# IEEE 2016 PROJECTS TITLES

## S3 Technologies

**43, North Masi Street, Simmakkal**

**Madurai- 625009.**

**Deliverable:**

- Source code
- Review Documents
- Review PPT
- How to run video demo
- Online support for execution via Remote support software

**Own Project concept / Paper implementation is done.**

**Technology Served:**

- Java/J2EE
- Hadoop/ Big data
- Dotnet
- NS2
- NS3

# JAVA TITLES

| S.No | Title | Domain |
|---|---|---|
| 1 | Efficient R-Tree Based Indexing Scheme for Server-Centric Cloud Storage System | Data Mining, June 2016 |
| 2 | Probabilistic Static Load-Balancing of Parallel Mining of Frequent Sequences | Data Mining, May 2016 |
| 3 | RSkNN: kNN Search on Road Networks by Incorporating Social Influence | Data Mining, June 2016 |
| 4 | Exploit Every Bit: Effective Caching for High-Dimensional Nearest Neighbor Search | Data Mining, May 2016 |
| 5 | Efficient and Exact Local Search for Random Walk Based Top-K Proximity Query in Large Graphs | Data Mining, May 2016 |
| 6 | Enabling Fine-Grained Multi-Keyword Search Supporting Classified Sub-Dictionaries over Encrypted Cloud Data | Dependable and Secure Computing, May-Jun 2016 |
| 7 | Group Key Agreement with Local Connectivity | Dependable and Secure Computing, May-Jun 2016 |
| 8 | PROVEST: Provenance-based Trust Model for Delay Tolerant Networks | Dependable and Secure Computing, Pre-print 2016 |
| 9 | GeTrust: A guarantee-based trust model in Chord-based P2P networks | Dependable and Secure Computing, Pre-print |

| | | |
|---|---|---|
| | | 2016 |
| 10 | Shared Relay Assignment (SRA) for Many-to-One Traffic in Cooperative Networks | Mobile Computing, June 2016 |
| 11 | Optimizing Video Request Routing in Mobile Networks with Built-in Content Caching | Mobile Computing, July 2016 |
| 12 | E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks | System Journal, Jun 2016 |
| 13 | Distributed Resource Management for Cognitive Ad Hoc Networks With Cooperative Relays | Networking, June 2016 |
| 14 | EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data | IOT, Apr 2016 |
| 15 | Optimizing Cloud-Based Video Crowdsensing | IOT Journal, June 2016 |
| 16 | BLITHE: Behavior Rule Based Insider Threat Detection for Smart Grid | IOT Journal, April 2016 |
| 17 | Privacy-Preserving Ride Sharing Scheme for Autonomous Vehicles in Big Data Era | IOT Journal, Preprint 2016 |
| 18 | Robust Relay Selection for Large-Scale Energy-Harvesting IoT Networks | IOT Journal, Preprint 2016 |
| 19 | A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks | IOT Journal, Preprint 2016 |
| 20 | Security, Privacy & Incentive Provision for Mobile Crowd Sensing Systems | IOT Journal, Preprint 2016 |
| 21 | Reversible Data Hiding in Encrypted Images With | Circuits and Systems for |

| | Distributed Source Encoding | Video Tech, Apr 2016 |
|---|---|---|

# HADOOP TITLES

| S.No | Title | Domain |
|---|---|---|
| 1 | FiDoop: Parallel Mining of Frequent Itemsets Using MapReduce | Systems, Man, And Cybernetics, Mar 2016 |
| 2 | Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowdsourcing | IOT, preprint 2016 |
| 3 | A Privacy-Preserving Data Sharing Framework for Smart Grid | IOT, preprint May 2016 |

S3 Technologies www.ieeeprojectsmadurai.com 9789339435/9500580008

finalyearprojects@s3techindia.com

# NS2 TITLES

| S.No | Title | Domain |
|---|---|---|
| 1 | 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET | Vehicular Technology, Feb 2016 |
| 2 | Shared Relay Assignment (SRA) for Many-to-One Traffic in Cooperative Networks | Mobile Computing, June 2016 |
| 3 | Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes | Mobile Computing, Jan 2016 |
| 4 | Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks | Mobile Computing, May 2016 |
| 5 | Energy and Memory Efficient Clone Detection in Wireless Sensor Networks | Mobile Computing, May 2016 |
| 6 | E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks | System Journal, Jun 2016 |
| 7 | Cloud-Assisted Data Fusion and Sensor Selection for Internet-of-Things | IOT Journal, Jun 2015 |
| 8 | RMER: Reliable and Energy-efficient Data Collection for Large-scale Wireless Sensor Networks | IOT, preprint 2016 |
| 9 | A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks | IOT, preprint 2016 |
| 10 | PROVEST: Provenance-based Trust Model for Delay Tolerant Networks | Dependable and Secure computing, Preprint 2016 |

| | | |
|---|---|---|
| 11 | GeTrust: A guarantee-based trust model in Chord-based P2P networks | Dependable and Secure Computing, Pre-print 2016 |
| 12 | A Provably Secure, Efficient and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks | Wireless communications, Jan 2016 |
| 13 | Dictionary Based Secure Provenance Compression for Wireless Sensor Networks | Parallel and distributed systems, Jan 2016 |
| 14 | ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks | Information Forensics and Security, Sep 2016 |

# JAVA TITLES WITH ABSTRACT

| S.No | Title | Domain |
|---|---|---|
| 1 | **Efficient R-Tree Based Indexing Scheme for Server-Centric Cloud Storage System**<br><br>Cloud storage system poses new challenges to the community to support efficient concurrent querying tasks for various data-intensive applications, where indices always hold important positions. A practical method to construct a two-layer indexing scheme for multi-dimensional data in diverse server-centric cloud storage system is proposed. RT-HCN, an indexing scheme integrating R-tree based indexing structure and HCN-based routing protocol is proposed. RT-HCN organizes storage and compute nodes into an HCN overlay, one of the newly proposed sever-centric data center topologies. Based on the properties of HCN, we design a specific index mapping technique to maintain layered global indices and corresponding query processing algorithms to support efficient query tasks. | **Data Mining, June 2016** |
| 2 | **Probabilistic Static Load-Balancing of Parallel Mining of Frequent Sequences**<br><br>Frequent sequence mining is well known and well studied problem in datamining. The output of the algorithm is used in many other areas like bioinformatics, chemistry, and market basket analysis. Unfortunately, the frequent sequence mining is computationally quite expensive. A novel parallel algorithm for mining of frequent sequences based on a static load-balancing. The static load-balancing is done by measuring the computational time | **Data Mining, May 2016** |

| | | |
|---|---|---|
| | using a probabilistic algorithm. For reasonable size of instance, the algorithms achieve speedups. In the experimental evaluation, we show that our method performs significantly better then the current state-of-the-art methods. The presented approach is very universal: it can be used for static load-balancing of other pattern mining algorithms such as itemset/tree/graph mining algorithms. | |
| **3** | **RSkNN: kNN Search on Road Networks by Incorporating Social Influence**<br><br>Although k NN search on a road network finding k nearest objects to a query user, has been extensively studied, existing works neglected the fact that the q 's social information can play an important role in this k NN query. Many real-world applications, such as location-based social networking services, require such a query. A new problem is studied: k NN search on road networks by incorporating social influence (RSkNN). Specifically, the state-of-the-art Independent Cascade (IC) model in social network is applied to define social influence. One critical challenge of the problem is to speed up the computation of the social influence over large road and social networks. To address this challenge, three efficient index-based search algorithms is proposed, i.e., road network-based (RN-based), social network-based (SN-based), and hybrid indexing algorithms. | **Data Mining, June 2016** |
| **4** | **Exploit Every Bit: Effective Caching for High-Dimensional Nearest Neighbor Search**<br><br>High-dimensional k nearest neighbor (kNN) search has a wide range of applications in multimedia information | **Data Mining, May 2016** |

| | | |
|---|---|---|
| | retrieval. Existing disk-based k NN search methods incur significant I/O costs in the candidate refinement phase. Cache compact approximate representations is proposed for data points in main memory in order to reduce the candidate refinement time during k NN search. This problem raises two challenging issues: (i) which is the most effective encoding scheme for data points to support k NN search and (ii) what is the optimal number of bits for encoding a data point. This approach is generic and applicable to exact / approximate k NN search methods. | |
| **5** | **Efficient and Exact Local Search for Random Walk Based Top-K Proximity Query in Large Graphs**<br><br>Top- k proximity query in large graphs is a fundamental problem with a wide range of applications. Various random walk based measures have been proposed to measure the proximity between different nodes. Although these measures are effective, efficiently computing them on large graphs is a challenging task. An efficient and exact local search method is developed, FLoS (Fast Local Search), for top- k proximity query in large graphs. FLoS guarantees the exactness of the solution. Moreover, it can be applied to a variety of commonly used proximity measures. FLoS is based on the no local optimum property of proximity measures. We show that many measures have no local optimum. Utilizing this property, we introduce several operations to manipulate transition probabilities and develop tight lower and upper bounds on the proximity values. The lower and upper bounds monotonically converge to the exact proximity value when | **Data Mining, May 2016** |

| | | |
|---|---|---|
| | more nodes are visited. | |
| **6** | **Enabling Fine-Grained Multi-Keyword Search Supporting Classified Sub-Dictionaries over Encrypted Cloud Data**<br><br>Using cloud computing, individuals can store their data on remote servers and allow data access to public users through the cloud servers. As the outsourced data are likely to contain sensitive privacy information, they are typically encrypted before uploaded to the cloud. This, however, significantly limits the usability of outsourced data due to the difficulty of searching over the encrypted data. This issue handled by developing the fine-grained multi-keyword search schemes over encrypted cloud data. The relevance scores and preference factors upon keywords which enable the precise keyword search and personalized user experience. Second, a practical and very efficient multi-keyword search scheme is developed. The proposed scheme can support complicated logic search the mixed "AND", "OR" and "NO" operations of keywords. Third, further employ the classified sub-dictionaries technique to achieve better efficiency on index building, trapdoor generating and query. | **Dependable and Secure Computing, May-Jun 2016** |
| **7** | **Group Key Agreement with Local Connectivity**<br><br>A group key agreement problem is studied where a user is only aware of his neighbors while the connectivity graph is arbitrary. There is no centralized initialization for users. A group key agreement with these features is very suitable for social networks. Under our setting, we construct two efficient protocols with passive security. We obtain lower bounds on the round complexity for this type | **Dependable and Secure Computing, May-Jun 2016** |

| | | |
|---|---|---|
| | of protocol, which demonstrates that our constructions are round efficient. Finally, we construct an actively secure protocol from a passively secure one. | |
| **8** | **PROVEST: Provenance-based Trust Model for Delay Tolerant Networks**<br><br>Delay tolerant networks (DTNs) are often encountered in military network environments where end-to-end connectivity is not guaranteed due to frequent disconnection or delay. A provenance-based trust framework is proposed, namely PROVEST (PROVEnance-baSed Trust model) that aims to achieve accurate peer-to-peer trust assessment and maximize the delivery of correct messages received by destination nodes while minimizing message delay and communication cost under resource-constrained network environments. Provenance refers to the history of ownership of a valued object or information. The interdependency between trustworthiness of information source and information itself in PROVEST. PROVEST takes a data-driven approach to reduce resource consumption in the presence of selfish or malicious nodes while estimating a node's trust dynamically in response to changes in the environmental and node conditions. | **Dependable and Secure Computing, Pre-print 2016** |
| **9** | **GeTrust: A guarantee-based trust model in Chord-based P2P networks**<br><br>More and more users are attracted by P2P networks characterized by decentralization, autonomy and anonymity. However, users' unconstrained behavior makes it necessary to use a trust model when establishing trust relationships between peers. Most | **Dependable and Secure Computing, Pre-print 2016** |

| | | |
|---|---|---|
| | existing trust models are based on recommendations, which, however, suffer from the shortcomings of slow convergence and high complexity of trust computations, as well as huge overhead of network traffic. Inspired by the establishment of trust relationships in human society, a guarantee-based trust model, GeTrust, is proposed for Chord-based P2P networks. A service peer needs to choose its guarantee peer(s) for the service it is going to provide, and they are both required to pledge reputation mortgages for the service. The request peer makes evaluations on all the candidates of service peer by referring their service reputations and their guarantee peers' reputations, and selects the one with highest evaluation to be its service provider. In order to enhance GeTrust's availability and prevent malicious behavior, incentive mechanism and anonymous reputation management strategy is proposed. | |
| **10** | **Shared Relay Assignment (SRA) for Many-to-One Traffic in Cooperative Networks**<br><br>Relay assignment significantly affects the performance of the cooperative communication, which is an emerging technology for the future mobile system. Previous studies in this area have mostly focused on assigning a dedicated relay to each source-destination pair for one-to-one (121) traffic. However, many-to-one (M21) traffic, which is also common in many situations (for example, several users associate with one access point in a wireless access network such as a WLAN), hasn't been well studied. Shared relay assignment (SRA) problem is studied for M21 traffic. Two new optimization problems are studied: one is to maximize the minimum throughput among all | **Mobile Computing, June 2016** |

| | | |
|---|---|---|
| | the sources (hereafter called M21-SRA-MMT), and the other is to maximize the total throughput over all the sources while maintaining some degree of fairness (hereafter called M21-SRA-MTT). | |
| **11** | **Optimizing Video Request Routing in Mobile Networks with Built-in Content Caching**<br><br>Built-in content caching in mobile core networks can help improve quality of service, reduce operation expenses, simplify inter-network cooperation, and thus is a promising approach for more efficient networking architectures. In addition to the complexity of content placement as revealed in the literature, routing video requests remains a challenging issue. Two problems must be addressed: (i) how to distribute video requests among multiple internal servers (i.e., server selection); and (ii) how to route so-generated video flows (i.e., flow routing). In this work, we jointly formulate these two problems with two traffic-engineering objectives considered, namely, minimizing maximum link utilization and minimizing total link cost. Fast algorithm is developed to solve the problems with provable approximation guarantees. A hop-by-hop routing protocol is proposed, which implements the optimization solutions by generating a set of flow-splitting and routing decisions for each router/caching node. | **Mobile Computing, July 2016** |
| **12** | **E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks**<br><br>Wireless sensor networks (WSNs) are resource constrained. Energy is one of the most important resources in such networks. Therefore, optimal use of energy is necessary. A novel energy-efficient routing protocol for WSNs is proposed. The protocol is reliable in terms of data delivery at the base station (BS). Considered mobility in sensor nodes and in the BS. The proposed protocol is hierarchical and cluster based. Each | **System Journal, Jun 2016** |

| | | |
|---|---|---|
| | cluster consists of one cluster head (CH) node, two deputy CH nodes, and some ordinary sensor nodes. The reclustering time and energy requirements have been minimized by introducing the concept of CH panel. At the initial stage of the protocol, the BS selects a set of probable CH nodes and forms the CH panel. Considering the reliability aspect of the protocol, it puts best effort to ensure a specified throughput level at the BS. Depending on the topology of the network, the data transmission from the CH node to the BS is carried out either directly or in multihop fashion. Moreover, alternate paths are used for data transmission between a CH node and the BS. | |
| **13** | **Distributed Resource Management for Cognitive Ad Hoc Networks With Cooperative Relays**<br><br>It is well known that the data transport capacity of a wireless network can be increased by leveraging the spatial and frequency diversity of the wireless transmission medium. This has motivated the recent surge of research in cooperative and dynamic-spectrum-access (which we also refer to as cognitive spectrum access) networks. Still, as of today, a key open research challenge is to design distributed control strategies to dynamically jointly assign: 1) portions of the spectrum and 2) cooperative relays to different traffic sessions to maximize the resulting network-wide data rate. In this paper, we make a significant contribution in this direction. First, we mathematically formulate the problem of joint spectrum management and relay selection for a set of sessions concurrently utilizing an interference-limited infrastructure-less wireless network. We then study distributed solutions to this (nonlinear and nonconvex) problem. The overall problem is separated into two subproblems: 1) spectrum management through | **Networking, June 2016** |

| | | |
|---|---|---|
| | power allocation with given relay selection strategy; and 2) relay selection for a given spectral profile. Distributed solutions for each of the two subproblems are proposed, which are then analyzed based on notions from variational inequality (VI) theory. | |
| **14** | **EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data**<br><br>With the pervasiveness of smart phones, location-based services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user's location privacy. Spatial range query, a popular LBS providing information about points of interest (POIs) is used within a given distance, an efficient and privacy-preserving location-based query solution is proposed, called EPLQ. Specifically, to achieve privacy-preserving spatial range query, the first predicate-only encryption scheme for inner product range (IPRE), which can be used to detect whether a position is within a given circular area in a privacy-preserving way. To reduce query latency, we further design a privacy-preserving tree index structure in EPLQ. Detailed security analysis confirms the security properties of EPLQ. | **IOT, Apr 2016** |
| **15** | **Optimizing Cloud-Based Video Crowdsensing**<br><br>Wearable and mobile devices are widely used for crowdsensing, as they come with many sensors and are carried everywhere. Among the sensing data, videos annotated with temporal-spatial metadata contain huge amount of information, but consume too much precious storage space. The problem of optimizing cloud-based | **IOT Journal, June 2016** |

| | | |
|---|---|---|
| | video crowdsensing in three steps is studied. First, we study the optimal transcoding problem on wearable and mobile cameras. An algorithm to optimally select the coding parameters is proposed to fit more videos at higher quality on wearable and mobile cameras. Investigate the throughput of different file transfer protocols from wearable and mobile devices to cloud servers. A real-time algorithm is proposed to select the best protocol under diverse network conditions, so as to leverage the intermittent WiFi access. | |
| **16** | **BLITHE: Behavior Rule Based Insider Threat Detection for Smart Grid**<br><br>A behavior rule-based methodology is proposed for insider threat (BLITHE) detection of data monitor devices in smart grid, where the continuity and accuracy of operations are of vital importance. Based on the dc power flow model and state estimation model, three behavior rules are extracted to depict the behavior norms of each device, such that a device (trustee) that is being monitored on its behavior can be easily checked on the deviation from the behavior specification. Specifically, a rule-weight and compliance-distance-based grading strategy is designed, which greatly improves the effectiveness of the traditional grading strategy for evaluation of trustees. The statistical property, i.e., the mathematical expectation of compliance degree of each trustee, is particularly analyzed from both theoretical and practical perspectives, which achieves satisfactory tradeoff between detection accuracy and false alarms to detect more sophisticated and hidden attackers. | **IOT Journal, April 2016** |

| | | |
|---|---|---|
| **17** | **Privacy-Preserving Ride Sharing Scheme for Autonomous Vehicles in Big Data Era**<br><br>Ride sharing can reduce the number of vehicles in the streets by increasing the occupancy of vehicles, which can facilitate traffic and reduce crashes and the number of needed parking slots. Autonomous Vehicles (AVs) can make ride sharing convenient, popular, and also necessary because of the elimination of the driver effort and the expected high cost of the vehicles. However, the organization of ride sharing requires the users to disclose sensitive detailed information not only on the pick-up/drop-off locations but also on the trip time and route. A scheme to organize ride sharing is proposed and address the unique privacy issues. This scheme uses a similarity measurement technique over encrypted data to preserve the privacy of trip data. The ride sharing region is divided into cells and each cell is represented by one bit in a binary vector. Each user should represent trip data as binary vectors and submit the encryptions of the vectors to a server. The server can measure the similarity of the users' trip data and find users who can share rides without knowing the data. | **IOT Journal, Preprint 2016** |
| **18** | **Robust Relay Selection for Large-Scale Energy-Harvesting IoT Networks**<br><br>Relay selection problem is considered in largescale energy-harvesting (EH) networks. It is known that if channel state information (CSI) is available at EH relays, a diversity order equal to the number of relays can be obtained, however at the penalty of a feedback overhead (necessary to obtain accurate CSI) which is not suitable | **IOT Journal, Preprint 2016** |

| | | |
|---|---|---|
| | for energy-limited devices intended e:g: for internet-of-things (IoT) applications. Therefore propose a new EH relay selection scheme which is based on the residual energy at each relay's battery, and on information on the distribution of the channels between relays and the destination. The method thus minimizes both the outage probability and the feedback cost. Where previous work relay selection based on channel distribution information (CDI) consider only small-scale fading distribution, employ a stochastic geometry approach to consider jointly the geometrical distribution (i:e:, large-scale fading) and small-scale fading yielding a simple relay selection criterion that furthermore utilizes only rough information on the relay's location, i:e:, an ordinal number from the destination. | |
| **19** | **A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks**<br><br>Affording secure and efficient big data aggregation methods is very attractive in the field of wireless sensor networks research. In real settings, the wireless sensor networks have been broadly applied, such as target tracking and environment remote monitoring. However, data can be easily compromised by a vast of attacks, such as data interception and data tampering, etc. Mainly focus on data integrity protection, give an identity-based aggregate signature scheme with a designated verifier for wireless sensor networks. According to the advantage of aggregate signatures, our scheme not only can keep data integrity, but also can reduce bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based aggregate signature scheme is | **IOT Journal, Preprint 2016** |

| | | |
|---|---|---|
| | rigorously presented based on the computational Diffie-Hellman assumption in random oracle model. | |
| **20** | **Security, Privacy & Incentive Provision for Mobile Crowd Sensing Systems**<br><br>Recent advances in sensing, computing, and networking have paved the way for the emerging paradigm of Mobile Crowd Sensing (MCS). The openness of such systems and the richness of data MCS users are expected to contribute to them raise significant concerns for their security, privacy preservation and resilience. Prior works addressed different aspects of the problem. But in order to reap the benefits of this new sensing paradigm, we need a holistic solution. That is, a secure and accountable MCS system that preserves user privacy, and enables the provision of incentives to the participants. At the same time, we are after a MCS architecture that is resilient to abusive users and guarantees privacy protection even against multiple misbehaving and intelligent MCS entities (servers). | **IOT Journal, Preprint 2016** |
| **21** | **Reversible Data Hiding in Encrypted Images With Distributed Source Encoding**<br><br>A novel scheme of reversible data hiding in encrypted images using distributed source coding. After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make room for the secret data. The selected bit series is Slepian-Wolf encoded using low-density parity check codes. On the receiver side, the secret bits can be extracted if the image receiver has the embedding key only. In case the receiver | **Circuits and Systems for Video Tech, Apr 2016** |

| | | |
|---|---|---|
| | has the encryption key only, he/she can recover the original image approximately with high quality using an image estimation algorithm. If the receiver has both the embedding and encryption keys, he/she can extract the secret data and perfectly recover the original image using the distributed source decoding. | |

# HADOOP TITLES

| S.No | Title | Domain |
|---|---|---|
| 1 | **FiDoop: Parallel Mining of Frequent Itemsets Using MapReduce**<br><br>Existing parallel mining algorithms for frequent itemsets lack a mechanism that enables automatic parallelization, load balancing, data distribution, and fault tolerance on large clusters. As a solution to this problem, we design a parallel frequent itemsets mining algorithm called FiDoop using the MapReduce programming model. To achieve compressed storage and avoid building conditional pattern bases, FiDoop incorporates the frequent items ultrametric tree, rather than conventional FP trees. In FiDoop, three MapReduce jobs are implemented to complete the mining task. In the crucial third MapReduce job, the mappers independently decompose itemsets, the reducers perform combination operations by constructing small ultrametric trees, and the actual mining of these trees separately. We implement FiDoop on our in-house Hadoop cluster. We show that FiDoop on the cluster is sensitive to data distribution and dimensions, because itemsets with different lengths have different decomposition and construction costs. | **Systems, Man, And Cybernetics, Mar 2016** |
| 2 | **Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowdsourcing**<br><br>The ubiquity of smartphones makes the mobile | **IOT, preprint 2016** |

| | | |
|---|---|---|
| | crowdsourcing possible, where the requester can crowdsource data from the workers by using their sensor-rich mobile devices. However, data collection, data aggregation, and data analysis have become challenging problems for a resource constrained requester when data volume is extremely large, i.e., big data. In particular to data analysis, set operations, including intersection, union, and complementation, exist in most big data analysis for filtering redundant data and preprocessing raw data. Facing challenges in terms of limited computation and storage resources, cloud-assisted approaches may serve as a promising way to tackle big data analysis issue. However, workers may not be willing to participate if the privacy of their sensing data and identity are not well preserved in the untrusted cloud. | |
| **3** | **A Privacy-Preserving Data Sharing Framework for Smart Grid**<br><br>Distributed energy resources, featured with small scale power generation technologies and renewable energy sources, are considered as necessary supplements for smart grid. To ensure that merged resources contribute effectively to the grid, data generated by consumer side should be shared among the energy resources. However, it also introduces challenges of the protection of consumer privacy. To address these difficulties, a new framework is proposed to share data in smart grid by leveraging new advances in homomorphic encryption and proxy re-encryption. Proposed framework allows energy resources to analyze consumer data while ensuring consumer privacy. An additional benefit of our proposed framework is that consumer data is transmitted over the smart grid only once. | **IOT, preprint May 2016** |

# NS2 TITLES

| S.No | Title | Domain |
|---|---|---|
| 1 | **2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET**<br><br>Authentication in a vehicular ad-hoc network (VANET) requires not only secure and efficient authentication with privacy preservation but applicable flexibility to handle complicated transportation circumstances as well. In this paper, we proposed a Two-Factor LIghtweight Privacy-preserving authentication scheme (2FLIP) to enhance the security of VANET communication. 2FLIP employs the decentralized certificate authority (CA) and the biological-password-based two-factor authentication (2FA) to achieve the goals. Based on the decentralized CA, 2FLIP only requires several extremely lightweight hashing processes and a fast message-authentication-code operation for message signing and verification between vehicles. Furthermore, any certificate revocation list (CRL)-related overhead on vehicles is avoided. 2FLIP makes the scheme resilient to denial-of-service attack in both computation and memory, which is caused by either deliberate invading behaviors or jammed traffic scenes. The proposed scheme provides strong privacy preservation that the adversaries can never succeed in tracing any vehicles, even with all RSUs compromised. | **Vehicular Technology, Feb 2016** |
| 2 | **Shared Relay Assignment (SRA) for Many-to-One Traffic in Cooperative Networks**<br><br>Relay assignment significantly affects the performance of the cooperative communication, which is an emerging technology for the future mobile system. Previous studies in this area have mostly focused on assigning a dedicated relay to each source- | **Mobile Computing, June 2016** |

| | | |
|---|---|---|
| | destination pair for one-to-one traffic. However, many-to-one (M21) traffic, which is also common in many situations, hasn't been well studied. This paper addresses the shared relay assignment (SRA) problem for M21 traffic. Optimization problems studied: one is to maximize the minimum throughput among all the sources (hereafter called M21-SRA-MMT), and the other is to maximize the total throughput over all the sources while maintaining some degree of fairness (hereafter called M21-SRA-MTT). As the optimal solutions to the two problems are hard to find, we propose two approximation algorithms whose performance factors are 5.828 and 3, respectively, based on the rounding mechanism. | |
| **3** | **Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes**<br><br>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. A novel solution is proposed to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. | **Mobile Computing, Jan 2016** |
| **4** | **Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks**<br><br>Delay Tolerant Network (DTN) is developed to cope with | **Mobile Computing, May 2016** |

| | | |
|---|---|---|
| | 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. A scheme is proposed 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, forwarding ratio metrics is defined 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. | |
| **5** | **Energy and Memory Efficient Clone Detection in Wireless Sensor Networks**<br><br>An energy-efficient location-aware clone detection protocol is proposed in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. Proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are | **Mobile Computing, May 2016** |

| | | |
|---|---|---|
| | compromised. | |
| **6** | **E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks**<br><br>Wireless sensor networks (WSNs) are resource constrained. Energy is one of the most important resources in such networks. Therefore, optimal use of energy is necessary. A novel energy-efficient routing protocol is proposed for WSNs. The protocol is reliable in terms of data delivery at the base station (BS). We consider mobility in sensor nodes and in the BS. The proposed protocol is hierarchical and cluster based. Each cluster consists of one cluster head (CH) node, two deputy CH nodes, and some ordinary sensor nodes. The reclustering time and energy requirements have been minimized by introducing the concept of CH panel. At the initial stage of the protocol, the BS selects a set of probable CH nodes and forms the CH panel. Considering the reliability aspect of the protocol, it puts best effort to ensure a specified throughput level at the BS. Depending on the topology of the network, the data transmission from the CH node to the BS is carried out either directly or in multihop fashion. | **System Journal, Jun 2016** |
| **7** | **Cloud-Assisted Data Fusion and Sensor Selection for Internet-of-Things**<br><br>The Internet of Things (IoT) is connecting people and smart devices on a scale that was once unimaginable. One major challenge for the IoT is to handle vast amount of sensing data generated from the smart devices that are resource-limited and subject to missing data due to link or node failures. By exploring cloud computing with the IoT, we present a cloud-based solution that takes into account the link quality and spatio-temporal | **IOT Journal, Jun 2015** |

| | | |
|---|---|---|
| | correlation of data to minimize energy consumption by selecting sensors for sampling and relaying data. We propose a multiphase adaptive sensing algorithm with belief propagation (BP) protocol (ASBP), which can provide high data quality and reduce energy consumption by turning on only a small number of nodes in the network. | |
| **8** | **RMER: Reliable and Energy-efficient Data Collection for Large-scale Wireless Sensor Networks**<br><br>A novel event data collection approach named RMER (Reliability and Multi-path Encounter Routing) is proposed for meeting reliability and energy efficiency requirements. The contributions of the RMER approach are the following: (a) Fewer monitor nodes are selected in hotspot areas that are close to the Sink, and more monitor nodes are selected in non-hotspot areas, which can lead to increased network lifetime and event detection reliability. (b) The RMER approach sends data to the Sink by converging multi-path routes of event monitoring nodes into a one-path route to aggregate data. Thus, energy consumption can be greatly reduced, thereby enabling further increased network lifetime. | **IOT, preprint 2016** |
| **9** | **A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks**<br><br>Affording secure and efficient big data aggregation methods is very attractive in the field of wireless sensor networks research. In real settings, the wireless sensor networks have been broadly applied, such as target tracking and environment remote monitoring. However, data can be easily compromised by a vast of attacks, such as data interception and data tampering, etc. In this paper, we mainly focus on data integrity protection, give an identity-based aggregate signature scheme with a designated verifier for wireless sensor networks. According to the advantage of aggregate | **IOT, preprint 2016** |

| | | |
|---|---|---|
| | signatures, our scheme not only can keep data integrity, but also can reduce bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based aggregate signature scheme is rigorously presented based on the computational Diffie-Hellman assumption in random oracle model. | |
| **10** | **PROVEST: Provenance-based Trust Model for Delay Tolerant Networks**<br><br>Delay tolerant networks (DTNs) are often encountered in military network environments where end-to-end connectivity is not guaranteed due to frequent disconnection or delay. This work proposes a provenance-based trust framework, namely PROVEST (PROVEnance-baSed Trust model) that aims to achieve accurate peer-to-peer trust assessment and maximize the delivery of correct messages received by destination nodes while minimizing message delay and communication cost under resource-constrained network environments. Provenance refers to the history of ownership of a valued object or information. We leverage the interdependency between trustworthiness of information source and information itself in PROVEST. PROVEST takes a data-driven approach to reduce resource consumption in the presence of selfish or malicious nodes while estimating a node's trust dynamically in response to changes in the environmental and node conditions. | **Dependable and Secure computing, Preprint 2016** |
| **11** | **GeTrust: A guarantee-based trust model in Chord-based P2P networks**<br><br>More and more users are attracted by P2P networks characterized by decentralization, autonomy and anonymity. However, users' unconstrained behavior makes it necessary to use a trust model when establishing trust relationships between peers. Most existing trust models are based on | **Dependable and Secure Computing, Pre-print 2016** |

| | | |
|---|---|---|
| | recommendations, which, however, suffer from the shortcomings of slow convergence and high complexity of trust computations, as well as huge overhead of network traffic. Inspired by the establishment of trust relationships in human society, a guarantee-based trust model, GeTrust, is proposed for Chord-based P2P networks. A service peer needs to choose its guarantee peer(s) for the service it is going to provide, and they are both required to pledge reputation mortgages for the service. The request peer makes evaluations on all the candidates of service peer by referring their service reputations and their guarantee peers' reputations, and selects the one with highest evaluation to be its service provider. In order to enhance GeTrust's availability and prevent malicious behavior, incentive mechanism and anonymous reputation management strategy is proposed. | |
| **12** | **A Provably Secure, Efficient and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks**<br><br>Smart card-based authentication scheme for heterogeneous ad hoc wireless sensor network. This scheme is very efficient since it employs only hash function and XOR operation. However, we found that Turkanovic et al.'s scheme is vulnerable to impersonation attack with node capture, stolen smart card attack, sensor node spoofing attack, stolen verifier attack, and fails to ensure backward secrecy. We propose an efficient scheme to overcome all those weaknesses. Moreover, an advanced scheme is proposed, which provides perfect forward secrecy without much modification from the first proposed scheme. | **Wireless communications, Jan 2016** |
| **13** | **Dictionary Based Secure Provenance Compression** | **Parallel and distributed** |

| | | |
|---|---|---|
| | **for Wireless Sensor Networks**<br><br>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, scheme binds the packet and its provenance through an AM-FM sketch and uses a secure packet sequence number generation technique, it can defend against most of the known provenance attacks. | **systems, Jan 2016** |
| **14** | **ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks**<br><br>Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. To conquer that challenge, an active detection-based security and trust routing scheme named ActiveTrust is proposed for WSNs. The most important innovation of ActiveTrust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. More importantly, the generation and the distribution of detection routes are given in the ActiveTrust scheme, which can fully use the energy in non-hotspots to create as many detection routes as needed to achieve the desired security and energy efficiency. | **Information Forensics and Security, Sep 2016** |