Ad Hoc Networks 11 (2013) 2623–2624

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Editorial

Security, privacy and trust management in the internet of things era – SePriT

In recent years, technology has advanced to the point at which it is possible and affordable to build and deploy the Internet of Things (IoT). Whilst there is ongoing debate about the exact nature of IoT, it is clear that a primary aim is to deliver personalised or even autonomic services to individuals, building on a pervasive digital ecosystem that collects information from, and offers control of devices that are embedded in our everyday lives. Short-range communication technologies, when jointly adopted with more classical networking solutions, are the key enabling technology with the power to make the vision of pervasive computing a reality. This being said, the design of systems that are characterized by complex and unpredictable interactions among highly heterogeneous resources necessitates additional effort in providing programming abstractions that allow developers to balance uniformity and simplicity with the flexibility andaccess to low-level information needed to create efficient and secure solutions. The vision of the Internet of Things has motivated technological challenge in areas that range from hardware design to network protocols, programming languages and frameworks for ease of robust and secure application development.

The intended and expected penetration of the IoT paradigm also poses challenging and interesting socio-technological issues. A consequence of realising the vision in which intelligence is applied to data collected from embedded systems to provide personalised services that affect our lives is the necessary availability of mechanisms for information gathering, for data analysis, and for control. The embedded nature of IoT technology and a lack of awareness of its potential social and personal consequences, as balanced against the more clearly articulated benefits, make a special issue dedicated to security, privacy and trust aspects of IoT extremelytimely.

This special issue aims to open a new critical debate on the IoT paradigm, with a special focus on security, privacy and trust management. It includes eight high-quality papers with diverse, but yet complementary topics that help in establishing a secure IoT framework.

More in details, the paper of Bianchi et al. is based on exploring the question of whether the employed energy harvesting mechanisms in sensor nodes can be leveraged for security as well. The authors' work is based on multi-authority Ciphertext Policy Attribute Based Encryption (CP-ABE) and presents how to mitigate the CP-ABE cryptographic operations with the help of Access control for GREEn wireless sensor networks (AGREE) framework. The idea is to pre-compute and cache appropriate CP-ABE-encrypted keys such that CP-ABE encryptions are minimal when there is no energy available. The proposed framework is evaluated with simulations and validated byreal-world energy-harvesting traces collected indoors as well as publicly available traces of radiant light energy.

The paper of M. Scatà et al. is based on the assumption that the nodes of a Wireless Sensor Network, deployed on a general topology, should follow a bio-inspired approach to respect the trustworthiness, information load, risk and energy-saving requirements, under bounded conditions of time, knowledge and computational power. Their model is based on a hierarchical clustering method and an aggregation/rejection mechanism, which follows sociological and heuristics theories. The model follows the principle of sense of community and the logic of tie for similarity. The main target is to integrate the inherent cooperation of a multi-agent system with the intelligence of Internet of Things entities.

P. Jokar et al. present in their paper a spoofing detection method for wireless networks based on a spatial correlationmodel for the received signal strength level using both magnitude and frequency features; the authors demonstrate the characteristics and performance gains of their method using an experimental IEEE 802.15.4 network testbed focusing on various metrics that include detection rate, resistance to environmental changes, and detection of high rate attacks.

S. Raza et al. propose in their paper an intrusion detection system with an integrated mini-firewall to prevent a range of routing attacks on resource-constrained devices in the context of the Internet of Things; they implement their proposed techniques in the open source Contiki operating system and evaluate their performance characteristics focusing on various metrics that include detection rate, protocol overhead, energy consumption, and storage memory requirements.

1570-8705/$ - see front matter
http://dx.doi.org/10.1016/j.adhoc.2013.06.006

J. Duan et al. address the access control issue in Wireless Sensor Network and define a distributed andfine-grained access control model based on the trust and centrality degree (TC-BAC). Their solution uses the combination of trust and risk to grant access control. To meet the security requirements of an access control system with the absence of Certificate Authority, a distributed trust mechanism is developed to allow access of a trusted node to a network. TC-BAC guarantees remote deployment, distributed configuration, and multi-domain access.

The paper of A.I González-Tablas Ferreres et al. defines a novel privacy-aware system for the on-the-fly verification of mandatory technical and administrative documentation of motor vehicles. In case of violation of the required regulations, the vehicles will be identified and sanctioned whereas those vehicles, observant of the mandatory regulations, will maintain anonymity and non-traceability of their whereabouts.

The paper of T. Kothmayr et al. faces the problem of secureauthentication in Internet of Things domain introducing the first fully implemented two-way authentication security scheme for the Internet of Things based on existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol. The suitability of the solution for hardware platform of Internet of Thing is extensively evaluated.

Furthermore, the paper of L. Veltri et al. presents a novel centralized method to efficiently distribute and manage a group key in generic ad hoc networks and Internet of Things. Such a solution reduces the computational overhead and network traffic due to group membership changes caused by users' joins and leaves. Two scenarios have been investigated: i) secure data aggregation in IoT and ii) Vehicle-to-Vehicle (V2V) communications in Vehicular Ad-hoc Networks (VANETs).

Sabrina Sicari
Dipartimento di Scienze Teoriche e Applicate (DiSTA)
Facoltà di Scienze Matematiche,
Fisiche e Naturali - Varese Università degli Studi dell'Insubria,
Italy
E-mail address: sabrina.sicari@uninsubria.it

Stephen Hailes
Department of Computer Science,
University College of London,
London WC1E 6BT, UK

Damla Turgut
Department of Electrical Engineering and Computer Science,
University of Central Florida,
Orlando, FL 32816-2362

Sanaa Sharafeddine
Division of Computer Science and Mathematics,
Lebanese American University, Beirut 1102 2801,
Lebanon

Uday B. Desai
Indian Institute of Technology Hyderabad,
Yeddumailaram 502205, Andhra Pradesh,
India

Available online 29 June 2013