ANSPRO TECHNOLOGIES

IEEE 2018-19 PROJECT LIST	
NETWORKING	
CODE	TITLE AND ABSTRACT
19ANSP-NW-001	**PROVEST: Provenance-Based Trust Model for Delay Tolerant Networks** ***Abstract***—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. This work adopts a model-based method to evaluate the performance of PROVEST (i.e., trust accuracy and routing performance) using Stochastic Petri Nets. We conduct a comparative performance analysis of PROVEST against existing trust-based and non-trust-based DTN routing protocols to analyze the benefits of PROVEST. We validate PROVEST using a real dataset of DTN mobility traces.
19ANSP-NW-002	**Modeling, Analysis, and Implementation of Universal Acceleration Platform Across Online Video Sharing Sites** ***Abstract***— User-generated video sharing service has attracted a vast number of users over the Internet. The most successful sites, such as YouTube and Youku, now enjoy millions of videos being watched every day. Yet, given limited network and server resources, the user experience of existing video sharing sites (VSSes) is still far from being satisfactory. To mitigate such a problem, peer-to-peer (P2P) based video accelerators

	have been widely suggested to enhance the video delivery on VSSes. In this paper, we find that the interference of multiple accelerators will lead to a severe bottleneck across the VSSes. Our model analysis shows that a universal video accelerator can naturally achieve better performance with lower deployment cost. Based on this observation, we further present the detailed design of Peer-to-Peer Video Accelerator (PPVA), a real-world system for universal and transparent P2P accelerating. Such a system has already attracted over 180 million users, with 48 million video transactions every day. We carefully examine the PPVA performance from extensive measurements. Our trace analysis indicates that it can significantly reduce server bandwidth cost and accelerate the video download speed by 80 percent.
19ANSP-NW-003	**CCLBR: Congestion Control-Based Load Balanced Routing in Unstructured P2P Systems** ***Abstract***— Given the growing popularity of the peer-to-peer (P2P) network systems in the recent years, efficient query routing under highly dynamic environments is still lacking in several P2P network systems. In response to this challenge, this paper proposes a new churn-resilient system to find alternative routing paths for the purpose of balancing the query loads under higher network churns and heavy workloads, ultimately to improve the search efficiency. Two novel methods are devised to balance the network query loads among both inter- and intragroup level peers. First, a resource grouping and a rewiring method is proposed to spontaneously organize and cluster the peers having same resources together. This strategy facilitates the peers to evolve the network into a cluster-like topology and balances the query loads among the intergroup peers. Second, a collaborative*Q*-learningmethod is proposed to balance the query loads among the intragroup peers in order to intelligently avoid queries being forwarded to the congested peers in the network. Experiments conducted under dynamic network scenarios demonstrate that our proposed method achieves better search performances with a more balanced network load than the existing methods, and further exhibits higher robustness and adaptability under higher network churns and heavy network loads.
19ANSP-NW-004	**LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities** ***Abstract***— Recent literature suggests that the Internet of Things (IoT) scales much better in an information-centric networking (ICN) model instead of the

	current host-centric Internet protocol (IP) model. In particular, the named data networking (NDN) project (one of the ICN architecture flavors) offers features exploitable by IoT applications, such as stateful forwarding, in-network caching, and built-in assurance of data provenance. Though NDN-based IoT frameworks have been proposed, none have adequately and holistically addressed concerns related to secure onboarding and routing. Additionally, emerging IoT applications such as smart cities require high scalability and thus pose new challenges to NDN routing. Therefore, in this paper, we propose and evaluate a novel, scalable framework for lightweight authentication and hierarchical routing in the NDN IoT. Our ns-3 based simulation analyses demonstrate that our framework is scalable and efficient. It supports deployment densities as high as 40 000 nodes/km2 with an average onboarding convergence time of around 250 s and overhead of less than 20 kibibytes per node. This demonstrates its efficacy for emerging large-scale IoT applications such as smart cities.
19ANSP-NW-005	**FlopCoin: A Cryptocurrency for Computation Offloading** ***Abstract—*** During the last years, researchers have proposed solutions to help smartphones improve execution time and reduce energy consumption by offloading heavy tasks to remote entities. Lately, inspired by the promising results of message forwarding in opportunistic networks, many researchers have proposed strategies for task offloading towards nearby mobile devices, giving birth to the Device-to-Device offloading paradigm. None of these strategies, though, offers any mechanism that considers selfish users and, most importantly, that motivates and defrays the participating devices who spend their resources. In this paper, we address these problems and propose the design of a framework that integrates an incentive scheme and a reputation mechanism. Our proposal follows the principles of the Hidden Market Design approach, which allows users to specify the amount of resources they are willing to sacrifice when participating in the offloading system. The underlying algorithm, that users are not aware of, is based on a truthful auction strategy and a peer-to-peer reputation exchange scheme. Extensive simulations on real traces depict how our designed mechanism achieves higher offloading rate and produces less traffic compared to three benchmark algorithms. Finally, we show how collaborating devices get rewarded for their contribution, while selfish ones get sidelined by others.

19ANSP-NW-006	**Data Connectivity and Smart Group Formation in Wi-Fi Direct Multi-Group Networks** ***Abstract*—** Users of device-to-device (D2D) communication need efficient content discovery mechanisms to steer their requests toward the node in their neighborhood that is most likely to satisfy them. The problem is further compounded by the lack of a central coordination entity as well as by the inherent mobility of devices, which leads to volatile topologies. In this paper, we first discuss group-based communication among non-rooted Android devices using Wi-Fi direct, a protocol recently standardized by the Wi-Fi alliance. We propose intra- and inter-group communication methodologies, which we validate through a simple testbed where content-centric routing is used. Next, we address the autonomous formation of groups with the goal of achieving efficient device resource utilization as well as full connectivity. Finally, we evaluate the performance of our group formation procedure both in simulation and in a real testbed involving Android devices in different topologies.
19ANSP-NW-007	**Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data** ***Abstract*—** Internet of Things (IoT) has been widely used in our daily life, which enables various objects to be interconnected for data exchange, including physical devices, vehicles, and other items embedded with network connectivity. Wireless sensor network (WSN) is a vital application of IoT, providing many kinds of information among sensors, whereas such network is vulnerable to a wide range of attacks, especially insider attacks, due to its natural environment and inherent unreliable transmission. To safeguard its security, intrusion detection systems (IDSs) are widely adopted in a WSN to defend against insider attacks through implementing proper trust-based mechanisms. However, in the era of big data, sensors may generate excessive information and data, which could degrade the effectiveness of trust computation. In this paper, we focus on this challenge and propose a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure. In the evaluation, we investigate

	the performance of our approach in both a simulated and a real network environment. Experimental results demonstrate that packet-based trust management would become ineffective in a heavy traffic environment, and that our approach can help lighten the burden of IDSs in handling traffic, while maintaining the detection of insider attacks.
19ANSP-NW-008	**EduCTX: A Blockchain-Based Higher Education Credit Platform** ***Abstract*—** Blockchain technology enables the creation of a decentralized environment, where transactions and data are not under the control of any third-party organization. Any transaction ever completed is recorded in a public ledger in a verifiable and permanent way. Based on the blockchain technology, we propose a global higher education credit platform, named EduCTX. This platform is based on the concept of the European Credit Transfer and Accumulation System (ECTS). It constitutes a globally trusted, decentralized higher education credit, and grading system that can offer a globally unified viewpoint for students and higher education institutions (HEIs), as well as for other potential stakeholders, such as companies, institutions, and organizations. As a proof of concept, we present a prototype implementation of the environment, based on the open-source Ark Blockchain Platform. Based on a globally distributed peer-to-peer network, EduCTX will process, manage, and control ECTX tokens, which represent credits that students gain for completed courses, such as ECTS. HEIs are the peers of the blockchain network. The platform is a first step toward a more transparent and technologically advanced form of higher education systems. The EduCTX platform represents the basis of the EduCTX initiative, which anticipates that various HEIs would join forces in order to create a globally efficient, simplified, and ubiquitous environment in order to avoid language and administrative barriers. Therefore, we invite and encourage HEIs to join the EduCTX initiative and the EduCTX blockchain network.
19ANSP-NW-009	**When Intrusion Detection Meets Blockchain Technology: A Review** ***Abstract*—** With the purpose of identifying cyber threats and possible incidents, intrusion detection systems (IDSs) are widely deployed in various computer networks. In order to enhance the detection capability of a single IDS, collaborative intrusion detection networks (or collaborative

	IDSs) have been developed, which allow IDS nodes to exchange data with each other. However, data and trust management still remain two challenges for current detection architectures, which may degrade the effectiveness of such detection systems. In recent years, blockchain technology has shown its adaptability in many fields, such as supply chain management, international payment, interbanking, and so on. As blockchain can protect the integrity of data storage and ensure process transparency, it has a potential to be applied to intrusion detection domain. Motivated by this, this paper provides a review regarding the intersection of IDSs and blockchains. In particular, we introduce the background of intrusion detection and blockchain, discuss the applicability of blockchain to intrusion detection, and identify open challenges in this direction.
19ANSP-NW-010	**Peer Assessment and Self-Assessment in Social Learning Environments Through a New Crowd-Sourced Mechanism** ***Abstract***— Social learning environments generally provide learners with the grounds to collaboratively create and share different learning contents. The variety and considerably large amount of created contents makes them infeasible for students to read through and often results in a continuous reduction in students' contribution. Therefore, social learning environments should be equipped with effective mechanisms to evaluate and accredit learner-created content relying on students' participation. In order to suggest a voluntary mechanism for peer assessment with the least overhead, the current study proposed a new crowd sourced approach. The approach called content-dependent multi-label voting (COMVO) offers various assessment options for each type of learning content consisting of resource, assignment, forum, discussion, reply, and comment. COMVO was implemented in a social learning environment and was utilized by students and experts during educational activities in a university course. Peer voting, self-voting, voting to experts, and expert voting were qualitatively analyzed. The results indicated that in contrast to peer voting, which mostly consists of positively describing labels, self-voting labels match those given by experts. Analysis implied that peer voting is reliable and expert-independent. This paper also provided insights about student behaviors and reciprocal effects in identified voting, investigating the role of students' extrinsic and intrinsic motivational orientation in their voting behavior. Results of a

	subjective evaluation indicated that the majority of respondents found COMVO an enthusiastic and efficient tool with the potential to complete other similar crowd sourced peer assessment mechanisms.
19ANSP-NW-011	**A Learning Evasive Email-Based P2P-Like Botnet** ***Abstract*—** Nowadays, machine learning is widely used in malware detection system as a core component. The machine learning algorithm is designed under the assumption that all datasets follow the same underlying data distribution. But the real-world malware data distribution is not stable and changes with time. By exploiting the knowledge of the machine learning algorithm and malware data concept drift problem, we show a novel learning evasive botnet architecture and a stealthy and secure C&C mechanism. Based on the email communication channel, we construct a stealthy email-based P2P-like botnet that exploit the excellent reputation of email servers and a huge amount of benign email communication in the same channel. The experiment results show horizontal correlation learning algorithm is difficult to separate malicious email traffic from normal email traffic based on the volume features and time-related features with enough confidence. We discuss the malware data concept drift and possible defense strategies.
19ANSP-NW-012	**A Regulation Scheme Based on the Ciphertext-Policy Hierarchical Attribute-Based Encryption in Bitcoin System** ***Abstract*—** In Bitcoin financial system, a user's privacy is supposed to be protected by means of anonymity. However, the anonymity makes illegal trades possible because nobody is able to reveal the real identities of the illegal users. In this paper, we propose a regulation scheme based on the ciphertext-policy hierarchical attribute-based encryption (CP-HABE). In the scheme, users' identities are encrypted by using access policy and are contained in their transaction. A type of user is defined as the dependable regulation node, which is responsible for the regulation of transactions and encrypted identities. A new signature algorithm instead of the elliptic curve signature is adopted to generate wallet key pairs, this establishes a connection between wallet addresses and encrypted identities. When a transaction is doubted to involve illegal activities, the authorized regulation nodes are capable of revealing the users' real identities and add the illegal identities to a public blacklist. Our system is based on a new CP-HABE scheme which is proved to be secure

	against chosen-plaintext attack in the standard model under the Bilinear Diffie-Hellman Exponent assumption. Finally, we give a performance analysis of our system. The proposed regulation system can reveal criminals' identities undertaking illegal activities.
19ANSP-NW-013	**Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin** ***Abstract*—** Bitcoin combines a peer-to-peer network and cryptographic algorithm to implement a distributed digital currency system, which keeps all transaction history on a public blockchain. Since all transactions recorded on the blockchain are public to everyone, Bitcoin users face a threat of leaking financial privacy. Many analysis and deanonymization approaches have been proposed to link transaction records to real identities. To eliminate this threat, we present an unlinkable coin mixing scheme that allows users to mix their bitcoins without trusting a third party. This mixing scheme employs a primitive known as ring signature with elliptic curve digital signature algorithm (ECDSA) to conceal the transfer of coins between addresses. The mixing server is only able to check whether the output addresses belong to its customers, but it cannot tell which address owned by which customer. Customers do not have to rely on the reputation of a third party to ensure his money will be returned, and his privacy will not be leaked. This scheme needs no modifications on current Bitcoin system and is convenient to deploy by any communities. We implemented a prototype of our scheme and tested it under the Bitcoin core's regtest mode. Security and privacy of our mixing scheme are ensured through the standard ring signature and ECDSA unforgeability.
19ANSP-NW-014	**Secure APIT Localization Scheme Against Sybil Attacks in Distributed Wireless Sensor Networks** ***Abstract*—** For location-aware applications in wireless sensor networks (WSNs), it is important to ensure that sensor nodes can get correct locations in a hostile WSNs. Sybil attacks, which are vital threats in WSNs, especially in the distributed WSNs. They can forge one or multiple identities to decrease the localization accuracy, or sometimes to collapse the whole localization systems. In this paper, a novel lightweight sybilfree (SF)-APIT algorithm is presented to solve the problem of sybil attacks in APIT localization scheme, which is a popular range-free method and

	performs at individual node in a purely distributed fashion. The proposed SF-APIT scheme requires minimal overhead for wireless devices and works well based on the received signal strength. Simulations demonstrate that SF-APIT is an effective scheme in detecting and defending against sybil attacks with a high detection rate in distributed wireless localization schemes.