission compare to original AODV. It has been observed from the study that our protocols needs less overhead and yield greater performance in compared to conventional AODV.
NXT63NS2	**TITLE: CBQoS-Vanet: Cluster-based artificial bee colony algorithm for QoS routing protocol in VANET** **ABSTRACT:** Recent years have seen a growing interest in Vehicular Ad hoc Networks (VANETs) and their benefits to the development of intelligent transportation systems (ITS). With the deployment of multimedia services over VANETs, there is a need to develop new approaches to insure higher level of quality of services (QoS) for real time applications, and integrate QoS into routing protocols. However, in VANETenvironment, it is not an easy task to search for routes which satisfy the QoS required by the applications. In this paper, we propose CBQoS-Vanet, a new QoS-based unicast routing protocol for vehicular networks. This protocol is based on the use of two techniques: a clustering algorithm which organizes and optimizes the exchange of the routing information based on QoS requirements, and an artificial bee colony algorithm, which finds the best routes from a source to a destination based on QoS

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	criteria. In our approach clusters are formed around cluster-heads that are elected based on QoS consideration. In this paper we consider the following QoS criteria: available bandwidth, end-to-end delay, jitter, and link expiration time. Through simulation experiments, we show that our method can improve greatly the performance of routing in VANET by selecting routes based on the above mentioned QoS criteria.
NXT64NS2	**TITLE: A VANET routing based on the real-time road vehicle density in the city environment** **ABSTRACT:** The intelligent transportation system (ITS) can enhance the driver's safety by providing safety-related information such as traffic conditions and accident information to drivers. The vehicular ad hoc network (VANET) is an essential technology for the deployment of ITS. And, for the reliable delivery of safety-related information to vehicles in the VANET, a reliable VANET routing protocol is required. VANETrouting is challenging since it is fundamentally different from conventional ad hoc networks; the vehicles move fast, and the network topology changes rapidly causing intermittent link connectivity. In this paper, we propose a routing protocol that works based on the real-time road vehicle density in order to provide fast and reliable communications so that it adapts to the dynamic vehicular city environment. In the proposed routing mechanism, each vehicle computes the vehicle density of the road to which it belongs by using beacon messages and the road information table. Based on the real-time road vehicle density information, each vehicle establishes a reliable route for packet delivery. In order to evaluate the performance of the proposed mechanism, we compare our proposed mechanism with GPSR through NS-2 based simulations and show that our mechanism outperforms GPSR in terms of delivery success rate and routing overhead.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT65NS2	**TITLE: Design and Implementation of the Travelling Time- and Energy-Efficient Android GPS Navigation App with the VANET-Based A* Route Planning Algorithm** **ABSTRACT:** This paper has three major contributions. First, a vehicular ad-hoc network (VANET)-based A* (VBA*) route planning algorithm is proposed to calculate the route with the shortest travelling time or the least oil consumption, depending on two real-time traffic information sources. The first one is the recorded traffic information of the road segment that the vehicle has passed through. This traffic information is further exchanged between vehicles when they enter the transmission range of IEEE 802.11p wireless link in the VANET. The second one is the traffic information provided by Google Maps. Then, a GPS navigation app is implemented on the Android platform to realize the VBA* route planning algorithm. Finally, simulations for six route planning algorithms are executed by the well-known VANET simulator, i.e., The ONE. In summary, VBA* achieves significant reductions on both the average travelling time and oil consumption of the planned route, as compared to traditional route planning algorithms.
NXT66NS2	**TITLE: A 3D Web-based visualization tool for VANET simulations** **ABSTRACT:** VANET Simulation schemes require a combination of mobility and wireless network simulation packages, coupled with custom scripts, visualization tools and various scenarios. The results of simulation studies need to be supported by special tools or scripts to analyze or visualize them easily. Some additional difficulties arise at sharing the results, visually comparing simulation runs across different platforms and showcasing the findings of a research to a larger audience. As a solution, we have developed a 3D Web-based Visualization Tool for VANET Simulations (WGL-VANET), which takes advantage of HTML5 and WebGL technologies to create a cross-platform, easy-to-use and flexible visualization tool for VANET simulations. WGL-VANET reads

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	simulation data from a JSON document and supports a variety of visual features, and displays the simulation run on a WebGL canvas inside a web-browser.
NXT67NS2	**TITLE: Scenario Based Performance Analysis of AODV and GPSR Routing Protocols in a VANET** **ABSTRACT:** Vehicular Ad Hoc Network (VANET) is formed by a number of moving vehicles that are equipped with wireless interfaces. It is a kind of Mobile Ad Hoc Network (MANET) in which communication takes place between moving vehicles on the road. VANETs are heterogeneous in nature as they provide wireless communication among moving vehicles (V2V) and vehicle to Road Side Units (RSU). It has become an exciting area of research as it is anticipated to improve Intelligent Transport System (ITS). To exploit effective communication among vehicles, routing is the key factor which needs to be investigated. This paper intends to analyze the performance of AODV and GPSR routing protocols in aVANET in various scenarios under different traffic conditions with respect to Packet Delivery Ratio (PDR) and average End-to-End Delay (E2ED). Simulation is performed using NS-2.35 in combination with Vanet MobiSim. It has been found that AODV performs better with respect to PDR and GPSR outperforms AODV with respect to E2ED. Also, the performance of both the routing protocols varies from one scenario to another and traffic types. The performance of both AODV and GPSR is improved by using IEEE 802.11p instead of IEEE 802.11.
NXT68NS2	**TITLE: Extended mobility management and routing protocols for internet-to-VANET multicasting** **ABSTRACT:** Emerging ITS applications such as fleet management and point of interest distribution require vehicles to have Internet access. However, allowing vehicles to access to the Internet is particularly challenging due to the

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	special characteristics of the vehicular environment. So far, multicasting approaches have been demonstrated to be effective for supporting group communication in traditional networks. However, such Internet-to-VANET multicast service involves several challenges including efficient multicast mobility management and multicast message delivery. This paper proposes a scheme that combines the existing multicast mobility management scheme with vehicular networking solutions to achieve Internet-to-VANET multicasting. The proposed scheme aims to: (i) provide multicast mobility management with low control overhead and efficient bandwidth utilization, as well as (ii) extend the service coverage provided by VANET membership management and multicast message delivery protocol. Simulation results indicate that our Motion-MAODV scheme improves the performance of both MAODV and traditional flooding dissemination schemes in terms of both packet delivery ratio and end-to-end transmission latency.
NXT69NS2	**TITLE: Geographical information extension for IPv6: Application to VANET** **ABSTRACT:** The availability of efficient location system receivers, numerous calculation techniques of the relative coordinates and the need to design an efficient and a scalable network are the main reasons for geographical information usage in vehicular networks (VANET). IPv6 is considered as the most appropriate technologies to support communication in VANET thanks to its extended address space, enhanced mobility support, ease of configuration and embedded security. Although, in the context ofVANET, the knowledge of the actual geographical location becomes crucial, this information is still lacking in IPv6. Thus, the main challenge is to integrate the geographical location into the current design of IP mechanism. Few studies have dealt with geographical addressing in IPv6 for VANET. In this paper, we study and analyze some possibilities to enrich IPv6 with geographical information.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT70NS2	**TITLE: Secure architecture dedicated for VANET alarm messages authentication through semantic verification** **ABSTRACT:** Vehicle communications are becoming increasingly popular, propelled by navigation safety requirements and by the investments of car manufacturers and Public Transport Authorities. Efforts and research have been performed to secure VANET communications. However, most of the solutions are based on cryptographic computation which is considerably slower and consumes extra energy and may also not satisfy the real-time requirement, without introducing trust in VANET. This gives rise to the need for new solutions aiming at network protection. This article presents a new architecture based on the verification of the alert message content and its semantics by deploying a new reputation system. For this aim, we included a new scheme of valorizing trust for each vehicle into the cryptographic algorithm based on PKI method. A part of simulation was done with the AVISPA web tool.
NXT71NS2	**TITLE: Acoustic noise pollution monitoring in an urban environment using a VANET network** **ABSTRACT:** The main objective of this work is the development of a Vehicle Ad Hoc NETwork (VANET) to collect data from GPS equipped mobile phones used as noise detectors. In this system, sensor nodes perioadically transmit acoustic noise levels to neighboring cars, data packets being shared and temporary stored by participating VANET nodes and ultimately forwarded to a collector node connected to the Internet, providing public real-time data. A routing technique called MP-OLSR that takes into account the spatially separation between the multiple paths is used, for better transmission reliability and congestion avoidance as well as for control message overhead minimization.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT72NS2	**TITLE: VANET Security Framework for Trusted Grouping Using TPM Hardware** **ABSTRACT:** Vehicular Ad hoc Network (VANET) is a network of vehicles on the roads, of which the success of its applications is highly dependent upon the underlying security mechanism. The default trial asymmetric PKI/ECDSA security mechanism is known for its high computational cost, thus lacking applicability in life-critical safety messaging. Alternative security schemes, such as symmetric methods provide faster communication at the expense of reduced security. Hence, hybrid and hardware based solutions were proposed by researchers to ease the issue. However, these solutions either do not support the existingVANET PKI standard or have larger message size. In this paper, we present a hardware based security framework that uses both standard asymmetric PKI and symmetric cryptography for faster and secure safety message exchange. The proposed framework is expected to improve security mechanism in VANET by developing trust relationship among the neighboring nodes, hence forming trusted groups. The trust is established via Trusted Platform Module (TPM) and group communication.
NXT73NS2	**TITLE: NetLogo Based Model for VANET Behaviors Dynamic Research** **ABSTRACT:** The meanings and contents of the vehicular networks simulation research are addressed. By the discussion of self-organization characteristics and the interaction between a large numbers of self-organizing vehicles, a new vehicle mobility model based on the true scene of the participants is proposed that is P-AOC modeling method. It aims to obtain a more profound comprehension of the complex behavior working mechanism of the vehicle in the VANET environment and be able to faithfully reproduce the real VANET scene. The emergent behavior and sudden existing behaviors of VANETentities are well reflected and this helps for safety driving and warning timely.

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

NXT74NS2	**TITLE: Improvizmg the public key infrastructure to build trust architecture for VANET by using short-time certificate management and Merkle Signature Scheme** **ABSTRACT:** Applications in Vehicular Adhoc NETwork (VANET) require high security for end to end communication especially for sensitive information. It is necessary to restrict the unauthorized users from accessing the VANET services using a trusted infrastructure. In addition, messages exchanged should have minimum authentication delay and communication overhead. In this paper, a novel architecture is proposed for trusted infrastructure using combination of short time certificate and Merkle Signature Scheme. In this architecture, secure VANET communication is achieved using psuedo ID generated by the vehicle and the issue of short certificate by the trusted infrastructure that grants the private public key pairs according to the priority of the messages exchanged. Therefore the message dissemination offers reduced overhead and meets the requirement of VANET communication.
NXT75NS2	**TITLE: Efficient VANET Unicast Routing Using Historical and Real-Time Traffic Information** **ABSTRACT:** In this paper, we propose an intersection graph-based vehicular ad hoc network (VANET) architecture. Using the available electronic MAP and historical traffic statistics from public traffic databases, we create an intersection graph (IG) consisting of all connected road segments, which have shorter average inter-vehicle distances than the wireless transmission range, as its edges and intersections of these road segments as its vertices. We then calculate the least cost routing path in the IG. Hence, the source vehicle leverages the proposed IG and IG bypass routing protocols to greedily forward unicast packets to the destination vehicle via each intermediate intersection on the least cost IG path. Further, we also propose the IG routing path recovery process to handle the broken IG path in real-time. Finally, we execute NS2

No. 273 | Peranaidu Layout | Ram Nagar | Gandhipuram
Coimbatore 641 009 | TamilNadu | India | 0422-4342339
98946 94339 | 99525 28451 info@nxtlogic.com
www.nxtlogic.com | www.nxtproject.com

	simulations to exhibit that the IG and IG bypass routing protocols significantly outperform four well-known VANET ones in terms of the average packet delivery ratio, end-to-end delay and hop count.

TRAINING AND SERVICES

- Training By Corporate Trainers
- Research Environment
- Coding Explanation
- Will Provide Full Source Code Of The Project
- Full Documentation And Diagrams (Min 80 Pages)
- Some Of Q&A Based On Final Viva
- Journal Publications / Conference Publications
- Study Materials & Certification
- Printing & Binding.
- Aptitude and Soft Skill Training.
- 100% Placement Assistance.
- Full Time/Part Time Job Assistance During Your Project
- Own Project Idea Also Welcome