ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

ELYSIUMPRO

—INSPIRING THE LEADING EDGE TECHNOLOGIES —

FINAL YEAR PROJECTS

NETWORKING 2018 - 2019

TITLES WITH ABSTRACTS

CALL US @

(+91) 9944 7933 98

(+91) 452-439 0702, 439 2702

19 Years of Experience | Automated Services | 24/7 Help Desk Support

Advanced Technologies and tools | Legitimate Members of all Journals

ELYSIUM GROUPS

ELYSIUMPRO

INSPIRING THE LEADING EDGE TECHNOLOGIES

www.elysiumpro.in

#227, Elysium Campus, Church Road, Anna Nagar,
Madurai - 625020, Tamil Nadu, India

CALL US @

+91 9944 7933 98

(+91) 452 439 0702, (+91) 452 439 2702

ELYSIUM GROUPS

EPRO NW - 001	Middlebox-Based Packet-Level Redundancy Elimination over Encrypted Network Traffic

To eliminate redundant transfers over WAN links and improve network efficiency, middleboxes have been deployed at ingress/egress. These middleboxes can operate on individual packets and are application layer protocol transparent. They can identify and remove duplicated byte strings on the fly. However, with the increasing use of HTTPS, current redundancy elimination (RE) solution can no longer work without violating end-to-end privacy. In this paper, we present RE over encrypted traffic (REET), the first middlebox-based system that supports both intra-user and inter-user packet-level RE directly over encrypted traffic. REET realizes this by using a novel protocol with limited overhead and protects end users from honest-but-curious middleboxes. We implement REET and show its performance for both end users and middleboxes using several hundred gigabytes of network traffic traces collected from a large U.S. university.

EPRO NW - 002	Root Cause Analysis of Anomalies of Multitier Services in Public Clouds

Anomalies of multitier services of one tenant running in cloud platform can be caused by the tenant's own components or performance interference from other tenants. If the performance of a multitier service degrades, we need to find out the root causes precisely to recover the service as soon as possible. In this paper, we argue that the cloud providers are in a better position than the tenants to solve this problem, and the solution should be non-intrusive to tenants' services or applications. Based on these two considerations, we propose a solution for cloud providers to help tenants to localize root causes of any anomaly. With the help of our solution, cloud operators can find out root causes of any anomaly no matter the root causes are in the same tenant as the anomaly or from other tenants. Particularly, we elaborate a non-intrusive method to capture the dependency relationships of components, which improves the feasibility. During localization, we exploit measurement data of both application layer and underlay infrastructure, and our two-step localization algorithm also includes a random walk procedure to model anomaly propagation probability. These techniques improve the accuracy of our root causes localization. Our small-scale real-world experiments and large-scale simulation experiments show a 15%-71% improvement in mean average precision compared with the current methods in different scenarios.

EPRO NW - 003	Redundancy-Guaranteed and Receiving-Constrained Disaster Backup in Cloud Data Center Network

Traffic anomaly detection is critical for advanced Internet management. Existing detection algorithms generally convert the high-dimensional data to a long vector, which compromises the detection accuracy due to the loss of spatial information of data. Moreover, they are generally designed based on the separation of normal and anomalous data in a time period, which not only introduces high storage and computation cost but also prevents timely detection of anomalies. Online and accurate traffic anomaly detection is critical but difficult to support. To address the challenge, this paper directly models the monitoring data in each time slot as a 2-D matrix, and detects anomalies in the new time slot based on bilateral principal component analysis (B-PCA). We propose several novel techniques in OnlineBPCA to support quick and accurate anomaly detection in real time, including a novel B-PCA-based anomaly detection principle that jointly considers the variation of both row and column principal directions for more accurate anomaly detection, an approximate algorithm to avoid using iteration procedure to calculate the principal directions in a close-form, and a sequential anomaly algorithm to quickly update principal directions with low computation and storage cost when receiving a new data matrix at a time slot. To the best of our knowledge, this is the first work that exploits 2-D PCA for anomaly detection. We have conducted extensive simulations to compare our OnlineBPCA with the state-of-art anomaly detection algorithms using real traffic traces Abilene and GÈANT.

EPRO NW - 004	Dynamic Radio Resource Slicing for a Two-Tier Heterogeneous Wireless Network

In this paper, a dynamic radio resource slicing framework is developed for a two-tier heterogeneous wireless network (HetNet). Through software-defined networking (SDN)-enabled wireless network func-tion virtualization (NFV), radio spectrum resources of heterogeneous wireless networks are re-managed into different bandwidth slices for different base stations (BSs). This framework facilitates spectrum sharing among heterogeneous BSs and achieves differentiated quality-of-service (QoS) provisioning for data service and machine-to-machine (M2M) service with network load dynamics. To determine the set of optimal bandwidth slicing ratios and optimal BS-device (user) association patterns, a network utility maximization problem is formulated with the consideration of different traffic statistics and QoS requirements, location distribution for end devices, load conditions in each cell, wireless channel conditions and inter-cell interference. For tractability, the optimization problem is transformed to a biconcave maximization problem. An alternative concave search (ACS) algorithm is then designed to solve for a set of partial optimal solutions. Simulation results verify the convergence property and display low complexity of the ACS algorithm. It is demonstrated that the proposed radio resource slicing framework outperforms the two other resource slicing schemes in terms of low communication overhead, high spectrum utilization and high aggregate network utility.

EPRO NW - 005	Toward Privacy-Preserving Symptoms Matching in SDN-Based Mobile Healthcare Social Networks

Mobile healthcare social networks (MHSNs) have arisen as a very promising brandnew healthcare system, which will greatly improve the quality of life. Moreover, with the help of software defined networking (SDN) paradigm, it can enhance the user experience. To achieve personal health information sharing and the access control among parities, a similar symptoms matching process should be executed before that. However, the matching process requires users to exchange symptoms information, conflicting with the ever-increasing privacy concerns on protecting private symptoms from strangers. To realize privacy-preserving symptoms matching, in this paper, we design two blind signature-based symptom matching schemes in SDN-based MHSNs, which can achieve the coarse-grained symptom matching and fine-grained symptom matching, respectively. Moreover, our schemes do not relay on any trusted third party. Security analysis and detailed simulations show that our proposed schemes can realize efficient privacy-preserving symptom matching. Finally, we do comprehensive experimental evaluation on real-world smartphones to demonstrate the practicality of our proposed schemes.

EPRO NW - 006	Secure Group Mobility Support for 6LoWPAN Networks

The Internet Protocol version 6 (IPv6) over low power wireless personal area networks (6LoWPANs) has introduced IP technologies to wireless sensor networks, which significantly promotes the development of the Internet of Things. To support effective mobility management of these resource constrained IP-based sensor nodes, the Proxy Mobile IPv6 has been proposed as a standard to minimize the communication over-head of those nodes. Although the standard has specified some issues of security and mobility in 6LoWPANs, the issues of supporting secure group handovers have not been addressed much by the currently existing solutions. To further reduce the handover latency and signaling overhead, a fast group authentication scheme is proposed in this paper to support secure and seamless handovers for multiple resource constrained 6LoWPAN devices. With the consideration of mobile sensors with limited energy, only simple hash functions and symmetric encryption algorithms are used. The security analysis and the performance evaluation show that the proposed 6LoWPAN group handover scheme could enhance the security functionalities with high efficiency to achieve a fast authentication for handovers.

EPRO NW - 007	Network-Aware Feasible Repairs for Erasure-Coded Storage

A significant amount of research on using erasure coding for distributed storage has focused on reducing the amount of data that needs to be transferred to replace failed nodes. This continues to be an active topic as the introduction of faster storage devices looks to put an even greater strain on the network. However, with a few notable exceptions, most published work assumes a flat, static network topology between the nodes of the system. We propose a general framework to find the lowest cost feasible repairs in a more realistic, heterogeneous and dynamic network, and examine how the number of repair strategies to consider can be reduced for three distinct erasure codes. We devote a significant part of the paper to determining the set of feasible repairs for random linear network coding (RLNC) and describe a system of efficient checks using techniques from the arsenal of dynamic programming. Our solution involves decomposing the problem into smaller steps, memorizing, and then reusing intermediate results. All computationally intensive operations are performed prior to the failure of a node to ensure that the repair can start with minimal delay, based on up-to-date network information. We show that all three codes benefit from being network aware and find that the extra computations required for RLNC can be reduced to a viable level for a wide range of parameter values.

EPRO NW - 008	On-Line Anomaly Detection with High Accuracy

Traffic anomaly detection is critical for advanced Internet management. Existing detection algorithms generally convert the high-dimensional data to a long vector, which compromises the detection accuracy due to the loss of spatial information of data. Moreover, they are generally designed based on the separation of normal and anomalous data in a time period, which not only introduces high storage and computation cost but also prevents timely detection of anomalies. Online and accurate traffic anomaly detection is critical but difficult to support. To address the challenge, this paper directly models the monitoring data in each time slot as a 2-D matrix, and detects anomalies in the new time slot based on bilateral principal component analysis (B-PCA). We propose several novel techniques in OnlineBPCA to support quick and accurate anomaly detection in real time, including a novel B-PCA-based anomaly detection principle that jointly considers the variation of both row and column principal directions for more accurate anomaly detection, an approximate algorithm to avoid using iteration procedure to calculate the principal directions in a close-form, and a sequential anomaly algorithm to quickly update principal directions with low computation and storage cost when receiving a new data matrix at a time slot. To the best of our knowledge, this is the first work that exploits 2-D PCA for anomaly detection. We have conducted extensive simulations to compare our OnlineBPCA with the state-of-art anomaly detection algorithms using real traffic traces Abilene and GÈANT.

EPRO NW - 009	FINE: A Framework for Distributed Learning on Incomplete Observations for Heterogeneous Crowdsensing Networks

In recent years, there has been a wide range of applications of crowdsensing in mobile social networks and vehicle networks. As centralized learning methods lead to unreliabitlity of data collection, high cost of central server, and concern of privacy, one important problem is how to carry out an accurate distributed learning process to estimate parameters of an unknown model in crowdsensing. Motivated by this, we present the design, analysis, and evaluation of FINE, a distributed learning framework for incomplete-data and non-smooth estimation. Our design, devoted to develop a feasible framework that efficiently and accurately learns the parameters in crowdsensing networks, well generalizes the previous learning methods in which it supports heterogeneous dimensions of data records observed by different nodes, as well as minimization based on non-smooth error functions. In particular, FINE uses a novel distributed record completion algorithm that allows each node to obtain the global consensus by an efficient communication with neighbors, and a distributed dual average algorithm that achieves the efficiency of minimizing non-smooth error functions. Our analysis shows that all these algorithms converge, of which the convergence rates are also derived to confirm their efficiency. We evaluate the performance of our framework with experiments on synthetic and real-world networks.

EPRO NW - 010	Enhancing Fault Tolerance and Resource Utilization in Unidirectional Quorum-Based Cycle Routing

Cycle-based optical network routing, whether using synchronous optical networking rings or p-cycles, provides sufficient reliability in the network. Light trails forming a cycle allow broadcasts within a cycle to be used for efficient multicasts. Optimal communication quorum sets forming optical cycles based on light trails have been shown to flexibly and efficiently route both point-to-point and multipoint-to-multipoint traffic requests. Commonly, cycle routing techniques use pairs of cycles to achieve both routing and fault tolerance, which use substantial resources and create the potential for underutilization. Instead, we intentionally utilize R redundancy within the quorum cycles for fault tolerance such that every point-to-point communication pairs occur in at least R cycles. We develop a generalized R redundancy cycle technique that provides optical networks high fault-tolerant communications capability. When applied using only the single unidirectional cycles rather than the standard paired cycles, the generalized R redundancy technique has been shown to almost halve the necessary light-trail resources in the network. However, due to unidirectional nature, a small percentage of node pairs for one-to-one communication may not have exactly two paths. For this reason, we further develop a greedy cycle direction heuristic and show a reduction of missing pairs. More importantly, we show that the resource requirement is reduced while maintaining the fault tolerance and dependability expected from cycle-based routing. The result is a set of cycles with 96.6%-99.37% fault coverage, while using 42.9%-47.18% fewer resources.

EPRO NW - 011	Urban-Scale Human Mobility Modeling With Multi-Source Urban Network Data

Expanding our knowledge about human mobility is essential for building efficient wireless protocols and mobile applications. Previous mobility studies have typically been built upon empirical single-source data (e.g., cellphone or transit data), which inevitably introduces a bias against residents not contributing this type of data, e.g., call detail records cannot be obtained from the residents without cellphone activities, and transit data cannot cover the residents who walk or ride private vehicles. To address this issue, we propose and implement a novel architecture mPat to explore human mobility using multi-source urban network data. A reference implementation of mPat was developed at an unprecedented scale upon the urban infrastructures of Shenzhen, China. The novelty and uniqueness of mPat lie in its three layers: 1) a data feed layer consisting of real-time data feeds from various urban networks with 24 thousand vehicles, 16 million smart cards, and 10 million cellphones; 2) a mobility abstraction layer exploring correlation and divergence among multi-source data to infer human mobility with a context-aware optimization model based on block coordinate decent; and 3) an application layer to improve urban efficiency based on the human mobility findings of the study. The evaluation shows that mPat achieves a 79% inference accuracy, and that its real-world application reduces passenger travel time by 36%.

EPRO NW - 012	Datum: Managing Data Purchasing and Data Placement in a Geo-Distributed Data Market

This paper studies two design tasks faced by a geodistributed cloud data market: which data to purchase (data purchasing) and where to place/replicate the data for delivery (data placement). We show that the joint problem of data purchasing and data placement within a cloud data market can be viewed as a facility location problem and is thus NP-hard. However, we give a provably optimal algorithm for the case of a data market made up of a single data center and then generalize the structure from the single data center setting in order to develop a near-optimal, polynomial-time algorithm for a geo-distributed data market. The resulting design, Datum, decomposes the joint purchasing and placement problem into two subproblems, one for data purchasing and one for data placement, using a transformation of the underlying bandwidth costs. We show, via a case study, that Datum is near optimal (within 1.6%) in practical settings.

EPRO NW - 013	Congestion Avoidance and Load Balancing in Content Placement and Request Redirection for Mobile CDN

With the development of network function virtualization and software-defined network standards, the mobile network operators are interested in integrating content delivery network (CDN) functionalities into the mobile network to enhance their capability for supporting content oriented services. We consider a mobile CDN system, where Base Stations (BSs) are equipped with storage for replicating content. In such a system, BSs cooperation in replying user requests through backhaul links is a widely adopted mechanism. Blindly redirect user requests upon content placement can cause traffic congestion. As a result, congestion avoidance and load balancing is an important issue to be tackled in this scenario. We investigated the joint optimization problem of content placement and request redirection for the BS-based mobile CDN. Specifically, each BS maintains a transmission queue for replying requests issued from other BSs. Network congestion and BSs load balancing can be jointly considered through guaranteeing network stability. We employ the stochastic optimization model to minimize the long-term time-average transmission cost under network stability constraints. By using the Lyapunov optimization technique, we transform the long-term problem into a set of linear programs solved in each short time duration, and we develop an on-line algorithm to efficiently decide content placement and request redirection without requiring a priori knowledge on the random network.

EPRO NW - 014	Joint Optimization of Multicast Energy in Delay-Constrained Mobile Wireless Networks

This paper studies the problem of optimizing multicast energy consumption in delay-constrained mobile wireless networks, where information from the source needs to be delivered to all the k destinations within an imposed delay constraint. Most existing works simply focus on deriving transmission schemes with the minimum transmitting energy, overlooking the energy consumption at the receiver side. Therefore, in this paper, we propose ConMap, a novel and general framework for efficient transmission scheme design that jointly optimizes both the transmitting and receiving energy. In doing so, we formulate our problem of designing minimum energy transmission scheme, called DeMEM, as a combinatorial optimization one, and prove that the approximation ratio of any polynomial time algorithm for DeMEM cannot be better than (1/4) lnk. Aiming to provide more efficient approximation schemes, the proposed ConMap first converts DeMEM into an equivalent directed Steiner tree problem through creating auxiliary graph gadgets to capture energy consumption, then maps the computed tree back into a transmission scheme. The advantages of ConMap are threefolded: 1) Generality- ConMap exhibits strong applicability to a wide range of energy models; 2) Flexibility- Any algorithm designed for the problem of directed Steiner tree can be embedded into our ConMap framework to achieve different performance guarantees and complexities; 3) Efficiency- ConMap preserves the approximation ratio of the embedded Steiner tree algorithm.

EPRO NW - 015	Information Spreading Forensics via Sequential Dependent Snapshots

Mining the characteristics of information spreading in networks is crucial in communication studies, network security management, epidemic investigations, etc. Previous works are restrictive because they mainly focused on the information source detection using either a single observation, or multiple but independent observations of the underlying network while assuming a homogeneous information spreading rate. We conduct a theoretical and experimental study on information spreading, and propose a new and novel estimation framework to estimate 1) information spreading rates, 2) start time of the information source, and 3) the location of information source by utilizing multiple sequential and dependent snapshots where information can spread at heterogeneous rates. Our framework generalizes the current state-of-the-art rumor centrality [1] and the union rumor centrality [2]. Furthermore, we allow heterogeneous information spreading rates at different branches of a network. Our framework provides conditional maximum likelihood estimators for the above three metrics and is more accurate than rumor centrality and Jordan center in both synthetic networks and real-world networks. Applying our framework to the Twitter's retweet networks, we can accurately determine who made the initial tweet and at what time the tweet was sent. Furthermore, we also validate that the rates of information spreading are indeed heterogeneous among different parts of a retweet network.

EPRO NW - 016	Scheduling Frameworks for Cloud Container Services

Compared with traditional virtual machines, cloud containers are more flexible and lightweight, emerging as the new norm of cloud resource provisioning. We exploit this new algorithm design space, and propose scheduling frameworks for cloud container services. Our offline and online schedulers permit partial execution, and allow a job to specify its job deadline, desired cloud containers, and inter-container dependence relations. We leverage the following classic and new techniques in our scheduling algorithm design. First, we apply the compact-exponential technique to express and handle nonconventional scheduling constraints. Second, we adopt the primal-dual framework that determines the primal solution based on its dual constraints in both the offline and online algorithms. The offline scheduling algorithm includes a new separation oracle to separate violated dual constraints, and works in concert with the randomized rounding technique to provide a near-optimal solution. The online scheduling algorithm leverages the online primal-dual framework with a learning-based scheme for obtaining dual solutions. Both theoretical analysis and trace-driven simulations validate that our scheduling frameworks are computationally efficient and achieve close-to-optimal aggregate job valuation.

EPRO NW - 017	Utility-Centric Networking: Balancing Transit Costs with Quality of Experience

This paper is focused on techniques for maximizing utility across all users within a total network transit cost budget. We present a new method for selecting between replicated servers distributed over the Internet. First, we introduce a novel utility framework that factors in quality of service metrics. Then we design an optimization algorithm, solvable in polynomial time, to allocate user requests to servers based on utility while satisfying network transit cost constraints, mapping service names to service instance locators. We then describe an efficient, low overhead distributed model which only requires knowledge of a fraction of the data required by the global optimization formulation. Next, a load-balancing variant of the algorithm is explored that substantially reduces blocking caused by congested servers. Extensive simulations show that our method is scalable and leads to higher user utility compared with mapping user requests to the closest service replica, while meeting network traffic cost constraints. We discuss several options for real-world deployment that require no changes to end-systems based on either the use of SDN controllers or extensions to the current DNS system.

EPRO NW - 018	Scalability and Satisfiability of Quality-of-Information in Wireless Networks

Quality of information (QoI) provides a context-dependent measure of the utility that a network delivers to its users by incorporating non-traditional information attributes. Quickly and easily predicting performance and limitations of a network using QoI metrics is a valuable tool for network design. Even more useful is an understanding of how network components like topology, bandwidth, and protocols, impact these limitations. In this paper, we develop a QoI-based framework that can provide accurate estimates for limitations on network size and achievable QoI requirements, focusing on completeness and timeliness. We extend this framework to model competing flows and data loads as random variables to capture the stochastic nature of real networks. We show that our framework can provide a characterization of delays for satisfied queries to further analyze performance when some late arrivals are acceptable. Analysis shows that the large tradeoffs exist between network parameters, such as QoI requirements, topology, and network size. Simulation results also provide evidence that the developed framework can estimate network limits and delays with high accuracy. Finally, this paper also introduces scalably feasible QoI regions, which provide upper bounds on QoI requirements that can be supported for certain network applications.

EPRO NW - 019	Anomaly Detection and Attribution in Networks with Temporally Correlated Traffic

Anomaly detection in communication networks is the first step in the challenging task of securing a network, as anomalies may indicate suspicious behaviors, attacks, network malfunctions, or failures. In this paper, we address the problem of not only detecting the anomalous events but also of attributing the anomaly to the flows causing it. To this end, we develop a new statistical decision theoretic framework for temporally correlated traffic in networks via Markov chain modeling. We first formulate the optimal anomaly detection problem via the generalized likelihood ratio test (GLRT) for our composite model. This results in a combinatorial optimization problem which is prohibitively expensive. We then develop two low-complexity anomaly detection algorithms. The first is based on the cross entropy (CE) method, which detects anomalies as well as attributes anomalies to flows. The second algorithm performs anomaly detection via GLRT on the aggregated flows transformation - a compact low-dimensional representation of the raw traffic flows. The two algorithms complement each other and allow the network operator to first activate the flow aggregation algorithm in order to quickly detect anomalies in the system. Once an anomaly has been detected, the operator can further investigate which specific flows are anomalous by running the CE-based algorithm. We perform extensive performance evaluations and experiment our algorithms on synthetic and semi-synthetic data, as well as on real Internet traffic data obtained from the MAWI archive

EPRO NW - 020	Toward Cloud-Based Distributed Interactive Applications: Measurement, Modeling, and Analysis

With the prevalence of broadband network and wireless mobile network accesses, distributed interactive applications (DIAs) such as online gaming have attracted a vast number of users over the Internet. The deployment of these systems, however, comes with peculiar hardware/software requirements on the user consoles. Recently, such industrial pioneers as Gaikai, Onlive, and Ciinow have offered a new generation of cloud-based DIAs (CDIAs), which shifts the necessary computing loads to cloud platforms and largely relieves the pressure on individual user's consoles. In this paper, we aim to understand the existing CDIA framework and highlight its design challenges. Our measurement reveals the inside structures as well as the operations of real CDIA systems and identifies the critical role of cloud proxies. While its design makes effective use of cloud resources to mitigate client's workloads, it may also significantly increase the interaction latency among clients if not carefully handled. Besides the extra network latency caused by the cloud proxy involvement, we find that computation-intensive tasks (e.g., game video encoding) and bandwidth-intensive tasks (e.g., streaming the game screens to clients) together create a severe bottleneck in CDIA.

EPRO NW - 021	A Software Defined Network-Based Security Assessment Framework for CloudIoT

The integration of cloud and Internet of Things (IoT), named CloudIoT, has been considered as an enabler for many different applications. However, the suspicion about the security issue is one main concern that some organizations hesitate to adopt such technologies while some just ignore the security issue while integrating the CloudIoT into their business. Therefore, given the numerous choices of cloud-resource providers and IoT devices, how to evaluate their security level becomes an important issue to promote the adoption of CloudIoT as well as reduce the business security risks. To solve this problem, considering the importance of the business data in CloudIoT, we develop an end-to-end security assessment framework based on software defined network (SDN) to evaluate the security level for the given CloudIoT offering. Specially, in order to simplify the network controls and focus on the analysis about the data flow through CloudIoT, we develop a three-layer framework by integrating SDN and CloudIoT, which consists of 23 different indicators to describe its security features. Then, the interviews from industry and academic are carried out to understand the importance of these features for the overall security. Furthermore, given the relevant evidences from the CloudIoT offering, the Google Brillo and Microsoft Azure IoT Suite, our framework can effectively evaluate the security level which can help the consumers for their CloudIoT selection.

EPRO NW - 022	Efficient Privacy-preserving Machine Learning in Hierarchical Distributed System

With the dramatic growth of data in both amount and scale, distributed machine learning has become an important tool to discover the essential knowledge from massive data. However, it is infeasible to aggregate data from all data owners due to the practical physical constraints. Potential privacy leakage during distributed machine learning also deters participants to share their raw data. To tackle this problem, various privacy-preserving learning approaches are introduced to protect the data privacy. Unfortunately, existing approaches have shortcomings used in practical applications. On the one hand, traditional privacy-preserving learning approaches rely on heavy cryptographic primitives on training data, in which the learning speed is dramatically slowed down due to computation overheads. On the other hand, complicated architectures of distributed system prevent existing solutions from being deployed in practical scenarios. In this paper, we propose a novel efficient privacy-preserving machine learning scheme for hierarchical distributed systems. With the study of different scenarios, the proposed scheme not only reduces the overhead for the learning process but also provides the comprehensive protection for the hierarchical distributed system. Extensive real-world experiments are implemented to evaluate the privacy, efficacy, and efficiency of our proposed schemes.

EPRO NW - 023	Adaptive and Fault-tolerant Data Processing in Healthcare IoT Based on Fog Computing

In recent years, healthcare IoT have been helpful in mitigating pressures of hospital and medical resources caused by aging population to a large extent. As a safety-critical system, the rapid response from the health care system is extremely important. To fulfill the low latency requirement, fog computing is a competitive solution by deploying healthcare IoT devices on the edge of clouds. However, these fog devices generate huge amount of sensor data. Designing a specific framework for fog devices to ensure reliable data transmission and rapid data processing becomes a topic of utmost significance. In this paper, a Reduced Variable Neighborhood Search (RVNS)-based sEnsor Data Processing Framework (REDPF) is proposed to enhance reliability of data transmission and processing speed. Functionalities of REDPF include fault-tolerant data transmission, self-adaptive filtering and data-load-reduction processing. Specifically, a reliable transmission mechanism, managed by a self-adaptive filter, will recollect lost or inaccurate data automatically. Then, a new scheme is designed to evaluate the health status of the elderly people. Through extensive simulations, we show that our proposed scheme improves network reliability, and provides a faster processing speed.

EPRO NW - 024	Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption

Cyber-Physical Systems (smart grid, smart transportation, smart cities, etc.), driven by advances in Internet of Things (IoT) technologies, will provide the infrastructure and integration of smart applications to accelerate the generation and collection of big data to an unprecedented scale. As now a fundamental commodity in our current information age, such big data is a crucial key to competitiveness in modern commerce. In this paper, we address the issue of privacy preservation for data auction in CPS by leveraging the concept of homomorphic cryptography and secured network protocol design. Specifically, we propose a generic Privacy-Preserving Auction Scheme (PPAS), in which the two independent entities of Auctioneer and Intermediate Platform comprise an untrusted third-party trading platform. Via the implementation of homomorphic encryption and one-time pad, a winner in the auction process can be determined and all bidding information is disguised. Yet, to further improve the security of the privacy-preserving auction, we additionally propose an Enhanced Privacy-Preserving Auction Scheme (EPPAS) that leverages an additional signature verification mechanism. The feasibilities of both schemes are validated through detailed theoretical analyses and extensive performance evaluations, including assessment of the resilience to attacks. In addition, we discuss some open issues and extensions relevant to our scheme.

EPRO NW - 025	Redundancy Avoidance for Big Data in Data Centers: A Conventional Neural Network Approach

As the innovative data collection technologies are applying to every aspect of our society, the data volume is skyrocketing. Such phenomenon poses tremendous challenges to data centers with respect to enabling storage. In this paper, a hybrid-stream big data analytics model is proposed to perform multimedia big data analysis. This model contains four procedures, i.e., data pre-processing, data classification, data recognition and data load reduction. Specifically, an innovative multi-dimensional Convolution Neural Network (CNN) is proposed to assess the importance of each video frame. Thus, those unimportant frames can be dropped by a reliable decision-making algorithm. In order to ensure video quality, minimal correlation and minimal redundancy (MCMR) are combined to optimize the decision-making algorithm. Simulation results show that the amount of processed video is significantly reduced, and the quality of video is preserved due to the addition of MCMR. The simulation also proves that the proposed model performs steadily and is robust enough to scale up to accommodate the big data crush in data centers.

EPRO NW - 026	Phishing-Aware: A Neuro-Fuzzy Approach for Anti-Phishing on Fog Networks

Phishing detection is recognized as a criminal issue of Internet security. By deploying a gateway anti-phishing in the networks, these current hardware-based approaches provide an additional layer of defense against phishing attacks. However, such hardware devices are expensive and inefficient in operation due to the diversity of phishing attacks. With promising technologies of virtualization in fog networks, an anti-phishing gateway can be implemented as software at the edge of the network and embedded robust machine learning techniques for phishing detection. In this paper, we use uniform resource locator (URL) features and web traffic features to detect phishing websites based on a designed neuro-fuzzy framework (dubbed Fi-NFN). Based on the new approach, fog computing as encouraged by Cisco, we design an anti-phishing model to transparently monitor and protect fog users from phishing attacks. The experiment results of our proposed approach, based on a large-scale dataset collected from real phishing cases, have shown that our system can effectively prevent phishing attacks and improve the security of the network.

EPRO NW - 027	A Private and Efficient Mechanism for Data Uploading in Smart Cyber-Physical Systems

To provide fine-grained access to different dimensions of the physical world, data uploading in smart cyber-physical systems suffers novel challenges on both energy conservation and privacy preservation. It is always critical for participants to consume as little energy as possible for data uploading. However, simply pursuing energy efficiency may lead to extreme disclosure of private information, especially when the uploaded contents from participants are more informative than ever. In this paper, we propose a novel mechanism for data uploading in smart cyber-physical systems, which considers both energy conservation and privacy preservation. The mechanism preserves privacy by concealing abnormal behaviors of participants, while still achieves an energy-efficient scheme for data uploading by introducing an acceptable number of extra contents. To derive an optimal uploading scheme is proved to be NP-hard. Accordingly, we propose a heuristic algorithm and analyze its effectiveness. The evaluation results towards a real-world dataset demonstrate that the results obtained through our proposed algorithm is comparable with the optimal ones.

EPRO NW - 028	Mobile Edge Computing Resources Optimization: A Geo-Clustering Approach

Mobile edge computing (MEC) is an emerging technology that aims at pushing applications and content close to the users (e.g., at base stations, access points, and aggregation networks) to reduce latency, improve quality of experience, and ensure highly efficient network operation and service delivery. It principally relies on virtualization-enabled MEC servers with limited capacity at the edge of the network. One key issue is to dimension such systems in terms of server size, server number, and server operation area to meet MEC goals. In this paper, we formulate this problem as a mixed integer linear program. We then propose a graph-based algorithm that, taking into account a maximum MEC server capacity, provides a partition of MEC clusters, which consolidates as many communications as possible at the edge. We use a dataset of mobile communications to extensively evaluate them with real world spatio-temporal human dynamics. In addition to quantifying macroscopic MEC benefits, the evaluation shows that our algorithm provides MEC area partitions that largely offload the core, thus pushing the load at the edge (e.g., with 10 small MEC servers between 55% and 64% of the traffic stay at the edge), and that are well balanced through time.

EPRO NW - 029	Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks

The medical industry is increasingly digitalized and Internet-connected (e.g., Internet of Medical Things), and when deployed in an Internet of Medical Things environment, software-defined networks (SDNs) allow the decoupling of network control from the data plane. There is no debate among security experts that the security of Internet-enabled medical devices is crucial, and an ongoing threat vector is insider attacks. In this paper, we focus on the identification of insider attacks in healthcare SDNs. Specifically, we survey stakeholders from 12 healthcare organizations (i.e., two hospitals and two clinics in Hong Kong, two hospitals and two clinics in Singapore, and two hospitals and two clinics in China). Based on the survey findings, we develop a trust-based approach based on Bayesian inference to figure out malicious devices in a healthcare environment. Experimental results in either a simulated and a real-world network environment demonstrate the feasibility and effectiveness of our proposed approach regarding the detection of malicious healthcare devices, i.e., our approach could decrease the trust values of malicious devices faster than similar approaches.

EPRO NW - 030	Structure-based Sybil Detection in Social Networks via Local Rule-based Propagation

Social networks are known to be vulnerable to Sybil attack, in which an attacker maintains massive Sybils to perform various malicious activities. Therefore, Sybil detection in social networks is a fundamental security research problem. Structure-based methods have been shown to be promising at detecting Sybils. Existing structure-based methods can be classified into Random Walk (RW)-based methods and Loop Belief Propagation (LBP)-based methods. RW-based methods cannot leverage labeled Sybils and labeled benign users simultaneously, which limits their detection accuracy, and they are not robust to noisy labels. LBP-based methods are not scalable, and cannot guarantee convergence. We propose SybilSCAR, a novel structure-based method to perform Sybil detection in social networks. SybilSCAR maintains the advantages of existing methods while overcoming their limitations. Specifically, SybilSCAR is Scalable, Convergent, Accurate, and Robust to label noises. We first propose a framework to unify RW-based and LBP-based methods. Under our framework, these methods can be viewed as iteratively applying a local rule to every user, which propagates label information among a social graph. Second, we design a new local rule, which SybilSCAR iteratively applies to every user to detect Sybils. We perform both theoretical and empirical evaluations to compare SybilSCAR with state-of-the-art RW-based and LBP-based methods

EPRO NW - 031	Traffic Load Minimization in Software Defined Wireless Sensor Networks

The emerging software defined networking enables the separation of control plane and data plane and saves the resource consumption of the network. Breakthrough in this area has opened up a new dimension to the design of software defined method in wireless sensor networks (WSNs). However, the limited routing strategy in software defined WSNs (SDWSNs) imposes a great challenge in achieving the minimum traffic load. In this paper, we propose a flow splitting optimization (FSO) algorithm for solving the problem of traffic load minimization (TLM) in SDWSNs by considering the selection of optimal relay sensor node and the transmission of optimal splitting flow. To this end, we first establish the model of different packet types and describe the TLM problem. We then formulate the TLM problem into an optimization problem which is constrained by the load of sensor nodes and the packet similarity between different sensor nodes. Afterwards, we present a Levenberg-Marquardt algorithm for solving the optimization problem of traffic load. We also provide the convergence analysis of the Levenberg-Marquardt algorithm. Finally, we implement the FSO algorithm in the NS-2 simulator and give extensive simulation results to verify the efficiency of FSO algorithm in SDWSNs.

EPRO NW - 032	NetworkAI: An Intelligent Network Architecture for Self-Learning Control Strategies in Software Defined Networks

The past few years have witnessed a wide deployment of software defined networks facilitating a separation of the control plane from the forwarding plane. However, the work on the control plane largely relies on a manual process in configuring forwarding strategies. To address this issue, this paper presents NetworkAI, an intelligent architecture for self-learning control strategies in SDN networks. NetworkAI employs deep reinforcement learning and incorporates network monitoring technologies such as the in-band network telemetry to dynamically generate control policies and produces a near optimal decision. Simulation results demonstrated the effectiveness of NetworkAI.

EPRO NW - 033	TNGuard: Securing IoT Oriented Tenant Networks Based on SDN

In the paradigm of infrastructure-as-a-service cloud computing involving an Internet of Things network, customers outsource their infrastructure to the cloud. An outsourced infrastructure is a virtual infrastructure that mimics the physical infrastructure of the precloud era; it is therefore referred to as a tenant network (TN) in this paper. This practice draws upon the notion of TN abstraction, which specifies how TNs should be managed. However, current virtual software-defined network (SDN) technology uses an SDN hypervisor to attain TNs, where the cloud administrator is given much-more-than-necessary privileges; thus, not only could violation of the security principle of least privilege occur, but the threat of a malicious or innocent-but-compromised administrator may be present. Motivated by this need, we propose the specification of TN abstraction, including its functions and security requirements. Then, we present a platform-independent concretization of this abstraction called TNGuard, which is an SDN-based architecture that protects the TNs while removing unnecessary privileges from the cloud administrator. In order to show that TNGuard concretizes the TN abstraction, we present an instantiation of TNGuard on the Xen virtualization platform with the Ryu controller. Experimental results show that the resulting system is practical, incurring a small performance overhead.

EPRO NW - 034	SDN-Enabled Traffic-Aware Load Balancing for M2M Networks

This paper proposes a traffic-aware load balancing scheme for machine-to-machine (M2M) networks using software-defined networking (SDN). Load balancing techniques are essential for M2M networks to relieve the heavy loading caused by bursty traffic. Leveraging the capability of SDN to monitor and control the network, the proposed load balancing scheme can satisfy different quality of service requirements through traffic identification and rerouting. Experimental results show that the proposed scheme can reduce service response time up to 50% compared to the non-SDN load balancing scheme.

EPRO NW - 035	Energy-Optimal Data Aggregation and Dissemination for the Internet of Things

Established approaches to data aggregation in wireless sensor networks (WSNs) do not cover the variety of new use cases developing with the advent of the Internet of Things (IoT). In particular, the current push toward fog computing, in which control, computation, and storage are moved to nodes close to the network edge, induces a need to collect data at multiple sinks, rather than the single sink typically considered in WSN aggregation algorithms. Moreover, for machine-to-machine communication scenarios, actuators subscribing to sensor measurements may also be present, in which case data should be not only aggregated and processed in-network but also disseminated to actuator nodes. In this paper, we present mixed-integer programming formulations and algorithms for the problem of energy-optimal routing and multiple-sink aggregation, as well as joint aggregation and dissemination, of sensor measurement data in IoT edge networks. We consider optimization of the network for both minimal total energy usage, and min-max per-node energy usage. We also provide a formulation and algorithm for throughput-optimal scheduling of transmissions under the physical interference model in the pure aggregation case. We have conducted a numerical study to compare the energy required for the two use cases, as well as the time to solve them, in generated network scenarios with varying topologies and between 10 and 40 nodes. Although aggregation only accounts for less than 15% of total energy usage in all cases tested, it provides substantial energy savings. Our results show more than 13 times greater energy usage for 40-node networks using direct, shortest-path flows from sensors to actuators, compared with our aggregation and dissemination solutions.

EPRO NW - 036	Self-Healing Framework for Next-Generation Networks through Dimensionality Reduction

Next-generation self-organizing networks (NG-SONs) are the key that will lead to the full automation of the network management in the forthcoming generations of cellular communications. New challenges, like the deployment of novel wireless services or the aim of operators to provide end-to-end monitoring and opimization, make it necessary to develop an innovative scheme for network management. Within SON, self-healing (SH) comprises fault detection, root cause analysis (RCA), and compensation. Within these, the automation of RCA activities is one of the key elements to reduce operational expenditures related to network management. In this article, an SH framework for next-generation networks using dimensionality reduction is proposed as the tool enabling the management of an increasingly complex network, taking advantage of both feature selection and feature extraction techniques. A proof of concept has been carried out in the context of automatic RCA in a live network. Results show that the proposed framework can effectively manage a high-dimensional environment from different data sources, eventually automating the tasks usually performed by troubleshooting experts while optimizing the performance of the RCA tool.

ELYSIUMPRO

A UNIT OF ELYSIUM GROUPS

Thank you!

ELYSIUM GROUPS