Submit Your Paper

View Articles

Guide for Authors

Abstracting/ Indexing

Track Your Paper

Order Journal

Journal Metrics

CiteScore: **3.26** ⓘ

More about CiteScore

Impact Factor: **2.516** ⓘ

5-Year Impact Factor: **2.594** ⓘ

Source Normalized Impact per Paper (SNIP): **1.694** ⓘ

SCImago Journal Rank (SJR): **0.652** ⓘ

› View More on Journal Insights

Article Enrichments

› AudioSlides

› Data in Brief co-submission

› Interactive MATLAB Figure Viewer

Related Links

› Author Stats ⓘ

› Publishing Campus

› Author Services

Most Cited Computer Networks Articles

The most cited articles published since 2012, extracted from Scopus.

The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization

Volume 56, Issue 16, November 2012, Pages 3594-3608

Luigi Atzori | Antonio Iera | Giacomo Morabito | Michele Nitti

Recently there has been quite a number of independent research activities that investigated the potentialities of integrating social networking concepts into Internet of Things (IoT) solutions. The resulting paradigm, named Social Internet of Things (SIoT), has the potential to support novel applications and networking services for the IoT in more effective and efficient ways. In this context, the main contributions of this paper are the following: (i) we identify appropriate policies for the establishment and the management of social relationships between objects in such a way that the resulting social network is navigable; (ii) we describe a possible architecture for the IoT that includes the functionalities required to integrate things into a social network; (iii) we analyze the characteristics of the SIoT network structure by means of simulations.

Cyber security in the Smart Grid: Survey and challenges

Volume 57, Issue 5, April 2013, Pages 1344-1371

Wenye Wang | Zhuo Lu

The Smart Grid, generally referred to as the next-generation power system, is considered as a revolutionary and evolutionary regime of existing power grids. More importantly, with the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. Along with the silent features of the Smart Grid, cyber security emerges to be a critical issue because millions of electronic devices are inter-connected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a widespread infrastructure. In this paper, we present a comprehensive survey of cyber security issues for the Smart Grid. Specifically, we focus on reviewing and discussing security requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the Smart Grid. We aim to provide a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security. © 2012 Elsevier B.V. All rights reserved.

Cloud monitoring: A survey

Volume 57, Issue 9, June 2013, Pages 2093-2115

Giuseppe Aceto | Alessio Botta | Walter De Donato | Antonio Pescapè

Nowadays, Cloud Computing is widely used to deliver services over the Internet for both technical and economical reasons. The number of Cloud-based services has increased rapidly and strongly in the last years, and so is increased the complexity of the infrastructures behind these services. To properly operate and manage such complex infrastructures effective and efficient monitoring is constantly needed. Many works in literature have surveyed Cloud properties, features, underlying technologies (e.g. virtualization), security and privacy. However, to the best of our knowledge, these surveys lack a detailed analysis of monitoring for the Cloud. To fill this gap, in this paper we provide a survey on Cloud monitoring. We start analyzing motivations for Cloud monitoring, providing also definitions and background for the following contributions. Then, we carefully analyze and discuss the properties of a monitoring system for the Cloud, the issues arising from such properties and how such issues have been tackled in literature. We also describe current platforms, both commercial and open source, and services for Cloud monitoring, underlining how they relate with the properties and issues identified before. Finally, we identify open issues, main challenges and future directions in the field of Cloud monitoring. © 2013 Elsevier B.V. All rights reserved.

On the features and challenges of security and privacy in distributed internet of things

Volume 57, Issue 10, July 2013, Pages 2266-2279

Rodrigo Roman | Jianying Zhou | Javier Lopez

In the Internet of Things, services can be provisioned using centralized architectures, where central entities acquire, process, and provide information. Alternatively, distributed architectures, where entities at the edge of the network exchange information and collaborate with each other in a dynamic way, can also be used. In order to understand the applicability and viability of this distributed approach, it is necessary to know its advantages and disadvantages - not only in terms of features but also in terms of security and privacy challenges. The purpose of this paper is to show that the distributed approach has various challenges that need to be solved, but also various interesting properties and strengths. © 2013 Elsevier B.V. All rights reserved.

Reprint of: The anatomy of a large-scale hypertextual web search engine

Volume 56, Issue 18, December 2012, Pages 3825-3833

Sergey Brin | Lawrence Page

In this paper, we present Google, a prototype of a large-scale search engine which makes heavy use of the structure present in hypertext. Google is designed to crawl and index the Web efficiently and produce much more satisfying search results than existing systems. The prototype with a full text and hyperlink database of at least 24 million pages is available at http://google.stanford.edu/ To engineer a search engine is a challenging task. Search engines index tens to hundreds of millions of web pages involving a comparable number of distinct terms. They answer tens of millions of queries every day. Despite the importance of large-scale search engines on the web, very little academic research has been done on them. Furthermore, due to rapid advance in technology and web proliferation, creating a web search engine today is very different from 3 years ago. This paper provides an in-depth description of our large-scale web search engine - the first such detailed public description we know of to date. Apart from the problems of scaling traditional search techniques to data of this magnitude, there are new technical challenges involved with using the additional information present in hypertext to produce better search results. This paper addresses this question of how to build a practical large-scale system which can exploit the additional information present in hypertext. Also we look at the problem of how to effectively deal with uncontrolled hypertext collections, where anyone can publish anything they want. © 2012 Elsevier B.V. All rights reserved.

GENI: A federated testbed for innovative network experiments

Volume 61, Issue , March 2014, Pages 5-23

Mark Berman | Jeffrey S. Chase | Lawrence Landweber | Akihiro Nakao | Max Ott | Dipankar Raychaudhuri | Robert Ricci | Ivan Seskar

GENI, the Global Environment for Networking Innovation, is a distributed virtual laboratory for transformative, at-scale experiments in network science, services, and security. Designed in response to concerns over Internet ossification, GENI is enabling a wide variety of experiments in a range of areas, including clean-slate networking, protocol design and evaluation, distributed service offerings, social network integration, content management, and in-network service deployment. Recently, GENI has been leading an effort to explore the potential of its underlying technologies, SDN and GENI racks, in support of university campus network management and applications. With the concurrent deployment of these technologies on regional and national R & E backbones, this will result in a revolutionary new national-scale distributed architecture, bringing to the entire network the shared, deeply programmable environment that the cloud has brought to the datacenter. This deeply programmable environment will support the GENI research mission and as well as enabling research in a wide variety of application areas. © 2014 Elsevier B.V. All rights reserved.

Security, privacy and trust in Internet of things: The road ahead

Volume 76, Issue , January 2015, Pages 146-164

S. Sicari | A. Rizzardi | L. A. Grieco | A. Coen-Porisini

© 2014 Elsevier B.V. Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains. In this scenario, the satisfaction of security and privacy requirements plays a fundamental role. Such requirements include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arises scalability issues; therefore a flexible infrastructure is needed able to deal with security threats in such a dynamic environment. In this survey we present the main research challenges and the existing solutions in the field of IoT security, identifying open issues, and suggesting some hints for future research.

Energy efficiency in wireless sensor networks: A top-down survey

Volume 67, Issue , July 2014, Pages 104-122

Tifenn Rault | Abdelmadjid Bouabdallah | Yacine Challal

The design of sustainable wireless sensor networks (WSNs) is a very challenging issue. On the one hand, energy-constrained sensors are expected to run autonomously for long periods. However, it may be cost-prohibitive to replace exhausted batteries or even impossible in hostile environments. On the other hand, unlike other networks, WSNs are designed for specific applications which range from small-size healthcare surveillance systems to large-scale environmental monitoring. Thus, any WSN deployment has to satisfy a set of requirements that differs from one application to another. In this context, a host of research work has been conducted in order to propose a wide range of solutions to the energy-saving problem. This research covers several areas going from physical layer optimisation to network layer solutions. Therefore, it is not easy for the WSN designer to select the efficient solutions that should be considered in the design of application-specific WSN architecture. We present a top-down survey of the trade-offs between application requirements and lifetime extension that arise when designing wireless sensor networks. We first identify the main categories of applications and their specific requirements. Then we present a new classification of energy-conservation schemes found in the recent literature, followed by a systematic discussion as to how these schemes conflict with the specific requirements. Finally, we survey the techniques applied in WSNs to achieve trade-off between multiple requirements, such as multi-objective optimisation. © 2014 Elsevier B.V. All rights reserved.

A tool for the generation of realistic network workload for emerging networking scenarios

Volume 56, Issue 15, October 2012, Pages 3531-3547

Alessio Botta | Alberto Dainotti | Antonio Pescapé

Internet workload is a mix of many and complex sources. Therefore, its accurate and realistic replication is a difficult and challenging task. Such difficulties are exacerbated by the multidimensional heterogeneity and scale of the current Internet combined with its constant evolution. The study and generation of network workload is a moving target, both in terms of actors (devices, access networks, protocols, applications, services) and in terms of case studies (the interest expands from performance analysis to topics like network neutrality and security). In order to keep up with the new questions that arise and with the consequent new technical cha llenges, networking research needs to continuously update its tools. In this paper, we describe the main properties that a network workload generator should have today, and we present a tool for the generation of realistic network workload that can be used for the study of emerging networking scenarios. In particular, we discuss (i) how it tackles the main issues challenging the representative replication of network workload, and (ii) our design choices and its advanced features that make it suitable to analyze complex and emerging network scenarios. To highlight how our tool advances the state-of-the-art, we finally report some experimental results related to the study of hot topics like (a) broadband Internet performance and network neutrality violations; (b) RFC-based security and performance assessment of home network devices; (c) performance analysis of multimedia communications. © 2012 Elsevier B.V. All rights reserved.

A roadmap for traffic engineering in software defined networks

Volume 71, Issue , October 2014, Pages 1-30

Ian F. Akyildiz | Ahyoung Lee | Pu Wang | Min Luo | Wu Chou

Software Defined Networking (SDN) is an emerging networking paradigm that separates the network control plane from the data forwarding plane with the promise to dramatically improve network resource utilization, simplify network management, reduce operating cost, and promote innovation and evolution. Although traffic engineering techniques have been widely exploited in the past and current data networks, such as ATM networks and IP/MPLS networks, to optimize the performance of communication networks by dynamically analyzing, predicting, and regulating the behavior of the transmitted data, the unique features of SDN require new traffic engineering techniques that exploit the global network view, status, and flow patterns/characteristics available for better traffic control and management. This paper surveys the state-of-the-art in traffic engineering for SDNs, and mainly focuses on four thrusts including flow management, fault tolerance, topology update, and traffic analysis/characterization. In addition, some existing and representative traffic engineering tools from both industry and academia are explained. Moreover, open research issues for the realization of SDN traffic engineering solutions are discussed in detail. © 2014 Elsevier B.V. All rights reserved.

Topology management techniques for tolerating node failures in wireless sensor networks: A survey

Volume 58, Issue 1, January 2014, Pages 254-283

Mohamed Younis | Izzet F. Senturk | Kemal Akkaya | Sookyoung Lee | Fatih Senel

In wireless sensor networks (WSNs) nodes often operate unattended in a collaborative manner to perform some tasks. In many applications, the network is deployed in harsh environments such as battlefield where the nodes are susceptible to damage. In addition, nodes may fail due to energy depletion and breakdown in the onboard electronics. The failure of nodes may leave some areas uncovered and degrade the fidelity of the collected data. However, the most serious consequence is when the network gets partitioned into disjoint segments. Losing network connectivity has a very negative effect on the applications since it prevents data exchange and hinders coordination among some nodes. Therefore, restoring the overall network connectivity is very crucial. Given the resource-constrained setup, the recovery should impose the least overhead and performance impact. This paper focuses on network topology management techniques for tolerating/handling node failures in WSNs. Two broad categories based on reactive and proactive methods have been identified for classifying the existing techniques. Considering these categories, a thorough analysis and comparison of all the recent works have been provided. Finally, the paper is concluded by outlining open issues that warrant additional research. © 2013 Elsevier B.V. All rights reserved.

A survey of routing protocols for smart grid communications

Volume 56, Issue 11, July 2012, Pages 2741-2771

Nico Saputro | Kemal Akkaya | Suleyman Uludag

With the recent initiatives to upgrade the existing power grid to the Smart Grid (SG), there has been a significant interest in the design and development of an efficien t communications infrastructure for connecting different components of the SG. In addition to the currently used underlying networks and protocols, new wired/wireless approaches are being planned for deployment for different components/applications of the SG. Based on the data requirements of the applications, new challenges have arisen at the network layer of the protocol stack with respect to routing and data forwarding. In this paper, we focus on the routing issues in the SG communications infrastructure which consists of different network components, such as Home Area Networks (HANs), Neighborhood Area Networks (NANs) and Wide Area Networks (WANs). We provide a comprehensive survey of the existing routing research and analyze the advantages and disadvantages of the proposed protocols with respect different applications areas. We also identify the future research issues that are yet to be addressed with respect to the applications and network components. This survey is the first to identify routing design issues for the SG and categorize the proposed routing protocols from the SG applications perspective. We believe that this work will be valuable for the utilities and other energy companies whose target is to develop and deploy a specific SG application that may span different network components. In addition, this work will provide valuable insights for the newcomers who would like to pursue routing related research in the SG domain. © 2012 Elsevier B.V. All rights reserved.

A survey on routing algorithms for wireless Ad-Hoc and mesh networks

Volume 56, Issue 2, February 2012, Pages 940-965

Eiman Alotaibi | Biswanath Mukherjee

Wireless networking technology is evolving as an inexpensive alternative for building federated and community networks (relative to the traditional wired networking approach). Besides its cost-effectiveness, a wireless network brings operational efficiencies, namely mobility and untethered convenience to the end user. A wireless network can operate in both the "Ad-Hoc" mode, where users are self-managed, and the "Infrastructure" mode, where an authority manages the network with some Infrastructure such as fixed wireless routers, base stations, access points, etc. An Ad-Hoc network generally supports multi-hopping, where a data packet may travel over multiple hops to reach its destination. Among the Infrastructure-based networks, a Wireless Mesh Network (with a set of wireless routers located at strategic points to provide overall network connectivity) also provides the flexibility of multi-hopping. Therefore, how to route packets efficiently in wireless networks is a very important problem. A variety of wireless routing solutions have been proposed in the literature. This paper presents a survey of the routing algorithms proposed for wireless networks. Unlike routing in a wired network, wireless routing introduces new paradigms and challenges such as interference from other transmissions, varying channel characteristics, etc. In a wireless network, routing algorithms are classified into various categories such as Geographical, Geo-casting, Hierarchical, Multi-path, Power-aware, and Hybrid routing algorithms. Due to the large number of surveys that study different routing-algorithm categories, we select a limited but representative number of these surveys to be reviewed in our work. This survey offers a comprehensive review of these categories of routing algorithms. In the early stages of development of wireless networks, basic routing algorithms, such as Dynamic Source Routing (DSR) and Ad-Hoc On-demand Distance Vector (AODV) routing, were designed to control traffic on the network. However, it was found that applying these basic routing algorithms directly on wireless networks could lead to some issues such as large area of flooding, Greedy Forwarding empty set of neighbors, flat addressing, widely-distributed information, large power consumption, interference, and load-balancing problems. Therefore, a number of routing algorithms have been proposed as extensions to these basic routing algorithms to enhance their performance in wireless networks. Hence, we study the features of routing algorithms, which are compatible with the wireless environment and which can overcome these problems. © 2011 Published by Elsevier B.V.

SmartSantander: IoT experimentation over a smart city testbed

Volume 61, Issue , March 2014, Pages 217-238

Luis Sanchez | Luis Muñoz | Jose Antonio Galache | Pablo Sotres | Juan R. Santana | Veronica Gutierrez | Rajiv Ramdhany | Alex Gluhak | Srdjan Krco | Evangelos Theodoridis | Dennis Pfisterer

This paper describes the deployment and experimentation architecture of the Internet of Things experimentation facility being deployed at Santander city. The facility is implemented within the SmartSantander project, one of the projects of the Future Internet Research and Experimentation initiative of the European Commission and represents a unique in the world city-scale experimental research facility. Additionally, this facility supports typical applications and services of a smart city. Tangible results are expected to influence the definition and specification of Future Internet architecture design from viewpoints of Internet of Things and Internet of Services. The facility comprises a large number of Internet of Things devices deployed in several urban scenarios which will be federated into a single testbed. In this paper the deployment being carried out at the main location, namely Santander city, is described. Besides presenting the current deployment, in this article the main insights in terms of the architectural design of a large-scale IoT testbed are presented as well. Furthermore, solutions adopted for implementation of the different components addressing the required testbed functionalities are also sketched out. The IoT experimentation facility described in this paper is conceived to provide a suitable platform for large scale experimentation and evaluation of IoT concepts under real-life conditions. © 2013 Elsevier B.V. All rights reserved.

VMPlanner: Optimizing virtual machine placement and traffic flow routing to reduce network power costs in cloud data centers

Volume 57, Issue 1, January 2013, Pages 179-196

Weiwei Fang | Xiangmin Liang | Shengxin Li | Luca Chiaraviglio | Naixue Xiong

In recent years, the power costs of cloud data centers have become a practical concern and have attracted significant attention from both industry and academia. Most of the early works on data center energy efficiency have focused on the biggest power consumers (i.e., computer servers and cooling systems), yet without taking the networking part into consideration. However, recent studies have revealed that the network elements consume 10-20% of the total power in the data center, which poses a great challenge to effectively reducing network power cost without adversely affecting overall network performance. Based on the analysis on topology characteristics and traffic patterns of data centers, this paper presents a novel approach, called VMPlanner, for network power reduction in the virtualization-based data centers. The basic idea of VMPlanner is to optimize both virtual machine placement and traffic flow routing so as to turn off as many unneeded network elements as possible for power saving. We formulate the optimization problem, analyze its hardness, and solve it by designing VMPlanner as a stepwise optimization approach with three approximation algorithms. VMPlanner is implemented and evaluated in a simulated environment with traffic traces collected from a data center test-bed, and the experiment results illustrate the efficacy and efficiency of this approach.© 2012 Elsevier B.V. All rights reserved.

Caching in information centric networking: A survey

Volume 57, Issue 16, November 2013, Pages 3128-3141

Guoqiang Zhang | Yang Li | Tao Lin

Internet usage has drastically shifted from host-centric end-to-end communication to receiver-driven content retrieval. In order to adapt to this change, a handful of innovative information/content centric networking (ICN) architectures have recently been proposed. One common and important feature of these architectures is to leverage built-in network caches to improve the transmission efficiency of content dissemination. Compared with traditional Web Caching and CDN Caching, ICN Cache takes on several new characteristics: cache is transparent to applications, cache is ubiquitous, and content to be cached is more ine-grained. These distinguished features pose new challenges to ICN caching technologies. This paper presents a comprehensive survey of state-of-art techniques aiming to address these issues, with particular focus on reducing cache redundancy and improving the availability of cached content. As a new research area, this paper also points out several interesting yet challenging research directions in this subject. © 2013 Elsevier B.V. All rights reserved.

Online social networks: A survey of a global phenomenon

Volume 56, Issue 18, December 2012, Pages 3866-3878

Julia Heidemann | Mathias Klier | Florian Probst

Online social networks became a global phenomenon with enormous social as well as economic impact within a few years. Alone, the most popular online social network, Facebook, counts currently more than 850 million users worldwide. Consequently, online social networks attract a great deal of attention among practitioners as well as researchers. The goal of this article is to provide an overview of online social networks in order to contribute to a better understanding of this worldwide phenomenon. In this context, we address for example the following questions: What are the major functionalities and characteristics of online social networks? What are the users' motives for using them and how did online social networks emerge and develop over time? What is the impact and value of online social networks from a business perspective and what are corresponding challenges and risks?

Communication network requirements for major smart grid applications in HAN, NAN and WAN

Volume 67, Issue , July 2014, Pages 74-88

Murat Kuzlu | Manisa Pipattanasomporn | Saifur Rahman

Since the introduction of the smart grid, accelerated deployment of various smart grid technologies and applications have been experienced. This allows the traditional power grid to become more reliable, resilient, and efficient. Despite such a widespread deployment, it is still not clear which communication technology solutions are the best fit to support grid applications. This is because different smart grid applications have different network requirements - in terms of data payloads, sampling rates, latency and reliability. Based on a variety of smart grid use cases and selected standards, this paper compiles information about different communication network requirements for different smart grid applications, ranging from those used in a Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide-Area Network (WAN). Communication technologies used to support implementation of selected smart grid projects are also discussed. This paper is expected to serve as a comprehensive database of technology requirements and best practices for use by communication engineers when designing a smart grid network. © 2014 Elsevier B.V. All rights reserved.

Dynamic routing and spectrum (re)allocation in future flexgrid optical networks

Volume 56, Issue 12, August 2012, Pages 2869-2883

Alberto Castro | Luis Velasco | Marc Ruiz | Mirosław Klinkowski | Juan Pedro Fernández-Palacios | Davide Careglio

Future flexible-grid elastic optical networks are very promising due to their higher spectrum efficiency and flexibility comparing to the rigid spectrum grid optical networks realized with the traditional wavelength division multiplexing (WDM) technology. The maturity of key system components enabling flexgrid optical networks, such as advanced modulation techniques and multi-granular switching, is already high enough and thus their deployment is expected in the near future. The main feature of such networks is the removal of fix grid-space assignment (in general 50 GHz) to the optical connections independently of the required bandwidth. In fact, the available optical spectrum in flexgrid network is divided into frequency slots of a fixed spectrum width and an optical connection can be allocated into the number of slots that better matches the actual bandwidth of the connection demand. Nonetheless, such allocation must satisfy two constraints, i.e. the slots must be (i) contiguous in the spectrum domain and (ii) continuous along the links on the routing path. These constraints result in a need for dedicated Routing and Spectrum Allocation (RSA) algorithms able to operate under dynamic traffic conditions. From the network design perspective, an important issue is the selection of the frequency slot width which may have an impact on the network performance. Last but not least, network dynamicity entails spectrum fragmentation, which significantly reduces the network performance. In this paper we address these topics and, in particular: (1) we present an RSA algorithm to be used in dynamic network scenarios, (2) we study the optimal slot width as a function of the foreseen traffic to be served, and (3) we propose an algorithm to reallocate already established optical connections so that to make room in the spectrum for the new ones. Exhaustive simulation results reveal that the proposed approach improves the blocking probability performance in flexgrid optical networks. © 2012 Elsevier B.V. All rights reserved.

Botnets: A survey

Volume 57, Issue 2, February 2013, Pages 378-403

Sérgio S.C. Silva | Rodrigo M.P. Silva | Raquel C.G. Pinto | Ronaldo M. Salles

Botnets, which are networks formed by malware-compromised machines, have become a serious threat to the Internet. Such networks have been created to conduct large-scale illegal activities, even jeopardizing the operation of private and public services in several countries around the world. Although research on the topic of botnets is relatively new, it has been the subject of increasing interest in recent years and has spawned a growing number of publications. However, existing studies remain somewhat limited in scope and do not generally include recent research and developments. This paper presents a comprehensive review that broadly discusses the botnet problem, briefly summarizes the previously published studies and supplements these with a wide ranging discussion of recent works and solution proposals spanning the entire botnet research field. This paper also presents and discusses a list of the prominent and persistent research problems that remain open. © 2012 Elsevier B.V. All rights reserved.

Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments

Volume 62, Issue , April 2014, Pages 122-136

K. Giotis | C. Argyropoulos | G. Androulidakis | D. Kalogeras | V. Maglaris

Software Defined Networks (SDNs) based on the OpenFlow (OF) protocol export control-plane programmability of switched substrates. As a result, rich functionality in traffic management, load balancing, routing, firewall configuration, etc. that may pertain to specific flows they control, may be easily developed. In this paper we extend these functionalities with an efficient and scalable mechanism for performing anomaly detection and mitigation in SDN architectures. Flow statistics may reveal anomalies triggered by large scale malicious events (typically massive Distributed Denial of Service attacks) and subsequently assist networked resource owners/operators to raise mitigation policies against these threats. First, we demonstrate that OF statistics collection and processing overloads the centralized control plane, introducing scalability issues. Second, we propose a modular architecture for the separation of the data collection process from the SDN control plane with the employment of sFlow monitoring data. We then report experimental results that compare its performance against native OF approaches that use standard flow table statistics. Both alternatives are evaluated using an entropy-based method on high volume real network traffic data collected from a university campus network. The packet traces were fed to hardware and software OF devices in order to assess flow-based data-gathering and related anomaly detection options. We subsequently present experimental results that demonstrate the effectiveness of the proposed sFlow-based mechanism compared to the native OF approach, in terms of overhead imposed on usage of system resources. Finally, we conclude by demonstrating that once a network anomaly is detected and identified, the OF protocol can effectively mitigate it via flow table modifications. © 2013 Elsevier B.V. All rights reserved.

A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network

Volume 57, Issue 3, February 2013, Pages 825-845

Reduan H. Khan | Jamil Y. Khan

A robust communication infrastructure is the touchstone of a smart grid that differentiates it from the conventional electrical grid by transforming it into an intelligent and adaptive energy delivery network. To cope with the rising penetration of renewable energy sources and expected widespread adoption of electric vehicles, the future smart grid needs to implement efficient monitoring and control technologies to improve its operational efficiency. However, the legacy communication infrastructures in the existing grid are quite insufficient, if not incapable of meeting the diverse communication requirements of the smart grid. Therefore, utilities from all over the world are now facing the key challenge of finding the most appropriate technology that can satisfy their future communication needs. In order to properly assess the vast landscape of available communication technologies, architectures and protocols, it is very important to acquire detailed knowledge about the current and prospective applications of the smart grid. With a view to addressing this critical issue, this paper offers an in depth review on the application characteristics and traffic requirements of several emerging smart grid applications and highlights some of the key research challenges present in this arena. © 2012 Elsevier B.V. All rights reserved.

RPL in a nutshell: A survey

Volume 56, Issue 14, September 2012, Pages 3163-3178

Olfa Gaddour | Anis Koubâa

IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is a routing protocol specifically designed for Low power and Lossy Networks (LLN) compliant with the 6LoWPAN protocol. It currently shows up as an RFC proposed by the IETF ROLL working group. However, RPL has gained a lot of maturity and is attracting increasing interest in the research community. The absence of surveys about RPL motivates us to write this paper, with the objective to provide a quick introduction to RPL. In addition, we present the most relevant research efforts made around RPL routing protocol that pertain to its performance evaluation, implementation, experimentation, deployment and improvement. We also present an experimental performance evaluation of RPL for different network settings to understand the impact of the protocol attributes on the network behavior, namely in terms of convergence time, energy, packet loss and packet delay. Finally, we point out open research challenges on the RPL design. We believe that this survey will pave the way for interested researchers to understand its behavior and contributes for further relevant research works. © 2012 Elsevier B.V. All rights reserved.

Virtual network embedding through topology awareness and optimization

Volume 56, Issue 6, April 2012, Pages 1797-1813

Xiang Cheng | Sen Su | Zhongbao Zhang | Kai Shuang | Fangchun Yang | Yan Luo | Jie Wang

Embedding a sequence of virtual networks (VNs) into a given physical network substrate to accommodate as many VN requests as possible is known to be NP-hard. This paper presents a new approach to studying this problem. In particular, we devise a topology-aware measure on node resources based on random walks and use it to rank a node's resources and topological attributes. We then devise a greedy algorithm that matches nodes in the VN to nodes in the substrate network according to node ranks. In most situations there exist multiple embedding solutions, and so we want to find the best embedding that increases the possibility of accepting future VN requests and optimizes the revenue for the provider of the substrate network. We present an integer linear programming formulation for this optimization problem when path splitting is not allowed. We then devise a fast-convergent discrete Particle Swarm Optimization algorithm to approximate this problem. Extensive simulation results show that our algorithms produce near optimal solutions and significantly outperform existing algorithms in terms of the ratio of the long-term average revenue over the VN request acceptance. © 2012 Elsevier B.V. All rights reserved.

Reliability in wireless sensor networks: A survey and challenges ahead

Volume 79, Issue , March 2015, Pages 166-187

Muhammad Adeel Mahmood | Winston K.G. Seah | Ian Welch

© 2015 Elsevier B.V. All rights reserved. Ensuring energy efficient and reliable transport of data in resource constrained Wireless Sensor Networks (WSNs) is one of the primary concerns to achieve a high degree of efficiency in monitoring and control systems. The two techniques typically used in WSNs to achieve reliability are either retransmission or redundancy. Most of the existing research focuses on traditional retransmission-based reliability, where reliable transmission of data packets is ensured in terms of recovering the lost packets by retransmitting them. This might result in additional transmission overhead that not only wastes sensors' limited energy resources but also makes the network congested and in turn affects the reliable transmission of data. On the other hand, employing redundancy to achieve reliability in WSNs has received comparatively lesser emphasis by the research community [35] and this area warrants further investigation. In redundancy-based reliability mechanisms, a bit loss within a packet can be recovered by utilizing some form of coding schemes. This ability to correct the lost or corrupted bits within a packet would significantly reduce the transmission overhead caused by the retransmission of the entire packet. Both retransmission and redundancy can either be performed on a hop-by-hop or an end-to-end basis. Hop-by-hop method allows the intermediate nodes to perform retransmission or redundancy. On the other hand, in the end-to-end approach, retransmission or redundancy is performed only at the source and the

destination nodes. However, a hybrid mechanism with an efficient combination of these retransmission and redundancy techniques in order to achieve reliability has so far been neglected by the existing research. Depending on the nature of the application, it is also important to define the amount of data required to ensure reliability. This introduces the concept of packet or event level reliability. Packet reliability requires all the packets from all the relevant sensor nodes to reach the sink, whereas event reliability ensures that the sink only gets enough information about a certain event happening. Thus retransmission or redundancy techniques using hop-by-hop or end-to-end mechanisms aim to achieve either packet or event level reliability. This paper presents a survey on reliability protocols in WSNs. We review several reliability schemes based on retransmission and redundancy techniques using different combinations of packet or event reliability in terms of recovering the lost data using hop-by-hop or end-to-end mechanisms. We further analyze these schemes by investigating the most suitable combination of these techniques, methods and required reliability level in order to provide energy efficient reliability mechanism for resource constrained WSNs. This paper also proposes a 3D reference model for classifying research in WSN reliability, which will be used to perform in-depth analysis of the unexplored areas.

Computer Networks

Readers
View Articles
Volume/ Issue Alert

Authors
Author Information Pack
Submit Your Paper
Track Your Paper
Early Career Resources
Webshop
Customer Service

Librarians
Ordering Information and Dispatch Dates
Abstracting/ Indexing

Editors
Publishing Ethics Resource Kit
Support
Guest Editors

Reviewers
Reviewer Guidelines
Log in as Reviewer

Advertisers Media Information

Societies

Advertising - Careers - Feedback - Site map - Terms and Conditions - Privacy Policy