



# S&T IN-DEPTH

THE LATEST IN SCIENCE AND TECHNOLOGY RESEARCH LITERATURE

## FEATURE TOPIC: INTERNET OF THINGS



## TABLE OF CONTENTS

Graphic courtesy of Phys.org

### REVIEW ARTICLES

- Cyber-physical-social-thinking space based science and technology framework for the Internet of Things (China) 2015
- The internet of things: a survey (England) 2015
- Internet of Things for Enterprise Systems of Modern Manufacturing (USA) 2014
- The Internet of Things - The future or the end of mechatronics (Scotland) 2015
- Internet of Things: Objectives and Scientific Challenges (China) 2011
- The Internet of Things vision: Key features, applications and open issues (Italy) 2014
- Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues (Portugal) 2015
- Security, privacy and trust in Internet of Things: The road ahead (Italy) 2015
- A Survey on Human-in-the-Loop Applications Towards an Internet of All (Portugal) 2015

### IoT APPLICATIONS

- Attack-Resistant Trust Management Model Based on Beta Function for Distributed Routing in Internet of Things (China) 2012
- Cloud infrastructure for ubiquitous M2M and IoT environment mobile application (South Korea) 2015
- High performance simulation technology in the Internet of Things (China) 2015
- How the Internet of things technology enhances emergency response operations (England) 2013
- The Internet of Nano-Things (USA) 2010

- Internet of Things in Industries: A Survey (China) 2014
- A Password-Based Secure Communication Scheme in Battlefields for Internet of Things (China) 2011

### IoT DATA MANAGEMENT

- Data Management for the Internet of Things: Design Primitives and Solution (Egypt) 2013
- A Dynamic Processing System for Sensor Data in IoT (China) 2015
- Increasing base station anonymity using distributed beamforming (USA) 2015
- An Intelligent Self-Organization Scheme for the Internet of Things (China) 2013
- An Internet of Things Approach for Managing Smart Services Provided by Wearable Devices (Spain) 2013
- An IoT-Oriented Data Storage Framework in Cloud Computing Platform (China) 2014
- IoT sensing framework with inter-cloud computing capability in vehicular networking (China) 2014
- A lightweight attribute-based encryption scheme for the Internet of Things (China) 2015
- Modeling IoT-Based Solutions Using Human-Centric Wireless Sensor Networks (Chile) 2014
- A secure and scalable storage system for aggregate data in IoT (USA) 2015

### IoT INFRASTRUCTURE

- Advancements of Data Anomaly Detection Research in Wireless Sensor Networks: A Survey and Open Issues (Malaysia) 2013
- Assessing the security of internet-connected critical infrastructures (Germany) 2014

- [A Distributed Cluster Computing Energy-Efficient Routing Scheme for Internet of Things Systems \(Taiwan\) 2015](#)
- [Extending the Internet of Things to the Future Internet through IPv6 support \(England\) 2014](#)
- [Fast Release/Capture Sampling in Large-Scale Sensor Networks \(China\) 2012](#)
- [Network-layer security for the Internet of Things using TinyOS and BLIP \(Portugal\) 2014](#)
- [A potential weakness in RFID-based Internet-of-things systems \(Turkey\) 2015](#)
- [Practical Swarm Optimization based Fault-Tolerance Algorithm for the Internet of Things \(China\) 2014](#)
- [SDN: Evolution and Opportunities in the Development IoT Applications \(Spain\) 2014](#)
- [Untraceable Sensor Movement in Distributed IoT Infrastructure \(Taiwan\) 2015](#)
- [Design of a Distributed Personal Information Access Control Scheme for Secure Integrated Payment in NFC \(South Korea\) 2015](#)
- [Directed Path Based Authentication Scheme for the Internet of Things \(China\) 2012](#)
- [An Effective Differential Fault Analysis on the Serpent Cryptosystem in the Internet of Things \(China\) 2014](#)
- [Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure \(India\) 2015](#)
- [A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things \(South Korea\) 2014](#)
- [Modeling of Malicious Code Propagations in Internet of Things \(China\) 2011](#)
- [A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography \(Algeria\) 2015](#)
- [Probabilistic yoking proofs for large scale IoT systems \(Spain\) 2015](#)
- [Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey \(Portugal\) 2015](#)
- [Security of the Internet of Things: perspectives and challenges \(China\) 2014](#)
- [Survey on secure communication protocols for the Internet of Things \(France\) 2015](#)

#### IoT SECURITY

- [Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things \(China\) 2015](#)
- [Autonomic schemes for threat mitigation in Internet of Things \(Malaysia\) 2015](#)
- [Big Data Privacy in the Internet of Things Era \(the Netherlands\) 2015](#)
- [Context-aware usage control for web of things \(China\) 2014](#)
- [Defending Internet of Things against Exploits \(Brazil\) 2015](#)

## Review Articles

### Cyber-physical-social-thinking space based science and technology framework for the Internet of Things (China) 2015

Author(s): Ning, HS (Ning HuanSheng); Liu, H (Liu Hong)

Source: SCIENCE CHINA-INFORMATION SCIENCES Volume: 58 Issue: 3 Article Number: 031102 DOI: 10.1007/s11432-014-5209-2 Published: MAR 2015

ABSTRACT: The Internet of Things (IoT) as an emerging network paradigm is bringing the next scientific and technological revolution for ubiquitous things' interactions in cyber-physical-social spaces. The IoT influences the current science and technology system by enabling its relatively stable interrelations for an inevitable architecture reconfiguration. In this paper, we aim to explore an updated science and technology framework for the IoT. Particularly, a novel cyber-physical-social-thinking (CPST) space is established by involving an attractive concept of the Internet of Thinking (IoTk), and a science and technology framework is accordingly proposed referring to both scientific aspect (i.e., cyber-physical, social, and noetic sciences) and technological aspect (i.e., fundamental, physical, cyber, and social technologies). According to the perspective of the traditional Chinese culture, we explain the established science and technology framework, in which the "Five Elements" (i.e., wood, fire, earth, metal, and water) have common properties with the restructured cyber-physical science in the IoT. Moreover, we introduce a scenario of smart city to identify the technological aspect in the IoT, and discuss the key enabling technologies, including resource management, energy management, data management, session management, security and privacy, loop control, space-time consistency, nanotechnology, and quantum technology. It turns out that the established science and technology framework will launch an innovation for academia and industry communities.

Author affiliation: [Ning HuanSheng] Univ Sci & Technol Beijing, Sch Comp & Commun Engn, Beijing 100083, Peoples R China. [Liu Hong] RUN Technol Co Ltd Beijing, Engn Lab, Beijing 100192, Peoples R China. ninghuansheng@ustb.edu.cn

Times Cited: 0

Number of references: 26

Tags: IoT Review article, Internet of Things

### The internet of things: a survey (England) 2015

Author(s): Li, SC (Li, Shancang); Xu, LD (Xu, Li Da); Zhao, SS (Zhao, Shanshan)

Source: INFORMATION SYSTEMS FRONTIERS Volume: 17 Issue: 2 Special Issue: SI Pages: 243-259 DOI: 10.1007/s10796-014-9492-7 Published: APR 2015

ABSTRACT: In recent year, the Internet of Things (IoT) has drawn significant research attention. IoT is considered as a part of the Internet of the future and will comprise billions of intelligent communicating 'things'. The future of the Internet will consist of heterogeneously connected devices that will further extend the borders of the world with physical entities and virtual components. The Internet of Things (IoT) will empower the connected things with new capabilities. In this survey, the definitions, architecture, fundamental technologies, and applications of IoT are systematically reviewed. Firstly, various definitions of IoT are introduced; secondly, emerging techniques for the implementation of IoT are discussed; thirdly, some open issues related to the IoT applications are explored; finally, the major challenges which need addressing by the research community and corresponding potential solutions are investigated.

Author affiliation: [Li, Shancang] Univ Bristol, Fac Engn, Clifton BS8 1UB, England.

[Xu, Li Da] Old Dominion Univ, Dept Informat Technol & Decis Sci, Norfolk, VA 23529 USA.

[Zhao, Shanshan] Univ West Scotland, Sch Comp, Paisley PA1 2BE, Renfrew, Scotland.

Reprint Address: Xu, LD (reprint author), Old Dominion Univ, Dept Informat Technol & Decis Sci, Norfolk, VA 23529 USA. shancang.li@bristol.ac.uk; lxu@odu.edu; sszhao.uk@gmail.com

Times Cited: 1

Number of references: 93

Tags: IoT Review article, Internet of Things

### Internet of Things for Enterprise Systems of Modern Manufacturing (USA) 2014

Author(s): Bi, ZM (Bi, Zhuming); Xu, LD (Xu, Li Da); Wang, CG (Wang, Chengen)

Source: IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS Volume: 10 Issue: 2 Pages: 1537-1546 DOI: 10.1109/TII.2014.2300338 Published: MAY 2014

ABSTRACT: Design and operation of a manufacturing enterprise involve numerous types of decision-making at various levels and domains. A complex system has a large number of design variables and decision-making requires real-time data collected from machines, processes, and business environments. Enterprise systems (ESs) are used to support data acquisition, communication,

and all decision-making activities. Therefore, information technology (IT) infrastructure for data acquisition and sharing affects the performance of an ES greatly. Our objective is to investigate the impact of emerging Internet of Things (IoT) on ESs in modern manufacturing. To achieve this objective, the evolution of manufacturing system paradigms is discussed to identify the requirements of decision support systems in dynamic and distributed environments; recent advances in IT are overviewed and associated with next-generation manufacturing paradigms; and the relation of IT infrastructure and ESs is explored to identify the technological gaps in adopting IoT as an IT infrastructure of ESs. The future research directions in this area are discussed.

*Author affiliation: [Bi, Zhuming] Indiana Univ Purdue Univ, Dept Engn, Ft Wayne, IN 46805 USA.*

*[Xu, Li Da] Chinese Acad Sci, Inst Comp Technol, Beijing 100190, Peoples R China.*

*[Xu, Li Da] Shanghai Jiao Tong Univ, Shanghai 200240, Peoples R China.*

*[Xu, Li Da] Univ Sci & Technol China, Hefei 230026, Peoples R China.*

*[Xu, Li Da] Old Dominion Univ, Norfolk, VA 23529 USA.*

*[Wang, Chengen] Northeastern Univ, State Key Lab Synthet Automat Proc Ind, Shenyang 110819, Peoples R China.*

*Reprint Address: Bi, ZM (reprint author), Indiana Univ Purdue Univ, Dept Engn, Ft Wayne, IN 46805 USA.*

*biz@ipfw.edu; wangc@mail.neu.edu.cn*

**Times Cited: 13**

**Number of references: 98**

*Tags: IoT Review article, IoT Applications - Manufacturing, Internet of Things*

### **The Internet of Things - The future or the end of mechatronics (Scotland) 2015**

*Author(s): Bradley, D (Bradley, David); Russell, D (Russell, David); Ferguson, I (Ferguson, Ian); Isaacs, J (Isaacs, John); MacLeod, A (MacLeod, Allan); White, R (White, Roger)*

**Source: MECHATRONICS Volume: 27 Pages: 57-74 DOI: 10.1109/TII.2014.2300338 Published: APR 2015**

**ABSTRACT:** The advent and increasing implementation of user configured and user oriented systems structured around the use of cloud configured information and the Internet of Things is presenting a new range and class of challenges to the underlying concepts of integration and transfer of functionality around which mechatronics is structured. It is suggested that the ways in which system designers and educators in particular respond to and manage these changes and challenges is going to have a significant impact on the way in which both the Internet of Things and mechatronics develop over time. The paper places the relationship between the Internet of Things and mechatronics into perspective and considers the issues and challenges facing systems designers and implementers in relation to managing the dynamics of the changes required. (C) 2015 Elsevier Ltd. All rights reserved.

*Author affiliation: [Bradley, David; Ferguson, Ian; MacLeod, Allan] Abertay Univ, Dundee DD1 1HG, Scotland.*

*[Russell, David] Penn State Great Valley, Malvern, PA 19355 USA.*

*[Isaacs, John] Robert Gordon Univ, Aberdeen AB10 7QB, Scotland.*

*[White, Roger] RC2 Inc, Ridgeway, ON, Canada.*

*Reprint Address: Bradley, D (reprint author), Abertay Univ, Bell St, Dundee DD1 1HG, Scotland.*

*dabonipad@gmail.com*

**Times Cited: 0**

**Number of references: 166**

*Tags: IoT Review article, Internet of Things*

### **Internet of Things: Objectives and Scientific Challenges (China) 2011**

*Author(s): Ma, HD (Ma, Hua-Dong)*

**Source: JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY Volume: 26 Issue: 6 Pages: 919-924 DOI: 10.1007/s11390-011-1189-5 Published: NOV 2011**

**ABSTRACT:** The Internet of Things (IoT) is aimed at enabling the interconnection and integration of the physical world and the cyber space. It represents the trend of future networking, and leads the third wave of the IT industry revolution. In this article, we first introduce some background and related technologies of IoT and discuss the concepts and objectives of IoT. Then, we present the challenges and key scientific problems involved in IoT development. Moreover, we introduce the current research project supported by the National Basic Research Program of China (973 Program). Finally, we outline future research directions.

*Author affiliation: Beijing Univ Posts & Telecommun, Sch Comp Sci, Beijing Key Lab Intelligent Telecommun Software &, Beijing 100876, Peoples R China.*

*Reprint Address: Ma, HD (reprint author), Beijing Univ Posts & Telecommun, Sch Comp Sci, Beijing Key Lab Intelligent Telecommun Software &, Beijing 100876, Peoples R China.*

*mhd@bupt.edu.cn*

**Times Cited: 22**

**Number of references: 9**

*Tags: IoT Review article, Internet of Things*

## [The Internet of Things vision: Key features, applications and open issues \(Italy\) 2014](#)

Author(s): Borgia, E (Borgia, Eleonora)

Source: COMPUTER COMMUNICATIONS Volume: 54 Pages: 1-31 DOI: 10.1016/j.comcom.2014.09.008 Published: DEC 1 2014

ABSTRACT: The Internet of Things (IoT) is a new paradigm that combines aspects and technologies coming from different approaches. Ubiquitous computing, pervasive computing, Internet Protocol, sensing technologies, communication technologies, and embedded devices are merged together in order to form a system where the real and digital worlds meet and are continuously in symbiotic interaction. The smart object is the building block of the IoT vision. By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and interact/control the physical world, but also to be interconnected, to each other, through Internet to exchange data and information. The expected huge number of interconnected devices and the significant amount of available data open new opportunities to create services that will bring tangible benefits to the society, environment, economy and individual citizens. In this paper we present the key features and the driver technologies of IoT. In addition to identifying the application scenarios and the correspondent potential applications, we focus on research challenges and open issues to be faced for the IoT realization in the real world. (C) 2014 Elsevier B.V. All rights reserved.

Author affiliation: CNR, Inst Informat & Telemat, Italian Natl Res Council, I-56124 Pisa, Italy.

Reprint Address: Borgia, E (reprint author), CNR, Inst Informat & Telemat, Italian Natl Res Council, Via G Moruzzi 1, I-56124 Pisa, Italy.

eleonora.borgia@iit.cnr.it

Times Cited: 0

Number of references: 313

Tags: IoT Review article, Internet of Things

## [Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues \(Portugal\) 2015](#)

Author(s): Granjal, J (Granjal, Jorge); Monteiro, E (Monteiro, Edmundo); Silva, JS (Silva, Jorge Sa)

Source: IEEE COMMUNICATIONS SURVEYS AND TUTORIALS Volume: 17 Issue: 3 Pages: 1294-1312 DOI: 10.1109/COMST.2015.2388550 Published: 2015

ABSTRACT: The Internet of Things (IoT) introduces a vision of a future Internet where users, computing systems, and everyday objects possessing sensing and actuating capabilities cooperate with unprecedented convenience and economical benefits. As with the current Internet architecture, IP-based communication protocols will play a key role in enabling the ubiquitous connectivity of devices in the context of IoT applications. Such communication technologies are being developed in line with the constraints of the sensing platforms likely to be employed by IoT applications, forming a communications stack able to provide the required power-efficiency, reliability, and Internet connectivity. As security will be a fundamental enabling factor of most IoT applications, mechanisms must also be designed to protect communications enabled by such technologies. This survey analyzes existing protocols and mechanisms to secure communications in the IoT, as well as open research issues. We analyze how existing approaches ensure fundamental security requirements and protect communications on the IoT, together with the open challenges and strategies for future research work in the area. This is, as far as our knowledge goes, the first survey with such goals.

Author affiliation: [Granjal, Jorge; Monteiro, Edmundo; Silva, Jorge Sa] Univ Coimbra, P-3000370 Coimbra, Portugal.

Reprint Address: Granjal, J (reprint author), Univ Coimbra, P-3000370 Coimbra, Portugal.

jgranjal@dei.uc.pt; edmundo@dei.uc.pt; sasilva@dei.uc.pt

Times Cited: 0

Number of references: 85

Tags: IoT review article, IoT Security, Internet of Things

## [Security, privacy and trust in Internet of Things: The road ahead \(Italy\) 2015](#)

Author(s): Sicari, S (Sicari, S.); Rizzardi, A (Rizzardi, A.); Grieco, LA (Grieco, L. A.); Coen-Porisini, A (Coen-Porisini, A.)

Source: COMPUTER NETWORKS Volume: 76 Pages: 146-164 DOI: 10.1016/j.comnet.2014.11.008 Published: JAN 15 2015

ABSTRACT: 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. (C) 2014 Elsevier B.V. All rights reserved.

*Author affiliation:* [Sicari, S.; Rizzardi, A.; Coen-Porisini, A.] Univ Insubria, Dep Theoret & Appl Sci, DISTA, I-21100 Varese, Italy. [Grieco, L. A.] Politecn Bari, Dep Elect & Informat Engn, DEI, I-70125 Bari, Italy.

*Reprint Address:* Sicari, S (reprint author), Univ Insubria, Dep Theoret & Appl Sci, DISTA, V Mazzini 5, I-21100 Varese, Italy. [sabrina.sicari@uninsubria.it](mailto:sabrina.sicari@uninsubria.it); [alessandra.rizzardi@uninsubria.it](mailto:alessandra.rizzardi@uninsubria.it); [a.grieco@poliba.it](mailto:a.grieco@poliba.it); [alberto.coenporisini@uninsubria.it](mailto:alberto.coenporisini@uninsubria.it)

Times Cited: 1

Number of references: 130

Tags: IoT review article, IoT Security, Internet of Things

## [A Survey on Human-in-the-Loop Applications Towards an Internet of All \(Portugal\) 2015](#)

*Author(s):* Nunes, DS (Nunes, David Sousa); Zhang, P (Zhang, Pei); Silva, JS (Silva, Jorge Sa)

Source: IEEE COMMUNICATIONS SURVEYS AND TUTORIALS Volume: 17 Issue: 2 Pages: 944-965 DOI: 10.1109/COMST.2015.2398816 Published: 2015

ABSTRACT: Our tools and appliances are becoming increasingly more intelligent and interconnected, giving birth to an “Internet of Things” that can be used to support new types of cyber-physical systems (CPSs). While many CPSs are human-centric applications where humans are an essential part of the system, unfortunately, most of these systems still consider the human as an external and unpredictable element to the control loop. In order for these systems to better serve human needs, future CPSs will need to bolster a closer tie with the human element, through Human-in-the-Loop controls that take into consideration human intents, psychological states, emotions and actions inferred through sensory data. This area is a natural confluence of multidisciplinary focus but currently lacks a general understanding of the underlying requirements, principles and theory. As far as we know, this survey is the first effort towards extending the field’s knowledge through an in-depth research of the state-of-the-art and a critical overview of the current taxonomic efforts in the area of Human-in-the-Loop CPSs. On top of this research, a novel taxonomic exercise focused on the general roles of the human component together with a requirement analysis, are presented.

*Author affiliation:* [Nunes, David Sousa; Silva, Jorge Sa] Univ Coimbra, Dept Informat Engn, P-3030290 Coimbra, Portugal. [Zhang, Pei] Carnegie Mellon Univ, Moffett Field, CA 94035 USA.

*Reprint Address:* Nunes, DS (reprint author), Univ Coimbra, Dept Informat Engn, P-3030290 Coimbra, Portugal. [dsnunes@dei.uc.pt](mailto:dsnunes@dei.uc.pt); [peizhang@cmu.edu](mailto:peizhang@cmu.edu); [sasilva@dei.uc.pt](mailto:sasilva@dei.uc.pt)

Times Cited: 0

Number of references: 108

Tags: IoT Review article, IoT Infrastructure, Internet of Things

## IoT Applications

### [Attack-Resistant Trust Management Model Based on Beta Function for Distributed Routing in Internet of Things \(China\) 2012](#)

*Author(s):* Dong, P (Dong Ping); Guan, JF (Guan Jianfeng); Xue, XP (Xue Xiaoping); Wang, HC (Wang Hongchao)

Source: CHINA COMMUNICATIONS Volume: 9 Issue: 4 Pages: 89-98 Published: APR 2012

ABSTRACT: With the rapid development of Internet of Things (IoT), the issue of trust in distributed routing systems has attracted more research attention. The existing trust management frameworks, however, suffer from some possible attacks in hostile environments, such as false accusation, collusion, on-off, and conflicting behavior. Therefore, more comprehensive models should be proposed to predict the trust level of nodes on potential routes more precisely, and to defeat several kinds of possible attacks. This paper makes an attempt to design an attack-resistant trust management model based on beta function for distributed routing strategy in IoT. Our model can evaluate and propagate reputation in distributed routing systems. We first describe possible attacks on existing systems. Our model is then proposed to establish reliable trust relations between self-organized nodes and defeat possible attacks in distributed routing systems. We also propose a theoretical basis and skeleton of our model. Finally, some performance evaluations and security analyses are provided to show the effectiveness and robustness of our model compared with the existing systems.

*Author affiliation:* [Xue Xiaoping] Tongji Univ, Dept Informat & Commun Engn, Shanghai 201804, Peoples R China.

[Dong Ping; Wang Hongchao] Beijing Jiaotong Univ, Beijing 100044, Peoples R China.

[Guan Jianfeng] Beijing Univ Posts & Telecommun, Beijing 100876, Peoples R China.

*Reprint Address:* Xue, XP (reprint author), Tongji Univ, Dept Informat & Commun Engn, Shanghai 201804, Peoples R China. [pdong@bjtu.edu.cn](mailto:pdong@bjtu.edu.cn); [jfguan@bupt.edu.cn](mailto:jfguan@bupt.edu.cn); [xuexp@tongji.edu.cn](mailto:xuexp@tongji.edu.cn); [05111041@bjtu.edu.cn](mailto:05111041@bjtu.edu.cn)

Times Cited: 2

Number of references: 19

Tags: IoT Applications - Military, Internet of Things

## [Cloud infrastructure for ubiquitous M2M and IoT environment mobile application \(South Korea\) 2015](#)

Author(s): Seo, D (Seo, DongBum); Jeong, CS (Jeong, Chang-Sung); Jeon, YB (Jeon, You-Boo); Lee, KH (Lee, Keun-Ho)

Source: CLUSTER COMPUTING-THE JOURNAL OF NETWORKS SOFTWARE TOOLS AND APPLICATIONS Volume: 18 Issue: 2 Special Issue: SI Pages: 599-608 DOI: 10.1007/s10586-014-0415-7 Published: JUN 2015

ABSTRACT: The demand for ubiquitous mobile application on cloud computing platform is increasing due to the rapid advancement of cloud technology. In this paper, we shall present a new architecture for ubiquitous computing environment on cloud computing platform for mobile application. Our system provides a combined architecture of ubiquitous and cloud computing which supports a powerful framework for mobile applications which requires high performance. It is composed of three layers: cloud service layer (CSL), machine to machine (M2M) service layer (MSL) and ubiquitous service layer. CSL provides an agent based processing platform for executing various distributed models, and offers on-demand VM allocation for dynamic execution of mobile processes. Also, CSL offers cloud infrastructure controller which supports a unified interface for various cloud infrastructure via cloud infrastructure interface so that mobile applications may be launched on any cloud environment. MSL is the development of the M2M and IoT open up all types of service motivated opportunities, sending increased efficiencies, well customer value and improved quality of mobile application environment. Also, we describe a soft-ware mobility model in terms of state transition and performance parameters for response time, dynamic migration, and loss ratio on cloud computing environment for mobile applications, and the experimental results show that the computation intensive cloud infrastructure on ubiquitous environment mobile applications can be executed efficiently.

Author affiliation: [Seo, DongBum; Jeon, You-Boo] Korea Univ, Dept Visual Informat Proc, Seoul 136713, South Korea.

[Jeong, Chang-Sung] Korea Univ, Dept Elect Engn, Seoul 136713, South Korea.

[Lee, Keun-Ho] Baekseok Univ, Div Informat, Cheonan Si 330704, Chungcheongnam, South Korea.

Reprint Address: Jeong, CS (reprint author), Korea Univ, Dept Elect Engn, Seoul 136713, South Korea.

treeline@korea.ac.kr; csjeong@korea.ac.kr; jeonyb@korea.ac.kr; root1004@bu.ac.kr

Times Cited: 0

Number of references: 34

Tags: IoT Applications - Communications, IoT Infrastructure, Internet of Things

## [High performance simulation technology in the Internet of Things \(China\) 2015](#)

Author(s): Liu, BQ (Liu, Buquan)

Source: INTERNATIONAL JOURNAL OF SENSOR NETWORKS Volume: 17 Issue: 3 Pages: 195-202 DOI: 10.1504/IJSNET.2015.068184 Published: 2015

ABSTRACT: The Internet of Things based on sensors is bound to trigger an epoch-making revolution in military affairs. However, the multitudinous sensors increase the processing time of a computer. This makes battlefield simulation get into great trouble. In addition, the outcome of a war is affected by many factors and an excellent battlefield simulation should consider these factors comprehensively. The supercomputer with the capabilities of ultra computation and communication should be applied into this kind of simulation. After introducing the hardware architecture of a high performance simulation supercomputer, this paper presents several techniques in our battlefield simulation software such as its monitoring policy, design principles and scheduling algorithm. These techniques are helpful to monitor the status of the supercomputer with numerous multi-core CPUs and enormous samples of a battlefield programme can be easily deployed and executed in batch. The evaluation conclusion of different samples for the battlefield situation can provide powerful support for the commander.

Author affiliation: Natl Univ Def Technol, Coll Informat Syst & Management, Changsha 410073, Hunan, Peoples R China.

Reprint Address: Liu, BQ (reprint author), Natl Univ Def Technol, Coll Informat Syst & Management, Changsha 410073, Hunan, Peoples R China.

bqliu@nudt.edu.cn

Times Cited: 0

Number of references: 16

Tags: IoT Applications - Military, Internet of Things

## [How the Internet of things technology enhances emergency response operations \(England\) 2013](#)

Author(s): Yang, L (Yang, L.); Yang, SH (Yang, S. H.); Plotnick, L (Plotnick, L.)

Source: TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE Volume: 80 Issue: 9 Pages: 1854-1867 DOI: 10.1016/j.techfore.2012.07.011 Published: NOV 2013

ABSTRACT: The Internet of Things (IoT) is a novel paradigm that connects the pervasive presence around us of a variety of things or objects to the Internet by using wireless/wired technologies to reach desired goals. Since the concept of the IoT was introduced in 2005, we see the deployment of a new generation of networked smart objects with communication, sensory and action

capabilities for numerous applications, mainly in global supply chain management, environment monitoring and other non-stress environments. This paper introduces the IoT technology for use in the emergency management community. Considering the information required for supporting three sequential and distinct rhythms in emergency response operations: mobilization rhythm, preliminary situation assessment rhythm, and intervention rhythm, the paper proposes a modified task-technology fit approach that is used to investigate how the IoT technology can be incorporated into the three rhythms and enhance emergency response operations. The findings from our research support our two hypotheses: H1: IoT technology Fits the identified information requirements; and H2: IoT technology provides added value to emergency response operations in terms of obtaining efficient cooperation, accurate situational awareness, and complete visibility of resources. (C) 2012 Elsevier Inc. All rights reserved.

*Author affiliation: [Yang, L.] Univ Loughborough, Sch Business & Econ, Loughborough LE11 3TU, Leics, England.*

*[Yang, S. H.] Univ Loughborough, Dept Comp Sci, Loughborough LE11 3TU, Leics, England.*

*[Plotnick, L.] Jacksonville State Univ, Jacksonville, AL 36265 USA.*

*Reprint Address: Yang, L (reprint author), Univ Loughborough, Sch Business & Econ, Ashby Rd, Loughborough LE11 3TU, Leics, England.*

*L.Yang@lboro.ac.uk*

**Times Cited: 5**

**Number of references: 79**

*Tags: IoT Applications - Communications, IoT Infrastructure, Internet of Things*

### [The Internet of Nano-Things \(USA\) 2010](#)

*Author(s): Akyildiz, IF (Akyildiz, Ian F.); Jornet, JM (Jornet, Josep Miquel)*

**Source: IEEE WIRELESS COMMUNICATIONS Volume: 17 Issue: 6 Pages: 58-63 DOI: 10.1109/MWC.2010.5675779 Published: DEC 2010**

**ABSTRACT:** Nanotechnology promises new solutions for many applications in the biomedical, industrial and military fields as well as in consumer and industrial goods. The interconnection of nanoscale devices with existing communication networks and ultimately the Internet defines a new networking paradigm that is further referred to as the Internet of Nano-Things. Within this context, this paper discusses the state of the art in electromagnetic communication among nanoscale devices. An in-depth view is provided from the communication and information theoretic perspective, by highlighting the major research challenges in terms of channel modeling, information encoding and protocols for nanonetworks and the Internet of Nano-Things.

*Author affiliation: [Akyildiz, Ian F.; Jornet, Josep Miquel] Georgia Inst Technol, Sch Elect & Comp Engr, Broadband Wireless Networking Lab, Atlanta, GA 30332 USA.*

*Reprint Address: Akyildiz, IF (reprint author), Georgia Inst Technol, Sch Elect & Comp Engr, Broadband Wireless Networking Lab, Atlanta, GA 30332 USA.*

*ian@ece.gatech.edu; jmjornet@ece.gatech.edu*

**Times Cited: 43**

**Number of references: 11**

*Tags: IoT Applications - Military, IoT Infrastructure, Internet of Things*

### [Internet of Things in Industries: A Survey \(China\) 2014](#)

*Author(s): Xu, LD (Xu, Li Da); He, W (He, Wu); Li, SC (Li, Shancang)*

**Source: IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS Volume: 10 Issue: 4 Pages: 2233-2243 DOI: 10.1109/TII.2014.2300753 Published: NOV 2014**

**ABSTRACT:** Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years. In an effort to understand the development of IoT in industries, this paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. A main contribution of this review paper is that it summarizes the current state-of-the-art IoT in industries systematically.

*Author affiliation: [Xu, Li Da] Chinese Acad Sci, Inst Comp Technol, Beijing 100190, Peoples R China.*

*[Xu, Li Da] Shanghai Jiao Tong Univ, Shanghai 200052, Peoples R China.*

*[Xu, Li Da] Univ Sci & Technol China, Hefei 230026, Peoples R China.*

*[Xu, Li Da; He, Wu] Old Dominion Univ, Norfolk, VA 23529 USA.*

*[Li, Shancang] Univ Bristol, Bristol BS8 1TH, Avon, England.*

*Reprint Address: Xu, LD (reprint author), Chinese Acad Sci, Inst Comp Technol, Beijing 100190, Peoples R China.*

*lxu@odu.edu; whe@odu.edu; shancang.li@bristol.ac.uk*

**Times Cited: 17**

**Number of references: 86**

*Tags: IoT Applications - Industry, IoT Infrastructure, Internet of Things*

*continued*

## [A Password-Based Secure Communication Scheme in Battlefields for Internet of Things \(China\) 2011](#)

Author(s): Zhang, H (Zhang Hua); Gao, F (Gao Fei); Wen, QY (Wen Qiaoyan); Jin, ZP (Jin Zhengping)

Source: CHINA COMMUNICATIONS Volume: 8 Issue: 1 Special Issue: SI Pages: 72-78 Published: JAN 2011

ABSTRACT: Mobile Ad hoc NETwork (MANET) is a part of the Internet of Things (IoT). In battlefield communication systems, ground soldiers, tanks, and unmanned aerial vehicles comprise a heterogeneous MANET. In 2006, Byun et al. proposed the first constant-round password-based group key exchange with different passwords for such networks. In 2008, Nam et al. discovered the shortcomings of the scheme, and modified it. But the works only provide the group key. In this paper, we propose a password-based secure communication scheme for the IoT, which could be applied in the battlefield communication systems and support dynamic group, in which the nodes join or leave. By performing the scheme, the nodes in the heterogeneous MANET can realize secure broadcast, secure unicast, and secure direct communication across realms. After the analyses, we demonstrate that the scheme is secure and efficient.

Author affiliation: [Zhang Hua; Gao Fei; Wen Qiaoyan; Jin Zhengping] Beijing Univ Posts & Telecommun, State Key Lab Networking & Switching Technol, Beijing 100876, Peoples R China.

Reprint Address: Zhang, H (reprint author), Beijing Univ Posts & Telecommun, State Key Lab Networking & Switching Technol, Beijing 100876, Peoples R China.

Times Cited: 1

Number of references: 16

Tags: IoT Applications - Military, IoT Infrastructure, Internet of Things

## IoT Data management

### [Data Management for the Internet of Things: Design Primitives and Solution \(Egypt\) 2013](#)

Author(s): Abu-Elkheir, M (Abu-Elkheir, Mervat); Hayajneh, M (Hayajneh, Mohammad); Abu Ali, N (Abu Ali, Najah)

Source: SENSORS Volume: 13 Issue: 11 Pages: 15582-15612 DOI: 10.3390/s131115582 Published: NOV 2013

ABSTRACT: The Internet of Things (IoT) is a networking paradigm where interconnected, smart objects continuously generate data and transmit it over the Internet. Much of the IoT initiatives are geared towards manufacturing low-cost and energy-efficient hardware for these objects, as well as the communication technologies that provide objects interconnectivity. However, the solutions to manage and utilize the massive volume of data produced by these objects are yet to mature. Traditional database management solutions fall short in satisfying the sophisticated application needs of an IoT network that has a truly global-scale. Current solutions for IoT data management address partial aspects of the IoT environment with special focus on sensor networks. In this paper, we survey the data management solutions that are proposed for IoT or subsystems of the IoT. We highlight the distinctive design primitives that we believe should be addressed in an IoT data management solution, and discuss how they are approached by the proposed solutions. We finally propose a data management framework for IoT that takes into consideration the discussed design elements and acts as a seed to a comprehensive IoT data management solution. The framework we propose adapts a federated, data-and sources-centric approach to link the diverse Things with their abundance of data to the potential applications and services that are envisioned for IoT.

Author affiliation: [Abu-Elkheir, Mervat] Mansoura Univ, Fac Comp & Informat Sci, Mansoura 35516, Egypt.

[Hayajneh, Mohammad; Abu Ali, Najah] United Arab Emirates Univ, Coll Informat Technol, Abu Dhabi 17551, U Arab Emirates.

Reprint Address: Abu-Elkheir, M (reprint author), Mansoura Univ, Fac Comp & Informat Sci, Mansoura 35516, Egypt.

mfahmy78@mans.edu.eg; mhayajneh@uaeu.ac.ae; najah@uaeu.ac.ae

Times Cited: 4

Number of references: 60

Tags: IoT Data management, Internet of Things

### [A Dynamic Processing System for Sensor Data in IoT \(China\) 2015](#)

Author(s): Li, MB (Li, Minbo); Liu, YL (Liu, Yanling); Cai, YF (Cai, Yuanfeng)

Source: INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS Article Number: 750452 DOI: 10.1155/2015/750452 Published: 2015

ABSTRACT: With the development of the Internet of Things (IoT for short), innumerable Wireless Sensor Networks (WSNs) are deployed to capture the information of environmental status in the surrounding physical environment. The data from WSNs, called sensor data, are generated in high frequency. Similar to data of other open-loop applications, for example, network monitoring data, sensor data are heterogeneous, redundant, real-time, massive, and streaming. Hence, sensor data cannot be treated as the IoT business data, which brings complexity and difficulty to information sharing in the open-loop environment. This paper proposes a dynamic sensor data processing (SDP) system to capture and process sensor data continuously on the basis of data streaming

*continued*

technology. Particle Swarm Optimization (PSO) algorithm is employed to train threshold dynamically for data compression avoiding redundancy. With the help of rules setting, the proposed SDP is able to detect exception situations. Meanwhile, the storage models in SQL and NOSQL databases are analyzed and compared trying to seek an appropriate type of database for sensor data storage. The experimental results show that our SDP can compress sensor data through dynamically balancing the accuracy and compression rate and the model on NOSQL database has better performance than the model on SQL database.

*Author affiliation: [Li, Minbo; Liu, Yanling; Cai, Yuanfeng] Fudan Univ, Software Sch, Shanghai 201203, Peoples R China.*

*[Li, Minbo] Fudan Univ, Shanghai Key Lab Data Sci, Shanghai 201203, Peoples R China.*

*Reprint Address: Li, MB (reprint author), Fudan Univ, Software Sch, Shanghai 201203, Peoples R China.*

*limb@fudan.edu.cn*

Times Cited: 0

Number of references: 22

Tags: IoT data management, Internet of Things

### **Increasing base station anonymity using distributed beamforming (USA) 2015**

*Author(s): Ward, JR (Ward, Jon R.); Younis, M (Younis, Mohamed)*

Source: AD HOC NETWORKS Volume: 32 Special Issue: SI Pages: 53-80 DOI: 10.1016/j.adhoc.2015.01.001 Published: SEP 2015

ABSTRACT: Advances in wireless communication technologies have enabled the networking of devices, which conventionally operated standalone, to form an Internet of Things (IoT). A typical network architecture consists of a set of data sources that report to a base station (BS), e.g., a data aggregation unit, over multi-hop paths. An example of such a network operation model includes surveillance of an unattended area using wireless sensor nodes, and advanced metering within a smart power grid. The unique role of the BS makes it a natural target for an adversary that desires to achieve the most impactful attack possible against an IoT network. Even if a network employs conventional security mechanisms such as encryption and authentication, an adversary may apply traffic analysis techniques to exploit unique traffic patterns within the network and ultimately identify the BS. The first step to successfully protect the BS from attack is to keep the BS's identity, role, and location anonymous. This paper proposes a novel, cross-layer approach that boosts BS anonymity using distributed beamforming. We demonstrate that the characteristics of distributed beamforming make it extremely effective in improving BS anonymity in a wireless network while minimizing the amount of required communication energy overhead. Through analysis and simulation we demonstrate that the proposed approach is both efficient and effective at countering an adversary that employs evidence theory analysis to locate the BS. (C) 2015 Elsevier B.V. All rights reserved.

*Author affiliation: [Ward, Jon R.; Younis, Mohamed] Univ Maryland, Dept Comp Sci & Elect Engr, Baltimore, MD 21201 USA.*

*Reprint Address: Ward, JR (reprint author), Univ Maryland, Dept Comp Sci & Elect Engr, Baltimore, MD 21201 USA.*

*jward3@umbc.edu; younis@umbc.edu*

Times Cited: 0

Number of references: 48

Tags: IoT Data management, IoT security, Internet of Things

### **An Intelligent Self-Organization Scheme for the Internet of Things (China) 2013**

*Author(s): Ding, YS (Ding, Yongsheng); Jin, YL (Jin, Yanling); Ren, LH (Ren, Lihong); Hao, KR (Hao, Kuangrong)*

Source: IEEE COMPUTATIONAL INTELLIGENCE MAGAZINE Volume: 8 Issue: 3 Pages: 41-53 DOI: 10.1109/MCI.2013.2264251 Published: AUG 2013

ABSTRACT: The Internet of Things (IoT) is emerging as the major trend in shaping the development of the next generation of information networks. The challenges of the enormous, dynamic, incredibly diverse and high complexity of the IoT urgently require novel self-organization scheme because most of the existing distributed self-organization schemes cannot be directly applied to it. In this paper, we propose an intelligent self-organizing scheme (ISOS) for the IoT inspired by the endocrine regulating mechanism. For each node in the network, an autonomous area is established, where the node can effectively interact with its peers and perform self-control according to its own status and dynamic circumstance in a decentralized infrastructure. By introducing the hormone mechanism as the medium for information transmission and data sharing, the nodes can collaborate with each other and work in a cooperative way. Through adjusting the release procedure of the hormones, the ability to effectively detect service randomly generated can also be guaranteed in the probabilistic partially-working IoT. Simulation results verify the performance of the proposed mechanism that entitles the IoT to the ability of maintaining its status in a globally stable status, while effectively discovering the random service requests in a resource-critical configuration. The ISOS would be of great significance for the practical implementation of the IoT.

*Author affiliation: [Ding, Yongsheng; Jin, Yanling; Ren, Lihong; Hao, Kuangrong] Donghua Univ, Shanghai, Peoples R China.*

*Reprint Address: Ding, YS (reprint author), Donghua Univ, Shanghai, Peoples R China.*

Times Cited: 10

Number of references: 33

Tags: *IoT Data management, IoT security, Internet of Things*

### [An Internet of Things Approach for Managing Smart Services Provided by Wearable Devices \(Spain\) 2013](#)

Author(s): *Castillejo, P (Castillejo, Pedro); Martinez, JF (Martinez, Jose-Fernan); Lopez, L (Lopez, Lourdes); Rubio, G (Rubio, Gregorio)*

Source: [INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS](#) Article Number: 190813 DOI: 10.1155/2013/190813 Published: 2013

ABSTRACT: The Internet of Things (IoT) is growing at a fast pace with new devices getting connected all the time. A new emerging group of these devices is the wearable devices, and the wireless sensor networks are a good way to integrate them in the IoT concept and bring new experiences to the daily life activities. In this paper, we present an everyday life application involving a WSN as the base of a novel context-awareness sports scenario, where physiological parameters are measured and sent to the WSN by wearable devices. Applications with several hardware components introduce the problem of heterogeneity in the network. In order to integrate different hardware platforms and to introduce a service-oriented semantic middleware solution into a single application, we propose the use of an enterprise service bus (ESB) as a bridge for guaranteeing interoperability and integration of the different environments, thus introducing a semantic added value needed in the world of IoT-based systems. This approach places all the data acquired (e. g., via internet data access) at application developers disposal, opening the system to new user applications. The user can then access the data through a wide variety of devices (smartphones, tablets, and computers) and operating systems (Android, iOS, Windows, Linux, etc.).

Author affiliation: *[Castillejo, Pedro; Martinez, Jose-Fernan; Lopez, Lourdes; Rubio, Gregorio] Tech Univ Madrid UPM, Next Generat Networks & Serv GRYS Res Grp, Res Ctr Software Technol & Multimedia Syst Sustai, Madrid 28031, Spain.*

Reprint Address: *Castillejo, P (reprint author), Tech Univ Madrid UPM, Next Generat Networks & Serv GRYS Res Grp, Res Ctr Software Technol & Multimedia Syst Sustai, La Arboleda Campus Sur Bldg, Km 7, Madrid 28031, Spain.*

*pcastillejo@diatel.upm.es*

Times Cited: 2

Number of references: 19

Tags: *IoT Data management, Internet of Things*

### [An IoT-Oriented Data Storage Framework in Cloud Computing Platform \(China\) 2014](#)

Author(s): *Jiang, LH (Jiang, Lihong); Xu, LD (Xu, Li Da); Cai, HM (Cai, Hongming); Jiang, ZH (Jiang, Zuhai); Bu, FL (Bu, Fenglin); Xu, BY (Xu, Boyi)*

Source: [IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS](#) Volume: 10 Issue: 2 Pages: 1443-1451 DOI: 10.1109/TII.2014.2306384 Published: MAY 2014

ABSTRACT: The Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of Radio Frequency IDentification (RFID) and wireless sensors devices. Benefiting from RFID and sensor network technology, common physical objects can be connected, and are able to be monitored and managed by a single system. Such a network brings a series of challenges for data storage and processing in a cloud platform. IoT data can be generated quite rapidly, the volume of data can be huge and the types of data can be various. In order to address these potential problems, this paper proposes a data storage framework not only enabling efficient storing of massive IoT data, but also integrating both structured and unstructured data. This data storage framework is able to combine and extend multiple databases and Hadoop to store and manage diverse types of data collected by sensors and RFID readers. In addition, some components are developed to extend the Hadoop to realize a distributed file repository, which is able to process massive unstructured files efficiently. A prototype system based on the proposed framework is also developed to illustrate the framework's effectiveness.

Author affiliation: *[Jiang, Lihong; Cai, Hongming; Jiang, Zuhai; Bu, Fenglin] Shanghai Jiao Tong Univ, Sch Software, Shanghai 200240, Peoples R China.*

*[Xu, Li Da] Chinese Acad Sci, Inst Comp Technol, Beijing, Peoples R China.*

*[Xu, Li Da] Shanghai Jiao Tong Univ, Shanghai 200052, Peoples R China.*

*[Xu, Li Da] Univ Sci & Technol China, Hefei 230026, Peoples R China.*

*[Xu, Li Da] Old Dominion Univ, Norfolk, VA 23529 USA.*

*[Xu, Boyi] Shanghai Jiao Tong Univ, Coll Econ & Management, Shanghai 200052, Peoples R China.*

Reprint Address: *Cai, HM (reprint author), Shanghai Jiao Tong Univ, Sch Software, Shanghai 200240, Peoples R China.*

*hmcai@sjtu.edu.cn; byxu@sjtu.edu.cn*

Times Cited: 4

Number of references: 39

Tags: *IoT data management, Internet of Things*

*continued*

## IoT sensing framework with inter-cloud computing capability in vehicular networking (China) 2014

Author(s): Wan, JF (Wan, Jiafu); Zou, CF (Zou, Caifeng); Zhou, KL (Zhou, Keliang); Lu, RS (Lu, Rongshuang); Li, D (Li, Di)

Source: ELECTRONIC COMMERCE RESEARCH Volume: 14 Issue: 3 Pages: 389-416 DOI: 10.1007/s10660-014-9147-2

Published: NOV 2014

ABSTRACT: In order to improve convenience, efficiency, and safety in vehicular networking applications (VNA), we propose a novel business model based on platform production services (PPS), design an inter-cloud architecture, and then apply this emerging scheme to vehicle maintenance services (VMS). Both internet of things (IoT) sensing framework and inter-cloud computing architecture are the crucial factors in implementing PPS business model. In the proposed scheme, implementation concept, system architecture, and scalable applications are introduced. Then we design IoT sensing framework for VNA, including cloud services and computation level scalability, inter-cloud architecture supporting telematics applications, and telematics application scenarios. After dissecting mobile cloud computing forming mechanism, we carry out the semantic modeling analysis for inter-cloud service model, and then design a VMS event processing flow to allow the management and cooperation among diverse components by means of event manager. The performance evaluation exemplified by VMS is implemented by means of probabilistic methods. The results show that convenience and efficiency increase in VNA as compared to existing schemes.

Author affiliation: [Wan, Jiafu; Li, Di] S China Univ Technol, Sch Mech & Automot Engn, Guangzhou, Guangdong, Peoples R China.

[Zou, Caifeng] Guangdong Jidian Polytech, Coll Informat Engn, Guangzhou, Guangdong, Peoples R China.

[Zhou, Keliang; Lu, Rongshuang] Jiangxi Univ Sci & Technol, Coll Elect Engn & Automat, Ganzhou, Peoples R China.

Reprint Address: Zou, CF (reprint author), Guangdong Jidian Polytech, Coll Informat Engn, Guangzhou, Guangdong, Peoples R China.

jiafu\_wan@ieee.org; caifengzou@gmail.com; nyzkl@sina.com; lrs197908@163.com; itdili@scut.edu.cn

Times Cited: 0

Number of references: 45

Tags: IoT data management, Internet of Things

## A lightweight attribute-based encryption scheme for the Internet of Things (China) 2015

Author(s): Yao, XX (Yao, Xuanxia); Chen, Z (Chen, Zhi); Tian, Y (Tian, Ye)

Source: FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF GRID COMPUTING AND ESCIENCE Volume: 49 Pages: 104-112 DOI: 10.1016/j.future.2014.10.010 Published: AUG 2015

ABSTRACT: Internet of Things (IoT) is an emerging network paradigm, which realizes the interconnections among the ubiquitous things and is the foundation of smart society. Since IoT are always related to user's daily life or work, the privacy and security are of great importance. The pervasive, complex and heterogeneous properties of IoT make its security issues very challenging. In addition, the large number of resources-constraint nodes makes a rigid lightweight requirement for IoT security mechanisms. Presently, the attribute-based encryption (ABE) is a popular solution to achieve secure data transmission, storage and sharing in the distributed environment such as IoT. However, the existing ABE schemes are based on expensive bilinear pairing, which make them not suitable for the resources-constraint IoT applications. In this paper, a lightweight no-pairing ABE scheme based on elliptic curve cryptography (ECC) is proposed to address the security and privacy issues in IoT. The security of the proposed scheme is based on the ECDDH assumption instead of bilinear Diffie-Hellman assumption, and is proved in the attribute based selective-set model. By uniformly determining the criteria and defining the metrics for measuring the communication overhead and computational overhead, the comparison analyses with the existing ABE schemes are made in detail. The results show that the proposed scheme has improved execution efficiency and low communication costs. In addition, the limitations and the improving directions of it are also discussed in detail. (C) 2014 Elsevier B.V. All rights reserved.

Author affiliation: [Yao, Xuanxia; Chen, Zhi] Univ Sci & Technol Beijing, Sch Comp & Commun Engn, Beijing 100083, Peoples R China.

[Tian, Ye] Chinese Acad Sci, Comp Network Informat Ctr, Beijing 100190, Peoples R China.

[Tian, Ye] China Internet Network Informat Ctr, DNSLAB, Beijing 100190, Peoples R China.

Reprint Address: Yao, XX (reprint author), Univ Sci & Technol Beijing, Sch Comp & Commun Engn, Beijing 100083, Peoples R China.

yaoxuanxia@163.com

Times Cited: 1

Number of references: 24

Tags: IoT data management, IoT security, Internet of Things

## [Modeling IoT-Based Solutions Using Human-Centric Wireless Sensor Networks \(Chile\) 2014](#)

Author(s): Monares, A (Monares, Alvaro); Ochoa, SF (Ochoa, Sergio F.); Santos, R (Santos, Rodrigo); Orozco, J (Orozco, Javier); Meseguer, R (Meseguer, Roc)

Source: SENSORS Volume: 14 Issue: 9 Pages: 15687-15713 DOI: 10.3390/s140915687 Published: SEP 2014

ABSTRACT: The Internet of Things (IoT) has inspired solutions that are already available for addressing problems in various application scenarios, such as healthcare, security, emergency support and tourism. However, there is no clear approach to modeling these systems and envisioning their capabilities at the design time. Therefore, the process of designing these systems is ad hoc and its real impact is evaluated once the solution is already implemented, which is risky and expensive. This paper proposes a modeling approach that uses human-centric wireless sensor networks to specify and evaluate models of IoT-based systems at the time of design, avoiding the need to spend time and effort on early implementations of immature designs. It allows designers to focus on the system design, leaving the implementation decisions for a next phase. The article illustrates the usefulness of this proposal through a running example, showing the design of an IoT-based solution to support the first responses during medium-sized or large urban incidents. The case study used in the proposal evaluation is based on a real train crash. The proposed modeling approach can be used to design IoT-based systems for other application scenarios, e. g., to support security operatives or monitor chronic patients in their homes.

Author affiliation: [Monares, Alvaro; Ochoa, Sergio F.] Univ Chile, Dept Comp Sci, Santiago 8370459, Chile.

[Santos, Rodrigo; Orozco, Javier] UNS CONICET, IIIE, Dept Elect Engr & Comp, RA-8000 Bahia Blanca, Buenos Aires, Argentina.

[Meseguer, Roc] Univ Politecn Cataluna, Dept Comp Architecture, ES-08034 Barcelona, Spain.

Reprint Address: Ochoa, SF (reprint author), Univ Chile, Dept Comp Sci, Beauchef 851, Santiago 8370459, Chile.

amonares@dcc.uchile.cl; sochoa@dcc.uchile.cl; ierms@criba.edu.ar; jorozco@uns.edu.ar; meseguer@ac.upc.edu

Times Cited: 0

Number of references: 40

Tags: IoT Data management, IoT security, Internet of Things

## [A secure and scalable storage system for aggregate data in IoT \(USA\) 2015](#)

Author(s): Jiang, H (Jiang, Hai); Shen, F (Shen, Feng); Chen, S (Chen, Su); Li, KC (Li, Kuan-Ching); Jeong, YS (Jeong, Young-Sik)

Source: FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF GRID COMPUTING AND ESCIENCE Volume: 49 Pages: 133-141 DOI: 10.1016/j.future.2014.11.009 Published: AUG 2015

ABSTRACT: Due to high demand on data mining and analytics activities in IoT, secure and scalable mass storage systems are highly demanded for aggregate data in efficient processing. In this paper, we propose such a secure and scalable IoT storage system based on revised secret sharing scheme with support of scalability, flexibility and reliability at both data and system levels. Shamir's secret sharing scheme is applied to achieve data security without complex key management associated with traditional cryptographic algorithms. The original secret sharing scheme is revised to utilize all coefficients in polynomials for larger data capacity at data level. Flexible data insert and delete operations are supported. Moreover, a distributed IoT storage infrastructure is deployed to provide scalability and reliability at system level. Multiple IoT storage servers are aggregated for large storage capacity whereas individual servers can join and leave freely for flexibility at system level. Experimental results have demonstrated the feasibility and benefits of the proposed system as well as tangible performance gains. (C) 2014 Elsevier B.V. All rights reserved.

Author affiliation: [Jiang, Hai; Shen, Feng; Chen, Su] Arkansas State Univ, Dept Comp Sci, Jonesboro, AR 72467 USA.

[Li, Kuan-Ching] Providence Univ, Dept Comp Sci & Informat Engr, Taichung, Taiwan.

[Jeong, Young-Sik] Dongguk Univ, Dept Multimedia Engr, Seoul, South Korea.

Reprint Address: Jiang, H (reprint author), Arkansas State Univ, Dept Comp Sci, POB 9, Jonesboro, AR 72467 USA.

hjiang@astate.edu; impsen@gmail.com; suchen.bupt@gmail.com; kuancli@pu.edu.tw; ysjeong2k@gmail.com

Times Cited: 1

Number of references: 29

Tags: IoT Data management, IoT Security, Internet of Things

## IoT Infrastructure

### [Advancements of Data Anomaly Detection Research in Wireless Sensor Networks: A Survey and Open Issues \(Malaysia\) 2013](#)

Author(s): Rassam, MA (Rassam, Murad A.); Zainal, A (Zainal, Anazida); Maarof, MA (Maarof, Mohd Aizaini)

Source: SENSORS Volume: 13 Issue: 8 Pages: 10087-10122 DOI: 10.3390/s130810087 Published: AUG 2013

ABSTRACT: Wireless Sensor Networks (WSNs) are important and necessary platforms for the future as the concept Internet of Things has emerged lately. They are used for monitoring, tracking, or controlling of many applications in industry, health care,

habitat, and military. However, the quality of data collected by sensor nodes is affected by anomalies that occur due to various reasons, such as node failures, reading errors, unusual events, and malicious attacks. Therefore, anomaly detection is a necessary process to ensure the quality of sensor data before it is utilized for making decisions. In this review, we present the challenges of anomaly detection in WSNs and state the requirements to design efficient and effective anomaly detection models. We then review the latest advancements of data anomaly detection research in WSNs and classify current detection approaches in five main classes based on the detection methods used to design these approaches. Varieties of the state-of-the-art models for each class are covered and their limitations are highlighted to provide ideas for potential future works. Furthermore, the reviewed approaches are compared and evaluated based on how well they meet the stated requirements. Finally, the general limitations of current approaches are mentioned and further research opportunities are suggested and discussed.

*Author affiliation: [Rassam, Murad A.; Zainal, Anazida; Maarof, Mohd Aizaini] Univ Teknol Malaysia, Fac Comp, Johor Baharu 81310, Malaysia.*

*[Rassam, Murad A.] Taiz Univ, Fac Engn & Informat Technol, Taizi 6803, Yemen.*

*Reprint Address: Rassam, MA (reprint author), Univ Teknol Malaysia, Fac Comp, Johor Baharu 81310, Malaysia.*

*murad.utm@gmail.com; Anazida@utm.my; aizaini@utm.my*

**Times Cited: 2**

**Number of references: 108**

*Tags: IoT Infrastructure, Internet of Things*

### **Assessing the security of internet-connected critical infrastructures (Germany) 2014**

*Author(s): Ghani, H (Ghani, Hamza); Khelil, A (Khelil, Abdelmajid); Suri, N (Suri, Neeraj); Csertan, G (Csertan, Gyoergy); Gonczy, L (Goenczy, Laszlo); Urbanics, G (Urbanics, Gabor); Clarke, J (Clarke, James)*

*Source: SECURITY AND COMMUNICATION NETWORKS Volume: 7 Issue: 12 Pages: 2713-2725 DOI: 10.1002/sec.399*

*Published: DEC 2014*

**ABSTRACT:** Because the Internet of Things (IoT) pervasively extends to all facets of life, the things are increasingly extending to include the interconnection of the Internet to critical infrastructures (CIs) such as telecommunication, power grid, transportation, e-commerce systems, and others. The objective of this paper is twofold: (i) addressing IoT from a CI protection (CIP) and connectivity viewpoint, and (ii) highlighting the need for security quantification to improve the quality of protection (QoP) of CIs. Using a financial infrastructure as an example, a CIP and trust quantification perspective is built up. To this end, we are developing a novel security metrics-based approach to assess and thereon enhance the CIP. We focus on the communication level of the CI where IoT is playing an increasingly important role with respect to sensing and communication across CI elements. Determining the security and dependability level of the communication over the CI constitutes a basic precondition for assessing the QoP of the whole CI, which is needed for any efforts to improve this QoP. Because metrics play a central role for such quantification, this paper develops their QoP use from an IoT perspective, and a reference implementation along with experimental results is presented. Copyright (c) 2012 John Wiley & Sons, Ltd.

*Author affiliation: [Ghani, Hamza; Khelil, Abdelmajid; Suri, Neeraj] Tech Univ Darmstadt, D-64289 Darmstadt, Germany.*

*[Csertan, Gyoergy; Goenczy, Laszlo; Urbanics, Gabor] OptXware R&D Ltd, Budapest, Hungary.*

*[Clarke, James] Waterford Inst Technol, Waterford, Ireland.*

*Reprint Address: Ghani, H (reprint author), Tech Univ Darmstadt, Dept Comp Sci, DEEDS Grp, Hsch Str 10, D-64289 Darmstadt, Germany.*

*ghani@cs.tu-darmstadt.de*

**Times Cited: 1**

**Number of references: 34**

*Tags: IoT Infrastructure, IoT Security, Internet of Things*

### **A Distributed Cluster Computing Energy-Efficient Routing Scheme for Internet of Things Systems (Taiwan) 2015**

*Author(s): Chang, JY (Chang, Jau-Yang)*

*Source: WIRELESS PERSONAL COMMUNICATIONS Volume: 82 Issue: 2 Pages: 757-776 DOI: 10.1007/s11277-014-2251-8*

*Published: MAY 2015*

**ABSTRACT:** An internet of things system is expected to integrate the sensing, communication, networking, and cloud computing technologies in large-scale monitoring environments. The main monitoring infrastructure of internet of things systems is wireless sensor networks. Energy saving becomes one of the most important features for the sensing nodes to extend their lifetime in such systems. To provide reasonable energy consumption and to improve the network lifetime for the internet of things systems, efficient energy saving schemes must be developed. In this paper, a distributed cluster computing energy-efficient routing scheme is proposed to reduce the energy consumption and to extend the network lifetime for the internet of things systems. The main

goal of this scheme is to reduce the data transmission distances of sensing nodes by using the cluster structure concepts. A center of gravity among the sensing nodes is calculated and the residual energy of each sensing node is taken into account in the cluster for selecting a suitable cluster head node. Based on the suitable cluster architecture, the data transmission distances between the sensing nodes can be reduced. The energy consumption is reduced and the lifetime is extended for the sensing nodes by balancing the network load. Simulation results show that the proposed scheme outperforms the previously known schemes in terms of the energy consumption and network lifetime for the internet of things systems.

*Author affiliation: Natl Formosa Univ, Dept Comp Sci & Informat Engr, Huwei, Yun Lin, Taiwan.*

*Reprint Address: Chang, JY (reprint author), Natl Formosa Univ, Dept Comp Sci & Informat Engr, Huwei, Yun Lin, Taiwan.*

*jychang@nfu.edu.tw*

Times Cited: 0

Number of references: 23

Tags: IoT Infrastructure, Internet of Things

### **Extending the Internet of Things to the Future Internet through IPv6 support (England) 2014**

*Author(s): Jara, AJ (Jara, Antonio J.); Varakliotis, S (Varakliotis, Socrates); Skarmeta, AF (Skarmeta, Antonio F.); Kirstein, P (Kirstein, Peter)*

Source: MOBILE INFORMATION SYSTEMS Volume: 10 Issue: 1 Pages: 3-17 DOI: 10.3233/MIS-130169 Published: 2014

ABSTRACT: Emerging Internet of Things (IoT)/Machine-to-Machine (M2M) systems require a transparent access to information and services through a seamless integration into the Future Internet. This integration exploits infrastructure and services found on the Internet by the IoT. On the one hand, the so-called Web of Things aims for direct Web connectivity by pushing its technology down to devices and smart things. On the other hand, the current and Future Internet offer stable, scalable, extensive, and tested protocols for node and service discovery, mobility, security, and auto-configuration, which are also required for the IoT. In order to integrate the IoT into the Internet, this work adapts, extends, and bridges using IPv6 the existing IoT building blocks (such as solutions from IEEE 802.15.4, BT-LE, RFID) while maintaining backwards compatibility with legacy networked embedded systems from building and industrial automation. Specifically, this work presents an extended Internet stack with a set of adaptation layers from non-IP towards the IPv6-based network layer in order to enable homogeneous access for applications and services.

*Author affiliation: [Jara, Antonio J.; Skarmeta, Antonio F.] Univ Murcia, Fac Comp Sci, Dept Informat & Commun Engr DIIC, ES-3100 Murcia, Spain.*

*[Varakliotis, Socrates; Kirstein, Peter] UCL, Dept Comp Sci, London, England.*

*Reprint Address: Jara, AJ (reprint author), Univ Murcia, Fac Comp Sci, Dept Informat & Commun Engr DIIC, ES-3100 Murcia, Spain.*

*jara@ieee.org*

Times Cited: 3

Number of references: 24

Tags: IoT Infrastructure, Internet of Things

### **Fast Release/Capture Sampling in Large-Scale Sensor Networks (China) 2012**

*Author(s): Peng, SL (Peng, Shaoliang); Xing, GL (Xing, Guoliang); Li, SS (Li, Shanshan); Jia, WJ (Jia, Weijia); Peng, YX (Peng, Yuxing)*

Source: IEEE TRANSACTIONS ON MOBILE COMPUTING Volume: 11 Issue: 8 Pages: 1274-1286 DOI: 10.1109/TMC.2011.152 Published: AUG 2012

ABSTRACT: Efficient estimation of global information is a common requirement for many wireless sensor network applications. Examples include counting the number of nodes alive in the network and measuring the scale of physically correlated events. These tasks must be accomplished at extremely low overhead due to the severe resource limitation of sensor nodes, which poses a challenge for large-scale sensor networks. In this paper, we develop a novel protocol FLAKE to efficiently and accurately estimate the global information of large-scale sensor networks based on the sparse sampling theory. Specially, FLAKE disseminates a small number of messages called seeds to the network and issues a query about which nodes receive a seed. The number of nodes that have the information of interest can be estimated by counting the seeds disseminated, the nodes queried, and the nodes that receive a seed. FLAKE can be easily implemented in a distributed manner due to its simplicity. Moreover, desirable tradeoffs can be achieved between the accuracy of estimation and the system overhead. Our simulations show that FLAKE significantly outperforms several existing schemes on accuracy, delay, and message overhead.

*Author affiliation: [Peng, Shaoliang; Li, Shanshan; Peng, Yuxing] Natl Univ Def Technol, Sch Comp Sci, Changsha 410073, Hunan, Peoples R China.*

*[Xing, Guoliang] Michigan State Univ, Dept Comp Sci & Engr, E Lansing, MI 48824 USA.*

*[Jia, Weijia] City Univ Hong Kong, Dept Comp Sci, Kowloon, Hong Kong, Peoples R China.*

*[Jia, Weijia] City Univ Hong Kong, Future Networking Ctr, Shenzhen Res Inst, Kowloon, Hong Kong, Peoples R China.*

Reprint Address: Peng, SL (reprint author), Natl Univ Def Technol, Sch Comp Sci, 47 YanWaChi ST, Changsha 410073, Hunan, Peoples R China.

[pengshaoliang@nudt.edu.cn](mailto:pengshaoliang@nudt.edu.cn); [glxing@msu.edu](mailto:glxing@msu.edu); [shanshanli@nudt.edu.cn](mailto:shanshanli@nudt.edu.cn); [wei.jia@cityu.edu.hk](mailto:wei.jia@cityu.edu.hk); [pyx@nudt.edu.cn](mailto:pyx@nudt.edu.cn)

Times Cited: 1

Number of references: 31

Tags: IoT Infrastructure, Internet of Things

### [Network-layer security for the Internet of Things using TinyOS and BLIP \(Portugal\) 2014](#)

Author(s): Granjal, J (Granjal, Jorge); Monteiro, E (Monteiro, Edmundo); Silva, JS (Silva, Jorge Sa)

Source: INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS Volume: 27 Issue: 10 Pages: 1938-1963 DOI: 10.1002/dac.2444 Published: OCT 2014

ABSTRACT: The design of standard communications and security mechanisms for resource-constrained sensing applications and devices may provide an important contribution for its integration with the Internet and consequently towards the realization of what we nowadays identify as the Internet of Things. This vision will only be realizable if appropriate security mechanisms are available, and in this context we target the design and experimental evaluation of security mechanisms for communications at the network-layer with sensing devices (smart objects) using the standard IPv6 protocol. Our work proposes and evaluates the usage of new compressed security headers for the network layer with smart objects. We implement and evaluate what is, as far as we know, the first proposal of security at the network layer experimentally evaluated using the TinyOS operating system and its networking stack. As we verify in the course of our evaluation study, various scenarios employing network-layer secure communications involving smart objects are feasible, particularly when security mechanisms are designed to benefit from cross-layer interactions that allow the optimization of expensive cryptographic operations. Copyright (C) 2012 John Wiley & Sons, Ltd.

Author affiliation: [Granjal, Jorge; Monteiro, Edmundo; Silva, Jorge Sa] Univ Coimbra, Dept Informat Engn, Coimbra, Portugal.

Reprint Address: Granjal, J (reprint author), Univ Coimbra, Dept Informat Engn, Coimbra, Portugal.

[jgranjal@dei.uc.pt](mailto:jgranjal@dei.uc.pt)

Times Cited: 1

Number of references: 30

Tags: IoT Infrastructure, Internet of Things

### [A potential weakness in RFID-based Internet-of-things systems \(Turkey\) 2015](#)

Author(s): Erguler, I (Erguler, Imran)

Source: PERVASIVE AND MOBILE COMPUTING Volume: 20 Pages: 115-126 DOI: 10.1016/j.pmcj.2014.11.001 Published: JUL 2015

ABSTRACT: In recent years, a large body of research has been devoted to the security and privacy of RFID that is expected to become a critical component of IoT (Internet of Things). Most of these studies have been conducted under the assumption that an RFID system consists of the following elements: RFID tags, a reader and a back-end server. However, in IoT scenario it is supposed that a high density of RFID readers will be deployed and networked to the system over the Internet. Hence, a multi-reader RFID environment circumstance, where readers may be mobile handsets like mobile phones, should be involved in the security analysis of RFID based IoT systems. In this paper, we point out that RFID authentication protocols in the IoT need new security mechanisms that consider untrustworthy RFID entities, compromised readers or insecure communication channel between the readers and the back-end servers. Thus, traditional RFID security schemes designed for closed-loop systems cannot fulfill security and privacy demands, if they are directly adapted to the IoT environment. To emphasize this discrimination, we demonstrate that a secure protocol in a closed-loop RFID system may jeopardize the security of the system in this new RFID concept. Furthermore, we address this fault by investigating the security of a recent IoT RFID authentication protocol, named as AKE-MRFID. We exploit security flaws that have gone unnoticed in the design and present three attacks: de-synchronization, replay and reader impersonation attacks. To defend against the aforementioned attacks, we amend the protocol with a stateful variant so that it holds the claimed security properties. (C) 2014 Elsevier B.V. All rights reserved.

Author affiliation: TUBITAK BILGEM, TR-41470 Gebze, Kocaeli, Turkey.

Reprint Address: Erguler, I (reprint author), TUBITAK BILGEM, TR-41470 Gebze, Kocaeli, Turkey.

[imran.erguler@tubitak.gov.tr](mailto:imran.erguler@tubitak.gov.tr)

Times Cited: 0

Number of references: 24

Tags: IoT Infrastructure, Internet of Things

## **Practical Swarm Optimization based Fault-Tolerance Algorithm for the Internet of Things (China) 2014**

*Author(s): Luo, SL (Luo, Shiliang); Cheng, LL (Cheng, Lianglun); Ren, B (Ren, Bin)*

*Source: KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS Volume: 8 Issue: 4 Pages: 1178-1191 DOI: 10.3837/tiis.2014.04.001 Published: APR 29 2014*

**ABSTRACT:** The fault-tolerance routing problem is one of the most important issues in the application of the Internet of Things, and has been attracting growing research interests. In order to maintain the communication paths from source sensors to the macronodes, we present a hybrid routing scheme and model, in which alternate paths are created once the previous routing is broken. Then, we propose an improved efficient and intelligent fault-tolerance algorithm (IEIFTA) to provide the fast routing recovery and reconstruct the network topology for path failure in the Internet of Things. In the IEIFTA, mutation direction of the particle is determined by multi-swarm evolution equation, and its diversity is improved by the immune mechanism, which can improve the ability of global search and improve the converging rate of the algorithm. The simulation results indicate that the IEIFTA-based fault-tolerance algorithm outperforms the EARQ algorithm and the SPSOA algorithm due to its ability of fast routing recovery mechanism and prolonging the lifetime of the Internet of Things.

*Author affiliation: [Luo, Shiliang] GanNan Normal Univ, Ganzhou 341000, Peoples R China.*

*[Cheng, Lianglun] Guangdong Univ Technol, Guangzhou 510006, Guangdong, Peoples R China.*

*[Ren, Bin] Dongguan Univ Technol, Dongguan 523808, Peoples R China.*

*Reprint Address: Cheng, LL (reprint author), Guangdong Univ Technol, Guangzhou 510006, Guangdong, Peoples R China. luoshiliang88@163.com*

**Times Cited: 0**

**Number of references: 27**

*Tags: IoT Infrastructure, Internet of Things*

## **SDN: Evolution and Opportunities in the Development IoT Applications (Spain) 2014**

*Author(s): Caraguay, ALV (Valdivieso Caraguay, Angel Leonardo); Peral, AB (Benito Peral, Alberto); Lopez, LIB (Barona Lopez, Lorena Isabel); Villalba, LJG (Garcia Villalba, Luis Javier)*

*Source: INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS Article Number: 735142 DOI: 10.1155/2014/735142 Published: 2014*

**ABSTRACT:** The exponential growth of devices connected to the network has resulted in the development of new IoT applications and on-line services. However, these advances are limited by the rigidity of the current network infrastructure, in which the administrator has to implement high-level network policies adapting and configuring protocols manually and usually through a command line interface (CLI). At this point, Software-Defined Networking (SDN) appears as a viable alternative network architecture that allows for programming the network and opening the possibility of creating new services and more efficient applications to cover the actual requirements. In this paper, we describe this new technology and analyze its opportunities in the development of IoT applications. Similarly, we present the first applications and projects based on this technology. Finally, we discuss the issues and challenges in its implementation.

*Author affiliation: [Valdivieso Caraguay, Angel Leonardo; Benito Peral, Alberto; Barona Lopez, Lorena Isabel; Garcia Villalba, Luis Javier] Univ Complutense Madrid, Dept Software Engn & Artificial Intelligence DISI, Sch Comp Sci, GASS,Off 431, E-28040 Madrid, Spain.*

*Reprint Address: Villalba, LJG (reprint author), Univ Complutense Madrid, Dept Software Engn & Artificial Intelligence DISI, Sch Comp Sci, GASS,Off 431, Calle Prof Jose Garcia Santesmases S-N, E-28040 Madrid, Spain.*

*javiervg@fdi.ucm.es*

**Times Cited: 0**

**Number of references: 45**

*Tags: IoT Infrastructure, Internet of Things*

## **Untraceable Sensor Movement in Distributed IoT Infrastructure (Taiwan) 2015**

*Author(s): Gope, P (Gope, Prosanta); Hwang, T (Hwang, Tzonelih)*

*Source: IEEE SENSORS JOURNAL Volume: 15 Issue: 9 Pages: 5340-5348 DOI: 10.1109/JSEN.2015.2441113 Published: SEP 2015*

**ABSTRACT:** Recent advances in information and communication technologies and embedded systems have given rise to a new disruptive technology, the Internet of Things (IoTs). IoT allows people and objects in the physical world as well as data and virtual environments to interact with each other so as to create smart environments, such as smart transport systems, smart cities, smart health, and so on. However, IoT raises some important questions and also introduces new challenges for the security of systems and processes and the privacy of individuals, such as their location and movements and so on. In this paper, at first, we propose a distributed IoT system architecture. Subsequently, we propose an anonymous authentication scheme, which can ensure some of

the notable properties, such as sensor anonymity, sensor untraceability, resistance to replay attacks, cloning attacks, and so on. It is argued that the proposed authentication scheme will be useful in many distributed IoT applications (such as radio-frequency identification-based IoT system, Biosensor-based IoT healthcare system, and so on), where the privacy of the sensor movement is greatly desirable.

*Author affiliation:* [Gope, Prosanta; Hwang, Tzonelih] Natl Cheng Kung Univ, Dept Comp Sci & Informat Engn, Tainan 701, Taiwan.  
*Reprint Address:* Hwang, T (reprint author), Natl Cheng Kung Univ, Dept Comp Sci & Informat Engn, Tainan 701, Taiwan.

*prosanta.nitdgp@gmail.com; hwangtl@ismail.csie.ncku.edu.tw*

**Times Cited: 0**

**Number of references: 27**

*Tags: IoT Infrastructure, IoT Security, Internet of Things*

## IoT Security

### [Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things \(China\) 2015](#)

*Author(s):* Ning, H (Ning, Huansheng); Liu, H (Liu, Hong); Yang, LT (Yang, Laurence T.)

*Source:* IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS Volume: 26 Issue: 3 Pages: 657-667 DOI: 10.1109/TPDS.2014.2311791 Published: MAR 2015

**ABSTRACT:** The Internet of Things (IoT) is becoming an attractive system paradigm to realize interconnections through the physical, cyber, and social spaces. During the interactions among the ubiquitous things, security issues become noteworthy, and it is significant to establish enhanced solutions for security protection. In this work, we focus on an existing U2IoT architecture (i.e., unit IoT and ubiquitous IoT), to design an aggregated-proof based hierarchical authentication scheme (APHA) for the layered networks. Concretely, 1) the aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission; 2) the directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication; 3) different access authorities are assigned to achieve hierarchical access control. Meanwhile, the BAN logic formal analysis is performed to prove that the proposed APHA has no obvious security defects, and it is potentially available for the U2IoT architecture and other IoT applications.

*Author affiliation:* [Ning, Huansheng] Univ Sci & Technol Beijing, Sch Comp & Commun Engn, Beijing 100083, Peoples R China.

[Ning, Huansheng; Liu, Hong] Beihang Univ, Sch Elect & Informat Engn, Beijing 100191, Peoples R China.

[Yang, Laurence T.] Huazhong Univ Sci & Technol, Sch Comp Sci & Technol, Wuhan 430074, HuBei, Peoples R China.

[Yang, Laurence T.] St Francis Xavier Univ, Dept Comp Sci, Antigonish, NS B2G 1C0, Canada.

*Reprint Address:* Ning, H (reprint author), Univ Sci & Technol Beijing, Sch Comp & Commun Engn, Beijing 100083, Peoples R China.

*ninghuansheng@ustb.edu.cn; liuhongler@ee.buaa.edu.cn; ltyang@stfx.ca*

**Times Cited: 0**

**Number of references: 26**

*Tags: IoT security, Internet of Things*

### [Autonomic schemes for threat mitigation in Internet of Things \(Malaysia\) 2015](#)

*Author(s):* Ashraf, QM (Ashraf, Qazi Mamoon); Habaebi, MH (Habaebi, Mohamed Hadi)

*Source:* JOURNAL OF NETWORK AND COMPUTER APPLICATIONS Volume: 49 Pages: 112-127 DOI: 10.1016/j.jnca.2014.11.011 Published: MAR 2015

*jnca.2014.11.011*

**ABSTRACT:** Internet of Things (IoT) refers to the expansion of Internet technologies to include wireless sensor networks (WSNs) and smart objects by extensive interfacing of exclusively identifiable, distributed communication devices. Due to the close connection with the physical world, it is an important requirement for IoT technology to be self-secure in terms of a standard information security model components. Autonomic security should be considered as a critical priority and careful provisions must be taken in the design of dynamic techniques, architectures and self-sufficient frameworks for future IoT. Over the years, many researchers have proposed threat mitigation approaches for IoT and WSNs. This survey considers specific approaches requiring minimal human intervention and discusses them in relation to self-security. This survey Author affiliation and brings together a broad range of ideas linked together by IoT, autonomy and security. More particularly, this paper looks at threat mitigation approaches in IoT using an autonomic taxonomy and finally sets down future directions. (C) 2014 Elsevier Ltd. All rights reserved.

*Author affiliation:* [Ashraf, Qazi Mamoon; Habaebi, Mohamed Hadi] Univ Islam Antarabangsa, Dept Elect & Comp Engn, Jalan Gombak, Selangor, Malaysia.

*Reprint Address:* Ashraf, QM (reprint author), Univ Islam Antarabangsa, Dept Elect & Comp Engn, Jalan Gombak, Selangor, Malaysia.

*mamoonq@gmail.com; habaebi@iium.edu.my*

**Times Cited: 0**

**Number of references: 135**

*Tags: IoT Security, Internet of Things*

*continued*

## [Big Data Privacy in the Internet of Things Era \(the Netherlands\) 2015](#)

Author(s): Perera, C (Perera, Charith); Ranjan, R (Ranjan, Rajiv); Wang, LZ (Wang, Lizhe); Khan, SU (Khan, Samee U.); Zomaya, AY (Zomaya, Albert Y.)

Source: IT PROFESSIONAL Volume: 17 Issue: 3 Pages: 32-39 DOI: 10.1109/MITP.2015.34 Published: MAY-JUN 2015

ABSTRACT: Over the last few years, we have seen a plethora of Internet of Things (IoT) solutions, products and services, making their way into the industry's market-place. All such solution will capture a large amount of data pertaining to the environment, as well as their users. The objective of the IoT is to learn more and to serve better the system users. Some of these solutions may store the data locally on the devices ('things'), and others may store in the Cloud. The real value of collecting data comes through data processing and aggregation in large-scale where new knowledge can be extracted. However, such procedures can also lead to user privacy issues. This article discusses some of the main challenges of privacy in IoT, and opportunities for research and innovation. We also introduce some of the ongoing research efforts that address IoT privacy issues.

Author affiliation: [Perera, Charith] Open Univ, Heerlen, Netherlands.

[Ranjan, Rajiv] CSIRO, Canberra, ACT, Australia.

[Wang, Lizhe] Chinese Acad Sci, Inst Remote Sensing & Digital Earth, Beijing 100864, Peoples R China.

[Khan, Samee U.] N Dakota State Univ, Elect & Comp Engn, Fargo, ND 58102 USA.

[Zomaya, Albert Y.] Univ Sydney, Sch Informat Technol, High Performance Comp & Networking, Sydney, NSW 2006, Australia.

Reprint Address: Perera, C (reprint author), Open Univ, Heerlen, Netherlands.

charith.perera@ieee.org; raj.ranjan@csiro.au; wanglz@radi.ac.cn; samee.khan@nds.edu; albert.zomaya@sydney.edu.au

Times Cited: 0

Number of references: 14

Tags: IoT Security, Internet of Things

## [Context-aware usage control for web of things \(China\) 2014](#)

Author(s): Bai, GD (Bai, Guangdong); Yan, L (Yan, Lin); Gu, L (Gu, Liang); Guo, Y (Guo, Yao); Chen, XQ (Chen, Xiangqun)

Source: SECURITY AND COMMUNICATION NETWORKS Volume: 7 Issue: 12 Pages: 2696-2712 DOI: 10.1002/sec.424 Published: DEC 2014

ABSTRACT: The Web of Things (WoT), inherited from the Internet of Things (IoT), encapsulates functionalities into publishable services on the Web to enable the IoT a seamless integration with the Web. The openness of the Web, in turn, directly exposes WoT to existing attacks from the Web. In addition, WoT possesses characteristics of high security and privacy concerns, mobility, and limited capabilities, which require specific and additional security and privacy protection beyond existing mechanisms. More importantly, WoT is inherently connected to its context, so context information must be taken into account in its security and privacy measures. To address these challenges, we propose a context-aware usage control model (ConUCON), which leverages the context information to enhance data, resource, and service protection for WoT. On the basis of ConUCON, we also design and implement a context-aware usage control framework on the middleware layer in our ongoing SmartHome project, to provide security and privacy protection. ConUCON is designed specifically to express the context-aware usage policy specification, such that security and privacy requirements can be easily specified and enforced with the proposed model and framework. Finally, we apply ConUCON to a remote appliance management prototype, as a case study, to demonstrates its feasibility in a real environment. Copyright (c) 2012 John Wiley & Sons, Ltd.

Author affiliation: [Bai, Guangdong; Yan, Lin; Gu, Liang; Guo, Yao; Chen, Xiangqun] Peking Univ, Sch EECS, Minist Educ, Key Lab High Confidence Software Technol, Beijing 100871, Peoples R China.

[Gu, Liang] Yale Univ, Dept Comp Sci, New Haven, CT 06520 USA.

[Gu, Liang] Peking Univ, Beijing 100871, Peoples R China.

[Gu, Liang] Yale Univ, New Haven, CT 06520 USA.

Reprint Address: Guo, Y (reprint author), Peking Univ, Inst Software, Sch EECS, Beijing 100871, Peoples R China.

yaoguo@sei.pku.edu.cn

Times Cited: 0

Number of references: 62

Tags: IoT security, Internet of Things

## [Defending Internet of Things against Exploits \(Brazil\) 2015](#)

Author(s): Teixeira, FA (Teixeira, F. A.); Machado, GV (Machado, G. V.); Fonseca, PM (Fonseca, P. M.); Pereira, FMQ (Pereira, F. M. Q.); Wong, HC (Wong, H. C.); Nogueira, JMS (Nogueira, J. M. S.); Oliveira, LB (Oliveira, L. B.)

Source: IEEE LATIN AMERICA TRANSACTIONS Volume: 13 Issue: 4 Pages: 1112-1119 Published: APR 2015 DOI: 10.1109/TLA.2015.7106364

ABSTRACT: The Internet of Things (IoT) demands tailor-made security solutions. Today, there are a number of proposals able to meet IoT's demands in the context of attacks from outsiders. In the context of insiders, however, this does not hold true. Existing

solutions to deal with this class of attacks not always take into consideration the IoT's idiosyncrasies and, therefore, they do not produce the best results. This work aims at coming up with tailor-made security schemes for thwarting attacks from insiders in the context of IoT systems. Our solution makes use of a pioneering solution to pinpoint vulnerabilities: we crosscheck data from communicating nodes. It provides the same guarantees as traditional security mechanisms, but it is about 83% more efficient, according to the experiments that this article describes.

*Author affiliation:* [Teixeira, F. A.; Machado, G. V.; Fonseca, P. M.; Pereira, F. M. Q.; Nogueira, J. M. S.; Oliveira, L. B.] Univ Fed Minas Gerais, Belo Horizonte, MG, Brazil. [Wong, H. C.] Intel Corp, Santa Clara, CA USA.

*Reprint Address:* Teixeira, FA (reprint author), Univ Fed Minas Gerais, Belo Horizonte, MG, Brazil.

*teixeira@dcc.ufmg.br; gvieira@dcc.ufmg.br; pablom@dcc.ufmg.br; fernando@dcc.ufmg.br; jmarcos@dcc.ufmg.br; leob@dcc.ufmg.br; chi.wong@intel.com*

Times Cited: 0

Number of references: 25

Tags: IoT security, Internet of Things

## Design of a Distributed Personal Information Access Control Scheme for Secure Integrated Payment in NFC (South Korea) 2015

*Author(s):* Kang, J (Kang, Jungho); Park, JH (Park, Jong Hyuk); Suk, S (Suk, Sangkee)

*Source:* SYMMETRY-BASEL Volume: 7 Issue: 2 Pages: 935-948 DOI: 10.3390/sym7020935 Published: JUN 2015

**ABSTRACT:** At the center of core technologies for a future cyber world, such as Internet of Things (IoT) or big data, is a context-rich system that offers services by using situational information. The field where context-rich systems were first introduced is near-field communication (NFC)-based electronic payments. Near-field Communication (NFC) integrated payment services collect the payment information of the credit card and the location information to generate patterns in the user's consumption or movement through big data technology. Based on such pattern information, tailored services, such as advertisement, are offered to users. However, there is difficulty in controlling access to personal information, as there is a collaborative relationship focused on the trusted service manager (TSM) that is close knit to shared personal information. Moreover, in the case of Hadoop, among the many big data analytical technologies, it offers access control functions, but not a way to authorize the processing of personal information, making it impossible to grant authority between service providers to process information. As such, this paper proposes a key generation and distribution method, as well as a secure communication protocol. The analysis has shown that the efficiency was greater for security and performance compared to relation works.

*Author affiliation:* [Kang, Jungho] Soongsil Univ, Dept Comp, Seoul 156743, South Korea.

[Park, Jong Hyuk; Suk, Sangkee] Seoul Natl Univ Sci & Technol, Dept Comp Sci & Engn, Seoul 139743, South Korea.

*Reprint Address:* Suk, S (reprint author), Seoul Natl Univ Sci & Technol, Dept Comp Sci & Engn, Gongneung 2 Dong, Seoul 139743, South Korea.

*kjh7548@naver.com; jhpark1@seoultech.ac.kr; sksuk@seoultech.ac.kr*

Times Cited: 0

Number of references: 25

Tags: IoT security, Internet of Things

## Directed Path Based Authentication Scheme for the Internet of Things (China) 2012

*Author(s):* Ning, HS (Ning, Huansheng); Liu, H (Liu, Hong); Liu, Q (Liu, Qing); Ji, GL (Ji, Genlin)

*Source:* JOURNAL OF UNIVERSAL COMPUTER SCIENCE Volume: 18 Issue: 9 Pages: 1112-1131 Published: 2012

**ABSTRACT:** The Internet of Things (IoT) is emerging as an attractive paradigm, and several IoT models and related security issues have received widespread attentions. In this paper, we focus on an existing U2IoT architecture (i.e., Unit IoT and Ubiquitous IoT), and propose a directed path based authentication scheme (DPAS) to realize security protection for the U2IoT architecture. Particularly, the directed path descriptor is introduced for the secret key distribution and cross-network authentication, and the proof mapping is applied to establish tri-dimensional equivalence relations among diverse nodes for achieving mutual authentication. Moreover, security analysis shows that DPAS achieves data confidentiality and integrity, authentication, anonymity and forward security, and performance analysis indicates that DPAS with moderate communication overhead and computation load is suitable for the IoT applications.

*Author affiliation:* [Ning, Huansheng; Liu, Hong] Beihang Univ, Sch Elect & Informat Engn, Beijing, Peoples R China.

[Liu, Qing; Ji, Genlin] Nanjing Normal Univ, Sch Comp Sci & Technol, Nanjing, Jiangsu, Peoples R China.

*Reprint Address:* Ning, HS (reprint author), Beihang Univ, Sch Elect & Informat Engn, Beijing, Peoples R China.

*ninghuansheng@buaa.edu.cn; liuhongler@ee.buaa.edu.cn; njnulq@163.com; glji@njnu.edu.cn*

Times Cited: 0

Number of references: 23

Tags: IoT security, Internet of Things

## [An Effective Differential Fault Analysis on the Serpent Cryptosystem in the Internet of Things \(China\) 2014](#)

Author(s): Li, W (Li Wei); Tao, Z (Tao Zhi); Gu, DW (Gu Dawu); Sun, L (Sun Li); Qu, B (Qu Bo); Liu, ZQ (Liu Zhiqiang); Liu, Y (Liu Ya)

Source: CHINA COMMUNICATIONS Volume: 11 Issue: 6 Pages: 129-139 Published: JUN 2014

ABSTRACT: Due to the strong attacking ability, fast speed, simple implementation and other characteristics, differential fault analysis has become an important method to evaluate the security of cryptosystem in the Internet of Things. As one of the AES finalists, the Serpent is a 128-bit Substitution-Permutation Network (SPN) cryptosystem. It has 32 rounds with the variable key length between 0 and 256 bits, which is flexible to provide security in the Internet of Things. On the basis of the byte-oriented model and the differential analysis, we propose an effective differential fault attack on the Serpent cryptosystem. Mathematical analysis and simulating experiment show that the attack could recover its secret key by introducing 48 faulty ciphertexts. The result in this study describes that the Serpent is vulnerable to differential fault analysis in detail. It will be beneficial to the analysis of the same type of other iterated crypto systems.

Author affiliation: [Li Wei; Tao Zhi; Sun Li] Donghua Univ, Sch Comp Sci & Technol, Shanghai 201620, Peoples R China.

[Li Wei; Gu Dawu; Liu Zhiqiang; Liu Ya] Shanghai Jiao Tong Univ, Dept Comp Sci & Engn, Shanghai 200240, Peoples R China.

[Li Wei] Chinese Acad Sci, State Key Lab Informat Secur, Inst Informat Engn, Beijing 100093, Peoples R China.

[Li Wei] Shanghai Key Lab Integrate Adm Technol Informat S, Shanghai 200240, Peoples R China.

[Qu Bo] Delft Univ Technol, NL-2628 CD Delft, Netherlands.

[Liu Zhiqiang] Katholieke Univ Leuven, ESAT COSIC, Leuven, Belgium.

[Liu Zhiqiang] Katholieke Univ Leuven, IBBT, Leuven, Belgium.

[Liu Ya] Shanghai Univ Sci & Technol, Dept Comp Sci & Engn, Shanghai 200093, Peoples R China.

Reprint Address: Sun, L (reprint author), Donghua Univ, Sch Comp Sci & Technol, Shanghai 201620, Peoples R China.

sli@dhu.edu.cn

Times Cited: 0

Number of references: 28

Tags: IoT security, Internet of Things

## [Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure \(India\) 2015](#)

Author(s): Asri, S (Asri, Satin); Pranggono, B (Pranggono, Bernardi)

Source: WIRELESS PERSONAL COMMUNICATIONS Volume: 83 Issue: 3 Pages: 2211-2223 DOI: 10.1007/s11277-015-2510-3 Published: AUG 2015

ABSTRACT: The age of Internet of Things has brought in new challenges specifically in areas such as security. The evolution of classic power grids to smart grids is a prime example of how everything is now being connected to the Internet. With the power grid becoming smart, the information and communication systems supporting it is subject to both classical and emerging cyber-attacks. The article investigates the vulnerabilities caused by a distributed denial-of-service (DDoS) attack on the smart grid advanced metering infrastructure. Attack simulations have been conducted on a realistic electrical grid topology. The simulated network consisted of smart meters, power plant and utility server. Finally, the impact of large scale DDoS attacks on the distribution system's reliability is discussed.

Author affiliation: [Asri, Satin] Manipal Inst Technol, Dept Comp Sci & Engn, Manipal, Karnataka, India.

[Pranggono, Bernardi] Glasgow Caledonian Univ, Sch Engn & Built Environm, Glasgow G4 0BA, Lanark, Scotland.

Reprint Address: Pranggono, B (reprint author), Glasgow Caledonian Univ, Sch Engn & Built Environm, Glasgow G4 0BA, Lanark, Scotland.

satinasri@gmail.com; bern@ieee.org

Times Cited: 0

Number of references: 21

Tags: IoT security, Internet of Things

## [A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things \(South Korea\) 2014](#)

Author(s): Oh, D (Oh, Doohwan); Kim, D (Kim, Deokho); Ro, AW (Ro, Andwon Woo)

Source: SENSORS Volume: 14 Issue: 12 Pages: 24188-24211 DOI: 10.3390/s141224188 Published: DEC 2014

ABSTRACT: With the emergence of the Internet of Things (IoT), a large number of physical objects in daily life have been aggressively connected to the Internet. As the number of objects connected to networks increases, the security systems face a critical challenge due to the global connectivity and accessibility of the IoT. However, it is difficult to adapt traditional security systems to the objects in the IoT, because of their limited computing power and memory size. In light of this, we present a

lightweight security system that uses a novel malicious pattern-matching engine. We limit the memory usage of the proposed system in order to make it work on resource-constrained devices. To mitigate performance degradation due to limitations of computation power and memory, we propose two novel techniques, auxiliary shifting and early decision. Through both techniques, we can efficiently reduce the number of matching operations on resource-constrained systems. Experiments and performance analyses show that our proposed system achieves a maximum speedup of 2.14 with an IoT object and provides scalable performance for a large number of patterns.

*Author affiliation: [Oh, Doohwan; Kim, Deokho; Ro, Andwon Woo] Yonsei Univ, Sch Elect & Elect Engn, Seoul 120749, South Korea.*

*Reprint Address: Ro, AW (reprint author), Yonsei Univ, Sch Elect & Elect Engn, 50 Yonsei Ro, Seoul 120749, South Korea.*

*ohdooh@yonsei.ac.kr; nautes87@yonsei.ac.kr; wro@yonsei.ac.kr*

Times Cited: 0

Number of references: 35

Tags: IoT Security, Internet of Things

### [Modeling of Malicious Code Propagations in Internet of Things \(China\) 2011](#)

*Author(s): Lin, ZW (Lin Zhaowen); Su, F (Su Fei); Ma, Y (Ma Yan)*

Source: CHINA COMMUNICATIONS Volume: 8 Issue: 1 Special Issue: SI Pages: 79-86 Published: JAN 2011

ABSTRACT: Nowadays, the main communication object of Internet is human-human. But it is foreseeable that in the near future any object will have a unique identification and can be addressed and connected. The Internet will expand to the Internet of Things. IPv6 is the cornerstone of the Internet of Things. In this paper, we investigate a fast active worm, referred to as topological worm, which can propagate twice to more than three times faster than a traditional scan-based worm. Topological worm spreads over AS-level network topology, making traditional epidemic models invalid for modeling the propagation of it. For this reason, we study topological worm propagation relying on simulations. First, we propose a new complex weighted network model, which represents the real IPv6 AS-level network topology. And then, a new worm propagation model based on the weighted network model is constructed, which describes the topological worm propagation over AS-level network topology. The simulation results verify the topological worm model and demonstrate the effect of parameters on the propagation.

*Author affiliation: [Lin Zhaowen; Su Fei; Ma Yan] Beijing Univ Posts & Telecommun, Inst Networking Technol, Beijing 100876, Peoples R China.*

*[Ma Yan] Beijing Univ Posts & Telecommun, Beijing Key Lab Intelligent Telecommun Software, Beijing 100876, Peoples R China.*

*Reprint Address: Lin, ZW (reprint author), Beijing Univ Posts & Telecommun, Inst Networking Technol, Beijing 100876, Peoples R China.*

Times Cited: 3

Number of references: 20

Tags: IoT Security, Internet of Things

### [A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography \(Algeria\) 2015](#)

*Author(s): Boudia, ORM (Boudia, Omar Rafik Merad); Senouci, SM (Senouci, Sidi Mohammed); Feham, M (Feham, Mohammed)*

Source: AD HOC NETWORKS Volume: 32 Special Issue: SI Pages: 98-113 DOI: 10.1016/j.adhoc.2015.01.002 Published: SEP 2015

ABSTRACT: Wireless sensor networks (WSNs) are nowadays considered as an important part of the Internet of Things (IoT). In these networks, data aggregation plays an essential role in energy preservation. However, WSNs are usually deployed in hostile and unattended environments (e.g. military applications) in which the confidentiality and integrity security services are widely desired. Recently, homomorphic encryptions have been applied to conceal sensitive information during aggregation such that algebraic operations are done directly on ciphertexts without decryption. The main benefit is that they offer the end-to-end data confidentiality and they do not require expensive computation at aggregator nodes since no encryption and decryption are performed. However, existing solutions either incur a considerable overhead or have limited applicability to certain types of aggregate queries. This paper presents a novel secure data aggregation protocol for WSNs. The scheme employs Stateful Public Key Encryption (StPKE) and some previous techniques in order to provide an efficient end-to-end security. Moreover, our solution does not impose any bound on the aggregation function's nature (Maximum, Minimum, Average, etc.). We present and implement our scheme on TelosB as well as MicaZ sensor network platforms and measure the execution time of our various cryptographic functions. Simulations are also conducted to show how our scheme can achieve a high security level (by providing the above security services) with a low overhead (in terms of computation and communication) in large-scale scenario. (C) 2015 Elsevier B.V. All rights reserved.

*Author affiliation: [Boudia, Omar Rafik Merad; Feham, Mohammed] Univ Tlemcen, STIC Lab, Tilimsen, Algeria.*

[Senouci, Sidi Mohammed] Univ Burgundy, Dr Lab, Nevers, France.  
 Reprint Address: Boudia, ORM (reprint author), Univ Tlemcen, STIC Lab, Tilimsen, Algeria.  
 om\_meradboudia@mail.univ-tlemcen.dz

Times Cited: 0

Number of references: 48

Tags: IoT Security, Internet of Things

### **Probabilistic yoking proofs for large scale IoT systems (Spain) 2015**

Author(s): de Fuentes, JM (de Fuentes, Jose M.); Peris-Lopez, P (Peris-Lopez, Pedro); Tapiador, JE (Tapiador, Juan E.); Pastrana, S (Pastrana, Sergio)

Source: AD HOC NETWORKS Volume: 32 Special Issue: SI Pages: 43-52 DOI: 10.1016/j.adhoc.2015.01.003 Published: SEP 2015

ABSTRACT: Yoking (or grouping) proofs were introduced in 2004 as a security construction for RFID applications in which it is needed to build an evidence that several objects have been scanned simultaneously or, at least, within a short time. Such protocols were designed for scenarios where only a few tags (typically just two) are involved, so issues such as preventing an object from abandoning the proof right after being interrogated simply do not make sense. The idea, however, is very interesting for many Internet of Things (IoT) applications where a potentially large population of objects must be grouped together. In this paper we address this issue by presenting the notion of Probabilistic Yoking Proofs (PYP) and introducing three main criteria to assess their performance: cost, security, and fairness. Our proposal combines the message structure found in classical grouping proof constructions with an iterative Poisson sampling process where the probability of each object being sampled varies over time. We introduce a number of mechanisms to apply fluctuations to each object's sampling probability and present different sampling strategies. Our experimental results confirm that most strategies achieve good security and fairness levels while keeping the overall protocol cost down. (C) 2015 Elsevier B.V. All rights reserved.

Author affiliation: [de Fuentes, Jose M.; Peris-Lopez, Pedro; Tapiador, Juan E.; Pastrana, Sergio] Univ Carlos III Madrid, Dept Comp Sci, Madrid 28911, Spain.

Reprint Address: de Fuentes, JM (reprint author), Univ Carlos III Madrid, Dept Comp Sci, Avda Univ 30, Madrid 28911, Spain.  
 jfuentes@inf.uc3m.es; pperis@inf.uc3m.es; jestevez@inf.uc3m.es; spastran@inf.uc3m.es

Times Cited: 0

Number of references: 23

Tags: IoT security, Internet of Things

### **Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey (Portugal) 2015**

Author(s): Granjal, J (Granjal, Jorge); Monteiro, E (Monteiro, Edmundo); Silva, JS (Silva, Jorge Sa)

Source: AD HOC NETWORKS Volume: 24 Pages: 264-287 DOI: 10.1016/j.adhoc.2014.08.001 Part: A Published: JAN 2015

ABSTRACT: The integration of low-power wireless sensing and actuating devices with the Internet will provide an important contribution to the formation of a global communications architecture encompassing Wireless Sensor Networks (WSN), and to enable applications using such devices designed to bring unprecedented convenience and economical benefits to our life. Such applications also take place in the context of our current vision on an Internet of Things (IoT), which promises to encompass heterogeneous devices and communication technologies, including WSN. Due to the characteristics of the devices in WSN and to the requirements of applications, low-power wireless communications are employed and the functionalities supported must be carefully balanced against the limited resources at the disposal of applications. Low-power communication technologies are also currently being designed with the purpose of supporting the integration of WSN with the Internet and, as in isolated WSN environments, security will be a fundamental enabling factor of future applications using Internet-integrated WSN. Although various surveys currently exist addressing security mechanisms for WSN environments, our goal is to analyze how security may be addressed as an enabling factor of the integration of low-power WSN with the Internet, in the context of its contribution to the IoT. We analyze the current research and industry proposals supporting this integration, together with the security solutions and mechanisms designed in its context. Our discussion is supported by an analysis on the attack and threat model against Internet-integrated WSN, and on the security requirements to consider in this context. We believe that a survey with such goals may provide an important contribution to readers interested in embracing this important area of research and ours is, as far as our knowledge goes, the first article with such goals. (C) 2014 Elsevier B.V. All rights reserved.

Author affiliation: [Granjal, Jorge; Monteiro, Edmundo; Silva, Jorge Sa] Univ Coimbra, Dept Informat Engn, P-3030290 Coimbra, Portugal.

Reprint Address: Granjal, J (reprint author), Univ Coimbra, Dept Informat Engn, P-3030290 Coimbra, Portugal.  
 jgranjal@dei.uc.pt; edmundo@dei.uc.pt; sasilva@dei.uc.pt

Times Cited: 1

Number of references: 106

Tags: *IoT security, Internet of Things*

### [Security of the Internet of Things: perspectives and challenges \(China\) 2014](#)

Author(s): *Jing, Q (Jing, Qi); Vasilakos, AV (Vasilakos, Athanasios V.); Wan, JF (Wan, Jiafu); Lu, JW (Lu, Jingwei); Qiu, DC (Qiu, Dechao)*

Source: WIRELESS NETWORKS Volume: 20 Issue: 8 Pages: 2481-2501 DOI: 10.1007/s11276-014-0761-7 Published: NOV 2014

ABSTRACT: Internet of Things (IoT) is playing a more and more important role after its showing up, it covers from traditional equipment to general household objects such as WSNs and RFID. With the great potential of IoT, there come all kinds of challenges. This paper focuses on the security problems among all other challenges. As IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT. And as IoT contains three layers: perception layer, transportation layer and application layer, this paper will analyze the security problems of each layer separately and try to find new problems and solutions. This paper also analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them. In the end, this paper compares security issues between IoT and traditional network, and discusses opening security issues of IoT.

Author affiliation: *[Jing, Qi; Lu, Jingwei; Qiu, Dechao] Peking Univ, Sch Software & Microelect, Beijing 100871, Peoples R China.*

*[Jing, Qi] Chinese Acad Sci, Inst Informat Engn, Lab Informat Secur, Beijing, Peoples R China.*

*[Jing, Qi] Chinese Acad Sci, Inst Informat Engn, Beijing Key Lab IOT Informat Secur Technol, Beijing, Peoples R China.*

*[Vasilakos, Athanasios V.] Kuwait Univ, Dept Comp Sci, Kuwait, Kuwait.*

*[Wan, Jiafu] S China Univ Technol, Sch Mech & Automot Engn, Guangzhou, Guangdong, Peoples R China.*

Reprint Address: *Wan, JF (reprint author), S China Univ Technol, Sch Mech & Automot Engn, Guangzhou, Guangdong, Peoples R China.*

*jiafuwan\_76@163.com*

Times Cited: 4

Number of references: 115

Tags: *IoT security, Internet of Things*

### [Survey on secure communication protocols for the Internet of Things \(France\) 2015](#)

Author(s): *Nguyen, KT (Kim Thuat Nguyen); Laurent, M (Laurent, Maryline); Oualha, N (Oualha, Nouha)*

Source: AD HOC NETWORKS Volume: 32 Special Issue: SI Pages: 17-31 DOI: 10.1016/j.adhoc.2015.01.006 Published: SEP 2015

ABSTRACT: The Internet of Things or "IoT" defines a highly interconnected network of heterogeneous devices where all kinds of communications seem to be possible, even unauthorized ones. As a result, the security requirement for such network becomes critical whilst common standard Internet security protocols are recognized as unusable in this type of networks, particularly due to some classes of IoT devices with constrained resources. The document discusses the applicability and limitations of existing IP-based Internet security protocols and other security protocols used in wireless sensor networks, which are potentially suitable in the context of IoT. The analysis of these protocols is discussed based on a taxonomy focusing on the key distribution mechanism. (C) 2015 Elsevier B.V. All rights reserved.

Author affiliation: *[Kim Thuat Nguyen; Oualha, Nouha] CEA, LIST, Commun Syst Lab, F-91191 Gif Sur Yvette, France.*

*[Laurent, Maryline] Telecom SudParis, Inst Mines Telecom, CNRS, UMR SAMOVAR 5157, F-91011 Evry, France.*

Reprint Address: *Nguyen, KT (reprint author), CEA, LIST, Commun Syst Lab, F-91191 Gif Sur Yvette, France.*

*kimthuat.nguyen@cea.fr; maryline.laurent@telecom-sudparis.eu; nouha.oualha@cea.fr*

Times Cited: 0

Number of references: 64

Tags: *IoT security, Internet of Things* ■

## ABOUT THIS PUBLICATION

The **S&T IN-DEPTH BULLETIN** is a compilation of selected recent technical articles on emerging fields in science and technology which may have long or short term implication for national security. Articles are selected from peer-reviewed journals and focus on providing a more detailed insight to the R&E community. Each quarter we will feature a topic and provide abstracts from the most timely and relevant review articles. Providing a comprehensive bibliography is beyond the scope of this publication but full articles may be requested via the Pentagon library or via your local Command's library. Personnel assigned to the Pentagon may request articles from John Mills at [john.mills@whs.mil](mailto:john.mills@whs.mil).

We welcome your feedback to improve the publication and make it more relevant to your work. To subscribe (or unsubscribe), visit <https://tin-ly.sainc.com/ASDRE>. To provide feedback or ask questions, contact us at [asdre-st-bulletin-reply@sainc.com](mailto:asdre-st-bulletin-reply@sainc.com).

This publication is authored and distributed by:

**Kristopher Gardner**

Director, Office of Technical Intelligence (OTI)

**Ms. Hema Viswanath**

OTI Corporate Librarian

*The appearance of external hyperlinks in this publication does not constitute endorsement by the United States Department of Defense (DoD) of the linked web sites, nor the information, products or services contained therein. In addition, the content featured does not necessarily reflect DoD's views or priorities.*