IoT Technology Tracking and Industrial Requirements for Security, Privacy and IPR/Data Protection

Project Acronym	IoT4Industry
Document-Id	D.2
File name	
Version	FINAL document
Date	Start: 01 October 2014 End: 31 September 2015
Author(s)	Dr. Violeta Damjanovic-Behrendt Robert Bob Mulrenin
QA Process	Georg Güntner

Table of Content

IoT4Industry in a Nutshell

IoT4Industry is an exploratory project funded by the Austrian Research Promotion Agency, for the period October 2014 – September 2015. It stands for "Secure, Privacy-preserving Agents for the Industrial Internet". The core research areas of IoT4Industry relate to security, privacy and IPR/data protection requirements, translated into game-theoretic agent behavior, which is simulated in a demo factory floor environment, supporting a supply chain negotiation. A demo factory floor is implemented within our IoT-lab, which is located at Salzburg Research.

While it is still not clear which protocols and technologies will become mainstream for the Industrial Internet, it has become clear that security and privacy will feature strongly in any risk assessment concerning the adoption of practices using the Industrial Internet. Thus, in IoT4Industry, we focus on the use of policy-enacting, multi-agent systems that securely manage machines and manufacturing cells, and we build a feasibility demonstrator based on open source tools and firmware. In addition, IoT4Industry helps us to prepare for internationally recognized contributions to science and technology in the field of Industrial Internet, notably in Horizon 2020.

IoT4Industry Task 2 Description

(from the *IoT4Industry* project proposal)

D2: IoT Technology Tracking and Industrial Requirements for Security, Privacy and IPR/Data Protection

Goals:

1. Report on IoT frameworks as they emerge
2. Catalogue of industrial needs w.r.t. IoT security
3. Understanding of security concerns from industrial practitioners

Description of the content

We will start our investigation by inviting three experts from production companies in order to elicit their expectations and security needs in an IoT/Industrial Internet scenario. These specific views will be balanced with desktop research on emerging requirements, gleaned from the on-line discourse in the field, and from following the relevant literature.

In parallel with the requirements gathering (technology pull), we will also track developments in the technical and scientific fields, to maintain an up-to-date view of Industrial Internet throughout the duration of the project.

Method

a) Three interviews with invited practitioners to obtain an initial understanding of industry needs

b) Technology tracking activity over the course of the project to keep knowledge of emerging IoT platforms up to date

c) Desktop research following the scientific/technological discourse concerning industrial requirements and expectations vis-à-vis the Industrial Internet

Milestones, results and deliverables

01/2015: Technical report on industrial requirements is published

09/2015: Technology scouting report on emerging IoT platforms for Industrial Internet

1. Problem Statement

A significant growth in the number of objects that are connected with the existing Internet infrastructure through various standards and communication protocols, leads to a new technological paradigm, known as the **Internet of Things (IoT)**. The research area of the IoT embraces diverse technological fields such as electronic engineering, mobile and wireless communication, computer science, which are additionally supplemented by technologies such as Wireless Sensor Networks (WSN), Machine-to-Machine (M2M) interfaces, RFID, and more. The idea of the IoT paradigm is to connect zillions of objects from both physical and virtual environments, to provide data exchange between those objects, and support decision making in a more federated way, in order to create smart environments for logistics, environmental monitoring, manufacturing and industry.

However, the challenges around the deployment of the IoT are many, ranging from IoT architectures, sensor development, real time processing, data analytics and storage, services, and communication, to the privacy and security of services, processes, individuals and objects involved in IoT. For example, a recent report on the IoT, published in January 2015 by the Federal Trade Commission (FTC) "... *urges companies to adopt best practices to address consumer privacy and security risks.*" The FTC recommends a series of concrete steps that businesses need to take in order to protect consumers' privacy and security [FTC15]:

- *build security into devices at the outset, rather than as an afterthought in the design process;*
- *train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;*
- *ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers;*
- *when a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk;*
- *consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;*
- *monitor connected devices throughout their expected life cycle, and where feasible, provide security patches to cover known risks.*

Furthermore, the authors in [FTC15] recommend the use of the **data minimization approach** for the companies, by limiting the collection of consumer data, and retaining the necessary information only for a set period of time: "*... companies can choose to collect no data, data limited to the categories required to provide the service offered by the device, less sensitive data; or choose to de-identify the data collected.*" This is not an easy step in IoT, where anyone can access ubiquitous services anyway and anytime, process information obtained from heterogeneous resources, and exchange the results interpreted from various perspectives. Therefore, the design and deployment of efficient security and data privacy mechanisms in IoT is considered to be of great importance.

In parallel, the real success and advancement of IoT systems depend on various security and privacy aspects of the IoT, bringing the protection of sensitive data exchanged through IoT as one of the biggest IoT challenges today. For example, the user data can be exposed to unlawful surveillance, data profiling, intrusion in private life, unauthorized access to personal data, infection by malware, etc. [WP29-14]. At the same time, user might easily lose track of the existing interconnected devices, or on intended usage of data created by IoT systems. Similarly, the industrial organisations strive to ensure that their services are equipped with the privacy-friendly default mechanisms, as expected by the EU citizens.

Our motivation in *IoT4Industry* is threefold: (i) to understand the IoT conceptually, (ii) to overview and elaborate on the current state of Internet security and privacy, and (iiI) to explore how to bridge the current constraints with requirements that can assure security, privacy and data protection in the IoT. Above all, we want to investigate current technologies and challenges in privacy and cybersecurity with the aim to help users in industry gain a better understanding of IoT potentials, technological benefits, and dangers. Herein, we explore various mechanism with the potential to control IoT devices, and we particularly focus on those solutions that could benefit from **knowledge-driven approaches**: for example, Semantic Web technologies that can facilitate data aggregation, cross-referencing, data analytics, and enable services and applications to make better decisions. However, quality of data may vary dramatically due to **data obfuscation** (c.f. hiding data due to policy constraints). To assess the quality, reliability and trustworthiness of connected objects and their data, we would explore the role of **data provenance** (information about contextual evidence of entities, services, objects in the IoT) based on the W3C PROV-O ontology (provenance ontology) and its data model supporting the interoperable interchange of provenance information in heterogeneous environments (c.f.

http://www.w3.org/TR/prov-overview/).

Document organization. After a brief description of the problem statement, we continue this report overviewing the state of the art in privacy, security, Intellectual Property Rights (IPR) and data protection in the IoT. **Section 2.1** explores the main privacy and data protection challenges in the IoT, which are related to privacy models, privacy mechanisms and data access control. **Section 2.2** discusses security challenges in IoT, including security vulnerabilities, the detection and prevention of attacks in IoT, data provenance and, game-theoretic approach to IoT security, by differentiating between game-theoretic model used to (i) prevent Denial of Services (DoS) attacks, (ii) detect intrusion, (iii) strengthen security, and (iv) detect coexistence with malicious sensor nodes. Please note that our next report, D.3 *"Specifying Game-Theoretic Behaviour for Agents in Industrial Supply Chain"*, presents an additional set of game-theoretic algorithms targeting supply chain negotiation rather than privacy and security. Our challenge in D.5 *"Security, Privacy, and IPR/Data Protection Requirements Translated into Game-Theoretic Agent Behaviour"* is to work on consolidation of GT algorithms from both privacy and security area and from supply chain management field, in order to find a common GT model to be applied in *IoT4Industry*. **Section 3** looks at the main industrial requirements on security and privacy in IoT, which is based on the following: (i) our discussion with industrial partners during the two *IoT Salzburg* meetups held in March 10, 2015 and May 19, 2015 (c.f. http://www.meetup.com/IoT-Salzburg/), (ii) recently published IIRA (Industrial Internet Reference Architecture), (iii) the RAMI (Reference Architecture Model Industry 4.0), and (iv) the SCISSOR project (Horizon 2020 N644425, February 2015 - January 2018), especially SCISSOR's report "*Technological assessments, scenarios and requirements*". Salzburg Research is the project partner in SCISSOR, with the role to develop a data source registration service to which semantic capability descriptions can be submitted in a form of metadata about the registered sensors and actuators. Based on this registry, semantic browse and search services will be offered for further analysis and decision making. SCISSOR analyses the requirements related to security services, ranging from industrial control processes, pipelines, power generation, nuclear plants, water distribution, ambient control, etc. The analysis covers the real-world expertise of the consortium partners related to the ICS (Industrial Control System) technologies, devices, and network infrastructure. Finally, we would like to mention the "Global IoT Day Vienna" event, 09. April 2015 (for more: http://www.iot-vienna.at/global-iot-day-event/2015/doku.php).

Section 4 gives some conclusion remarks. Note that the document given in Appendix 1 of D.2 is the *IoT4Industry* interview template, which has been created to serve as a basis for the discussion with the industrial experts in Austria, during *IoT Salzburg* meetups.

2. State-of-the-Art in Privacy, Security, and IPR/Data Protection in the IoT

The IoT allows people and objects ("things"), as well as data and virtual environments, to actively participate in virtual process, and interact with each other through various "technologically smart" environments, improving the quality of people's lives, and increasing economic growth. However, the IoT introduces new challenges for both the security of systems and processes (e.g., water distribution) and the privacy of individuals (e.g., purchasing preferences, health condition). For example, the interaction of people with the IoT based environment calls for the protection of their privacy, while the interaction with the services and process in IoT calls for their safety. Hence, in this section, we address the privacy and security in IoT, perceiving possible threats and the ways of preventing attacks.

Note that the following state-of-the-art analysis on security, privacy and data protection, described in Section 2.1, is based on the WP29's[1] document [WP29-14], which identifies the main data protection risks in the context of the EU legal data protection framework. In addition to WP29 document, we consider additional literature discussing challenges and risks related to the IoT systems, such as privacy preservation technologies in IoT, cyber security in IoT, etc.

2.1. Privacy and Data Protection Challenges in the IoT

The existing privacy and security mechanisms in the IoT, such as lightweight cryptography, privacy assurance, and secure protocols, are not protective enough. The authors in [RONL11] emphasize that "*... researchers … must analyze current security protocols and mechanisms and decide if such approaches are worth integrating into the IoT as is or if adaptations or entirely new designs will better accomplish security goals.*"

The authors in [WP29-14] identify the following privacy and data protection challenges in the IoT:

[1] WP29 is an independent European advisory body on data protection and privacy.

- **Lack of data control and information asymmetry:** To prevent situations in which users experience loss of control over data, as a result of multiple interconnections and interactions in the IoT, user's data flows need to be collected and processed in a transparent manner, ensuring privacy and data protection.
- **Quality of the user's consent:** Many IoT devices (objects) are designed neither to provide information about their nature (e.g., many IoT devices cannot be distinguished from "non-connected" ones) nor to provide a mechanism for obtaining the user's consent. At the same time, these devices can embed various motion sensors, cameras, microphones, etc. , which can record and transfer data without users being aware of it. Such lack of information constitutes a significant barrier to demonstrating valid consent under EU law, according to which the data subject must be informed about the usage of their data. Some possible ways to offer a data subject real control over her data could be supported using:
    - *Privacy Proxies*, which define sensor-policy pairs that authorize, limit or reject access to sensor data by third parties;
    - *Sticky Policies,* as a way to establish the context of use of the data, the purposes, policies on third party access and a list of trusted users.
- **Inferences derived from data and repurposing of original processing:** The IoT systems allow for *sensor fusion*, which is a process of using sensor data collected by other parties and from different sources, for secondary uses. For example, the gyroscope from a smartphone can be used to reason about the individual's driving habits, or motion sensors that count the number of steps, which can be used for reasoning about the user's physical condition. Hence, it is important for IoT stakeholders to assure the users that the data is used only for predefined and known purposes.
- **Intrusive bringing out of behaviour patterns and profiling:** Generating knowledge from various sensor sources, analysing and reasoning on top of sensor data, can reveal private aspects of user's habits, user's behaviour patterns and preferences. Such a trend might be very intrusive on the private life and the intimacy of individuals and must be closely monitored.
- **Limitations on the possibility to remain anonymous when using services:** Clearly, remaining anonymous and preserving privacy in the IoT becomes increasingly difficult with the current proliferation of sensors. For instance,

wearables kept in close proximity of data subjects, result in the collection of multiple MAC addresses of multiple sensor devices, which can be used for a range of purposes, including location analytics or the analysis of movement patterns of crowds and individuals.

2.1.1 Privacy models

Regarding techniques designed to protect user privacy, we would like to mention models such as the k-anonymity [SWEE02], data transformation/ randomization, the cryptography, and cryptographic techniques, such as Secure Multiparty Computation.

The k-anonymity model distinguishes the following three entities [SWEE02]:

- individuals, whose privacy needs to be protected,
- the database owner, and
- the attacker.

This model assumes both the domain of the data (the nature of the domain, its attributes and their values, e.g. a height of an individual) and the algorithms used for anonymization are known to attackers. The k-anonymity model of privacy was studied intensively in the context of public data releases in [AFKM05] [BAAG05] [BOYD05] [IYEN02] [SWEE02].

The authors in [SEN11] introduce the idea of **Secure Multiparty Computations (SMC)** in the context of IoT. SMCs "*are cryptographic techniques that enable computations on data received from different parties in a way that each party knows only its own input and the result of the computations"* [GOLD97]. Practically, the SMC functions operate on top of private data that two or more parties contribute to the particular computation, without allowing other participants or third party to access data. The authors in [GOLD97] defines SMC "... *as a mechanism to compute a function* $f(x1, x2, \ldots, xn)$ *with private inputs* $x1, x2, \ldots, xn$ *in a distributed environment with* n *participants, where each participant* i *knows only its input* xi *and no other information, except the value of the output* $f(x1, x2, \ldots, xn)$*".*

The authors in [DUAT01] discuss several efficient solutions to the general SMC problem, for ubiquitous environments with either energy or computational or communication resources constraints. These solutions are often problem-specific and may be resource demanding. In the following, we summarize examples of resource efficient SMC:

- ***the secure sum protocol*** [CKVL02], which tries to find the best match between the user privacy protection and the service efficiency;
- ***the homomorphic encryption*** [BENA94] [PAIL99] [NACC98], which allows for a specific algebraic operation to be executed without decrypting the data;
- ***the location- and identity-based encryption*** of the 2G/3G mobile systems, which is based on three-way authentication [KOOL05];
- *privacy preserving online dating systems*, and/or *privacy preserving service discovery systems*, can be seen as ***access control systems***, offering user's identification without revealing her identity;
- ***privacy preserving attribute-based access control system***, which protects user identity by enforcing access control based on required attributes [FRAL06];
- ***private collaborative forecasting and benchmarking***, which is based on the computation of the aggregated results, while private data remain secret [ABLF04].

The authors in [SIN11] noticed that "...*most of the SMC protocols require considerable computational and communication overhead, and are inefficient in real world ubiquitous applications.... The future research effort should attempt to develop security and privacy models that may provide low-cost practical solutions with acceptable security level for a given type of application.*"

2.1.2 Privacy mechanisms

The authors in [RONL11] discuss several privacy mechanisms, such as: privacy by design, data transparency, data management, trust and governance. In our analysis, we add to it mechanisms such as obscurity by design, identity management, data obfuscation, tamper-proofing, watermarking or fingerprinting.

Privacy by design mechanism provides users with the tools created to support the management of their own data. For example, whenever users produce a data fragment, they can use dynamic consent tools that permit certain services to access as little or as much of that data as desired [RONL11]. The implementation of the privacy by design faces a number of challenges, including a lack of specificity, and weak market forces motivating adoption [RUBI12]. To date, it includes mainly back-end implementation principles, such as data minimization and security [GÜTD11] [KUFK11] [SPCR09].

Obscurity by design mechanism incorporates flexible set of principles, which designers should consider when building privacy mechanisms. The authors in [STHA12] discuss obscurity by design in the context of Social Media, and define obscurity as follows: "*Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors: 1) search visibility, 2) unprotected access, 3) identification, and 4) clarity.*"

Data transparency mechanism informs users about entities involved in managing their data. This mechanism will affect both stakeholders and users, in sense of the amount of user's personal (or corporates) data, which are provided to IoT services.

Data management mechanism includes data management policies and policy-enforcement mechanisms, which "*requires interpreting, translating, and optimally reconciling a series of rules, each of which might be in a different language. And any policies must align with legislation on data protection, which itself could change.*" [RONL11] A well known protocol and tool suite for specifying privacy policies of both Web sites and users is *Platform for Privacy Preferences (P3P)* [CRAN03] [LIBH05]. The authors in [REBE03] notice that privacy solutions for the Web (notably P3P-based) would be better utilized if they were a part of data they are supposed to protect. Hence, in [LIBH05], the idea of coupling privacy protection mechanisms with metadata has been proposed based on a work presented in [BHLX04] [REBE03].

Identity management mechanisms differ between several object identity principles, such as core and temporary identities, identity of a group of objects, identity based on owner's identity or some specific features (quantity, ingredients, etc.), authorization and authentication. One approach to identify the device or its owner is known as ***digital shadowing*** [SAGI09], which only implicitly identifies the owner. In other words, digital shadowing is based on the notion of a digital shadow: user's sensors do not store the owner's real identity, only a virtual identity that contains information about the user's attributes and their interactions with the IoT environment.

Digital shadows could be further linked to RFID tags that are accessible only to authorized readers. This implies that an unauthorized RFID reader is not able to track the user. This concept is known as - ***revocable access delegation*** [RERG10]. Another concept in which an RFID reader scans the tags embedded in some object, downloads the companion privacy policy, and compare two of them is called - ***the privacy coach*** [BROE10]. If the company's privacy policy does not match the user's preferences, the user can choose not

to use it at all. Additionally, whenever an RFID reader tries to read the mobile phone's signal, the phone can check the reader's privacy policy and ask for user's consent.

Trust and governance frameworks are considered as the enforcing mechanisms towards simplification of data protection: **trust** should reduce the uncertainty of objects interacting in a dynamic and ubiquitous IoT environment, while **governance** framework should reduce liability of billions of IoT objects in the environment. Recently, the authors in [HGZZ14] presented a data-driven qualitative model for the evaluation of the trust value of sensed products in supply chains. In this model, a big volume of sensed data is used through a Bayesian network to calculate a quantitative trust value, rather than expert's subjective experiences and knowledge. The authors in [HGZZ14] additionally explore other trust models designed for IoT, such as:

- TRM-IOT model uses only reputation as the main index of trust [CHCH11];
- A multi-dimensional trust evaluation model for large-scale P2P computing, as proposed in [LIZY11], combines several factors to evaluate the trust, e.g., assumptions, expectations, behaviors, etc.;
- Hexmoor et al. in [HEWB06] proposed a trust-based security model, in which evaluation requires behavior data and expert's experiences;
- Wang et al. in [WAWU10] proposed a topology transform-based recommendation trust model, which can relieve the malicious effects on the accuracy of recommendation trust. This model uses recommendation mechanisms that are rather not suitable in the IoT;
- Shi et al. in [SHBA05] proposed a trust model that assists users and machines in online decision-making using past behavior as a predictor of likely future behavior.

Other approaches for protecting software clients or agents from a malicious host include [COTH00]: (a) data obfuscation, (b) tamper-proofing, and (c) watermarking or fingerprinting. **Data obfuscation** is "*a mechanism for hiding private data by using misleading, false, or ambiguous information, with the intention of confusing an adversary*" [BRNI11]. This mechanism acts as a noisy information channel between a user's private data and an untrusted observer [CHPA08] [SHOK15]. Some problems related to data obfuscation that still need to be addressed in the IoT are as follows:

- how to design an obfuscation mechanisms that protects the privacy of the user and, at the same time, imposes a minimum utility cost, and

- how to guarantee the user's privacy, despite the lack of a single best metric for privacy.

Regarding privacy protection, there are two major metrics proposed in [SHOK15]:

- **Differential privacy**, which limits the information leakage through observation, but does not reflect the absolute privacy level of the user; and
- **Distortion privacy** (inference error), which measures the error of inferring user's secret from the observation. This requires assumption of a prior knowledge which enables quantification of absolute privacy, but is not robust to adversaries with arbitrary knowledge.

Thus, either of these metrics alone is incapable of capturing privacy as a whole. They rather complement each other: Differential privacy is sensitive to the likelihood of observation given data. Distortion privacy is sensitive to the joint probability of observation and data.

The authors in [SHOK15] model the optimal obfuscation mechanism that minimizes utility loss, satisfies differential privacy, and guarantees distortion privacy, given a public knowledge on prior leakage about the secrets. The authors measure the involved metrics based on separate distance functions defined on the set of secrets. They model prior leakage as a probability distribution over secrets, which can be estimated from the user's prior data.

The problem of optimizing the tradeoff between privacy and utility has been discussed in the literature, but notably in the context of statistical databases [BRNI10] [GHRS09] [GHRS12] [LHRM10] [BRSH08] [IMWB14]. A protection mechanism for distortion privacy metric can be designed to be independent of the adversary's inference algorithm (e.g., Bayesian inference [MCKY03] [BERG85] as privacy attacks). Distortion privacy, which evaluates privacy as the inference error [STBH11], is a follow-up of information theoretic metrics for anonymity and information leakage [DSCP03] [SEDA03]. This class of metrics is concerned with what can be inferred about the true secret of the user by combining the observation (or obfuscated information) and prior knowledge. The problem of maximizing privacy under utility constraint, assuming prior knowledge, is proven to be equivalent to the user's best strategy in a zero-sum game against adaptive adversaries [STTH12]. With this approach, one can find the optimal strategies using linear programming. However, if we want to guarantee a certain level of privacy for the user and maximize her utility, the problem cannot be modeled as a zero-sum game anymore and there has been no solution

for it so far. Hence, the authors in [SHOK15] adapt a game-theoretic notion of privacy for designing optimal obfuscation mechanisms against adaptive inference. They formulate this game as a **Stackelberg game** and solve it using linear programming. They add the differential privacy guarantee as a constraint in the linear program and solve it to construct the optimal mechanism. The result is that not only the perturbed data samples are indistinguishable from the true secret (due to differential privacy bound), but they cannot be used to accurately infer the secret using the prior leakage (due to distortion privacy measure). Finally, the authors in [MZAB12] explore examples combining security and game theory.

2.1.3 Data Access Control in the IoT

In the IoT, both the device manufacturer and the service provider may have access to more data that could be analyzed [WP29-14]. Third parties may want to make use of this data for different purposes in order to infer various information about users; for example, user's habits, daily routines, health and physical conditions, political opinions, location analytics, etc. The Article 6 of Directive 95/4/EC constitute a cornerstone of EU data protection law, emphasizing the following principles:

- personal data should be collected and processed **fairly** (never without the individual being aware of it) and **lawfully**;
- data can only be collected for specified, explicit and legitimate purposes (**the purpose limitation principle**);
- data unnecessary for a specific purpose should not be collected and stored "just in case" or because "it might be useful later" (**the data minimization principle**);
- personal data collected and processed in the context of IoT is kept for **no longer than is necessary**.

In addition, the owners of data (data subjects) must have a possibility to revoke any prior consent given to a specific data processing and to object to the processing of data relating to them. The exercise of such rights must be possible without any technical or organizational constraints or hindrances and the tools provided to register this withdrawal should be accessible, visible and efficient. Furthermore, some wearable IoT devices (glasses, clothes, etc.) must include a possibility to disable the "connected" feature of the thing and allow it to work as the unconnected item. **Today practices in the design of IoT devices still DO NOT PROVIDE ANY CONTROL of the data.**

2.2. Security Challenges in the IoT

The development of the IoT entails significant security concerns. For example, the authors in [WP29-14] identify several challenges that force device manufacturers to balance the implementation of confidentiality, integrity and device security, with the need to optimise battery efficiency (the use of computational resources and energy). The current solutions are usually compromise solutions, offering low security, the ease of surveillance practices and data breaches, for the price of better battery efficiency. This comes with the risk that the IoT "*may turn an everyday object into a potential privacy and information security target, while distributing those targets far more widely than the current version of the Internet*."

The security in the IoT is not only about securing devices; it might affect other IoT components, such as the communication links, storage infrastructure, data access controls, data itself. All IoT components must be designed and manufactured in a way that guarantees high security standards. The compliance with the Article 17 of Data Protection Directive 95/46/EC should be additionally presented.

Before trying to use the software to secure any system, it is necessary to proof the hardware itself, and to create a security protocol for selecting securable devices. It should include any device connected in the network, such as USB sticks or chargers, and power outlets, etc. IoT sensors that allow direct wireless connection might also be hopeless to secure the network; preferably routers or other gateways will enhance security of the sensor array.

The future communication between agents and various devices may use **homographic encryption** to encrypt all data flowing in the system. The encrypted data can be passed with an infrastructure and operations can be performed on the data. Complete homographic encryption libraries are not yet offered; there are only simple research based libraries.

In the following, we summarize several recommendations on securing the IoT:

- Identification of the security weaknesses of any hardware and IoT devices, including USB connectors, sticks, power extenders, etc.;
- IoT devices should support an API that can be secured either by the vendor mechanism or by an IoT stack local security gateway. Vendors offering "security by obscurity" should be encouraged to offer alternative solutions;
- Users or integrators may not use USB related devices unless USB protection is utilized to prevent attacks on the whole network;

- The IoT stack must offer a local security gateway and registration mechanism for any registered IoT device;
- The IoT stack should simplify how components or agents interact. For example, peers (agents or system components) could use a secure proxy (a master server peer in P2P network) for communicating with other peers or agents.

2.2.1 Top security vulnerabilities in the IoT

The Open Web Application Security Project (OWASP)[2] identifies 10 top vulnerabilities in the IoT, discusses their technical and business impacts, and the ways to prevent application attacks and reduce network vulnerabilities. Here is a brief overview of OWASP's top IoT vulnerabilities:

- **Insecure Web interface** (e.g., ensuring that weak passwords are not allowed; account lockout after 3 -5 failed login attempts, etc.);
- **Insufficient Authentication/Authorization** (e.g., ensuring that granular access control is in place when necessary; credentials are properly protected; password recovery mechanisms are secure, and implement two factor authentication where possible, etc.);
- **Insecure Network Services** (e.g., ensuring that only necessary ports are exposed and available; services are not vulnerable to buffer overflow and fuzzing attacks);
- **Lack of Transport Encryption** (e.g., ensuring that data is encrypted using protocols such as SSL and TLS while transiting network, etc.);
- **Privacy Concerns** (e.g., ensuring that only data critical to the functionality of the device is collected; not collecting sensitive data; data anonymization, etc.);
- **Insecure Cloud Interface** (e.g., ensuring that credentials are not exposed over the internet; two factor authentication implemented);
- **Insecure Mobile Interface** (e.g., ensuring that user accounts can not be enumerated using functionality such as password reset mechanisms; implementing two factor authentication if possible);
- **Insufficient Security Configurability** (e.g., ensuring the ability to separate normal users from administrative users, the ability to force strong password policies, etc.);
- **Insecure Software/Firmware** (e.g., ensuring that the device has the ability to

[2] OWASP project: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=Main

update (very important); the update file is encrypted using accepted encryption methods, etc.);

- **Poor Physical Security** (e.g., ensuring that data storage medium can not be easily removed; device can not be easily disassembled, etc.).

2.2.2 Detecting and preventing attacks in the IoT

Attacks in the IoT may lead to disconnecting significant parts of the network, replication of strategic nodes in the network, and more. Existing approaches to sensor network security are mainly based on detection of distributed, replicated nodes, either by using the topology of the network to detect replication (**line-selected multicast**), or by exploiting the birthday paradox to detect replicated nodes (**randomized multicast**) [PAPG05].

The authors in [KAWA02] note that security issues present in ad-hoc networks are similar to those in sensor networks (as previously discussed in [ZHHA99] [STAN99]), but the defense mechanisms developed for ad-hoc networks are not directly applicable to sensor networks. The reasons for it could be the following:

- **public key cryptography** used in some ad-hoc network security mechanisms for authentication and secure routing protocols [ZHHA99] [HUBC01] [KZLZ01] [ZAPA01] [BITR01] is too expensive to be implemented in sensor nodes;
- **symmetric key cryptography** for ad-hoc networks in secure routing protocols have been proposed in [HUJP02] [HUPJ01] [BHRB01] [PAHA02]. These protocols are based on source routing or distance vector protocols, but they are unsuitable for sensor networks;
- Marti et al. in [MGLB00] and Buchegger and Boudec in [BUBO02] consider the problem of minimizing the effect of misbehaving or selfish nodes on routing through punishment, reporting, and holding grudges. They introduce two extensions to the Dynamic Source Routing Protocol (DSR), called **Watchdog** (detects misbehaving nodes by overhearing transmission, although it might not detect the presence of ambiguous collisions, receiver collisions, limited transmission power) and **Pathrater** (avoids routing packets through misbehavior nodes);
- Perrig et al. in [PSWC01] present two building block security protocols optimized for use in sensor networks, such as SNEP and (micro)TESLA. SNEP provides confidentiality, authentication, and freshness between nodes and the sink, and (micro)TESLA provides authenticated broadcast.

The authors in [KAWA02] analyze **the security features of the major sensor network routing protocols**, crippling attacks against those protocols, and suggest possible countermeasures. One of the major assertion here is that "*sensor network routing protocols must be designed with security in mind, which is the only effective solution for secure routing in sensor networks".* Most network layer attacks against sensor networks falls into one of the following categories:

- **Spoofed, altered or replayed routing information**: Spoofing allows for many other forms of network attacks, such as creating routing loops, generating false error messages, partitioning the network, etc. The authors in [SRUM13] propose a method for detecting spoofing attacks that utilizes K-means cluster analysis (as localization algorithms), and integrate this method into a real time indoor localization system, which localize the position of the attacker.
- **Selective forwarding:** A simple form of this attack is a case when a malicious node behaves like a black hole, and refuses to forward every packet she sees. A more subtle form of selective forwarding attack is a case when an adversary selectively forwards packets.
- **Sinkhole attacks:** the adversary's goal is to lure the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center.
- **Sybil attacks:** a single node that presents multiple identities to other nodes.
- **Wormholes:** an adversary is tunneling messages received in one part of the network over a low latency link and replays in a different part [HUPJ02] [KAWA02].
- **HELLO flood attacks:** this attack uses a single hop broadcast with the aim to transmit a message to a large number of receivers [KAWA02].
- **Acknowledgement spoofing:** an adversary is spoofing link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Acknowledgment spoofing is about convincing the sender that a weak link is actually strong, or that a dead or disabled node is alive, then transmitting packets on exactly those links.

Protecting sensor network routing protocols against outsiders, Sybil attacks, HELLO floods, spoofing, can be achieved by augmenting existing protocols with the mechanisms such as: link-layer encryption and authentication using a globally shared key, multipath routing,

identity verification, bi-directional link verification, and authenticated broadcast [KAWA02]. Cryptography itself is not enough to defend against laptop-class adversaries. Hence, **the design of the secure routing protocol need to be considered from the early design and the development of sensor network, in order to provide an effective detection and prevention of attacks in the IoT.**

Table below summarizes on various types of attacks and their countermeasures. For example, HELLO flood attack responds to bi-directional link verification, and/or authenticated broadcast, but cannot be solved through link-layer encryption.

	Link-layer encryption and authentication using a globally shared key	Multipath routing	Identity verification	Bidirectional link verification	Authenticated broadcast
Sybil attack	+		+	+	+
Selective forwarding	+	+			
Sinkhole attack	+	+			
Wormhole attack	-	+			
HELLO flood attack	-			+	+
Spoofing attack	-				+

2.2.3 Securing Data Provenance in the IoT

The provenance, which is also known as Information lineage, or archival principles, has been extensively studied in archival theory. The authors in [HASW07] define data provenance as a summary of "*the history of the ownership of the item, as well as the actions performed on it*". Furthermore, the authors in [HASW07] explore the secure provenance problems and challenges in the area of computing and legal proceedings that

involves data. They define the *security components model,* which consists of **confidentiality**, **integrity** and **availability** (CIA) as the main facets of data security.

The authors in [SIPG05] present taxonomy of the application of provenance in science, and classifies provenance systems into the following three categories: database-oriented, service-oriented, and miscellaneous. For example, [WIDO05] presents a system called Trio, which purpose is to provide lineage and provenance in databases. The examples of provenance management systems for scientific computing include: Chimera [FVWZ02] (physics and astronomy), myGrid [ZGSB04] (biology), CMCS [MYER04] (chemical sciences), and ESSW [FRBO01] (earth sciences).

Buneman et al. in [BUKT00] explore various aspects of provenance of electronic records, and introduce the notions of ***why-provenance*** (process that generated the data) and ***where-provenance*** (the origin of data). Workflow provenance in scientific computing has been studied in [BADI06]. Provenance of data streams has been presented in [VIPL06], while the use of provenance in generating trust in social networks is explored in [GOLB06].

The authors in [LKMS04] emphasized the need for trust and provenance in information retrieval. **Provenance as a mechanism for establishing trust in data**, as defined by the W3C Provenance Working Group, represents "*... information about entities, activities, and people involved in producing a piece of data or thing, which can be used to form assessments about its quality, reliability or trustworthiness.*" [3]

The existing implementations of the provenance mechanisms include mainly systems for collecting provenance information, such as Provenance Aware Storage System (PASS) [MURE06], and Lineage File System [SACA05]. In parallel, secure file systems have been developed to store and secure data files in untrusted servers [HASA05]. Existing techniques for detecting breach of integrity, as described in secure file systems, can be utilized to provide trustworthy provenance.

Corruption of a provenance may lead to incorrect and possible harmful conclusions, leakage of privacy-related information (e.g., revealing information such as social security numbers) (see http://www.w3.org/TR/2013/NOTE-prov-aq-20130430/), etc. Publishing information about provenance must include access controls and mechanisms for enforcement and auditing of privacy policies (for example, standard HTTP authorization mechanisms can restrict access to resources, returning *401 Unauthorized*, *403 Forbidden*, or *404 Not Found* as appropriate, or SSL, rate-limiting, spam filters, moderation queues,

[3] W3C Provenance Working Group: http://www.w3.org/TR/2013/NOTE-prov-overview-20130430/

user acknowledgements and validation). Reasonable preventions should be taken to prevent malicious use, such as Distributed Denial of Service (DDoS) attacks, Cross-Site Request Forgery (CSRF), spamming and hosting of inappropriate materials, or provenance pingback with a malicious site that presents a pingback URI executing an instruction on a different web site.

Provenance in the IoT brings many novel applications, as summarized in [COCT14]:

- supporting the understanding and reuse of sensor data, including data that has been aggregated or processed [PAHE08];
- ensuring the correct attribution of publicly available sensor data [CHSV10];
- supporting users trace the involvement of sensor data in experiments for reproducibility purposes [HESN13];
- searching for, and identifying sensor data within data stores [LNHM05];
- verifying data transmitted through nodes in a sensor network [SSGB12];
- supporting quality [CEBM13] and trustworthiness assessments [UMBR12], and many more.

2.2.3.1 Data Provenance and Sensor Ontologies

There exists a significant research track about the data provenance and sensor ontologies, for example:

- **The Open Provenance Model (OPM)** [MCFF11] is used by Lie et al. [LFMR10] to record the provenance of sensors within Tupelo, a semantic Content Management System (CMS). In Tupelo, data is modeled as the OPM equivalent of `prov:Entity` and actions as `prov:Activity`; no further alignments are described.
- Patni et al. [PSHS10] use **the Provenir ontology** [SBGS09] to capture and store the provenance of sensor data in their sensor management system. Alignments between Provenir ontology and the Sensor ontology are defined through series of `rdfs:subClassOf` and `rdfs:subPropertyOf` relationships that model e.g., observation values as the Provenir equivalent of `prov:Entity`, and the sampling time property as the equivalent of `prov:atTime`.
- Stasch et al. in [SSAK11] describe their **extension of the Semantic Sensor Network Ontology (SSNO)** to represent aggregations of observations, and use the

Provenance Vocabulary and OPM to record each aggregated provenance. However, it is unclear if the remaining SSNO concepts have been aligned to a provenance model, or if these alignments have been explicitly defined in an ontology to enable their reuse.

- Corsar et al. in [CEBM13] define an **alignment between the SSNO and PROV-O (W3C Provenance Ontology)**, which covers only relationships between the SSNO observation, sensor, and sensing concepts and the PROV-O entity, agent, and activity concepts, respectively. The alignment is used to integrate SSNO data with other data via the PROV-O model to support quality assessment of observations from citizen sensors.
- Finally, the **W3C Provenance Working Group** defines the following:
    - PROV-DM, data model for provenance, which introduces a set of concepts to represent provenance information in a variety of application domains, in order "*to enable the interoperable interchange of provenance information in heterogeneous environments such as the Web*",
    - PROV-O ontology, which maps the PROV-DM to RDF (see: http://www.w3.org/ns/prov),
    - PROV-AQ mechanisms for accessing and querying provenance,
    - PROV-CONSTRAINTS, a set of constraints applied to the PROV data model, and more.

  In addition, the W3C Provenance Working Group developed an alignment between the SSNO and PROV-O ontologies, as two major reference models.

2.2.3.2 PROV-DM, PROV-AQ and PROV-O

In the following, we summarize the main idea behind the W3C Provenance Working Group's definitions of (i) PROV-DM, (ii) PROV-O ontology, (iii) PROV-AQ mechanisms.

PROV-DM. Types and relations in PROV-DM are shown in Figure 1.

- **C1: Entities and Activities.** It consists of entities, activities, and concepts such as generation, usage, start, end.
- **C2: Derivations.** It contains derivations and derivation subtypes.
- **C3: Agents, Responsibility, and Influence.** It consists of agents and concepts defining responsibility of agents.
- **C4: Bundles.** It is concerned with bundles, which is a mechanism to support

provenance.

- **C5: Alternate.** It consists of relations between entities, referring to the same thing.
- **C6: Collections.** This component is about collections.

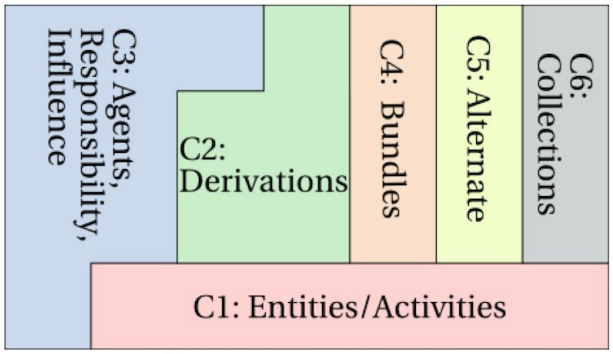

Figure 1: PROV-DM components (source: http://www.w3.org/TR/2013/REC-prov-dm-20130430/#component2)

PROV-AQ (c.f. http://www.w3.org/TR/2012/WD-prov-aq-20120619/) defines mechanisms for accessing, locating and querying provenance information. For example, there are three mechanisms for the resource provider to indicate a provenance-URI or service-URI along with a target-URI, such as:

- The requester knows the resource URI and the resource is accessible via HTTP
- The requester has a copy of a resource represented as HTML or XHTML
- The requester has a copy of a resource represented as RDF (or HTML with embedded RDFa).

PROV-O. The PROV-O ontology encodes the PROV-DM to RDF, using the OWL2 Web Ontology Language. PROV-O is a lightweight ontology that can be adopted in a wide range of applications. It can be used for modeling application-specific provenance details, or as a reference model for creating other domain-specific provenance ontologies.

The PROV-O terms (classes and properties) are grouped into three categories:

- **Starting Point classes and properties** provide the basis for the PROV-O (e.g. classes: `prov:Entity`, `prov:Agent`, `prov:Activity`; properties: `prov:wasGeneratedBy`, `prov:wasDerivedFrom`, `prov:used`, ...). These terms are used to create simple provenance descriptions that can be elaborated using terms from other categories.

- **Expanded classes and properties** provide additional terms that can be used to relate classes in the *Starting Point* category (e.g. classes: `prov:Collection`, `prov:Bundle`, `prov:Person`; properties: `prov:wasQuotedFrom`, `prov:wasInvalidatedBy`, `prov:value`, ...).
- **Qualified classes and properties** provide elaborated information about binary relations asserted using *Starting Point* and *Expanded* properties (e.g. classes: `prov:Plan`, `prov:Role`, `prov:Communication`; properties: `prov:wasInfluencedBy`, `prov:hadUsage`, `prov:hadRole`, ...). The terms in this category are applied using a pattern that differs from those in the *Starting Point* and *Expanded* categories. While the relations from the previous two categories are applied as direct, binary assertions, the terms in this category are used to provide additional attributes of the binary relations.

2.2.3.3 PROV-O and SSNO Ontology Alignment

The authors in [COCT14] present an ontology alignment between PROV-O (http://www.w3.org/ns/prov) and SSNO (Semantic Sensor Networks Ontology) (http://purl.oclc.org/NET/ssnx/ssn), which are both W3C's ontologies. While the PROV-O ontology is a W3C recommendation for the representation and interchange of provenance information on the Web [LSGB14], the SSNO ontology [CBBG12][LHTB12] represents a de-facto standard for the semantic specification of sensors, sensor devices, systems, processes, and observations. The alignment between PROV-O and SSNO considers PROV-O as an upper ontology, which further extends SSNO concepts and properties. This allows for representation of observation details and sensor deployments that are not possible in the SSNO alone, and gives a basis for alignment with Open Geospatial Consortium Observations & Measurements ontologies.

SSNO is built around the *Stimulus-Sensor-Observation pattern* [JACO10] that describes the relationship between an observing `ssn:Sensor`, the `ssn:Property` that is measured, the real-world `ssn:Stimulus`, the `ssn:Sensing` procedure followed and the resultant `ssn:Observation`. The Stimulus-Sensor-Observation pattern is a basis for the alignment to PROV-O.

2.2.4 Game Theory to support IoT security

Symantec's security study from 2012 indicates that cyber attacks are continuing to raise! Only in 2012, cyber attacks increased by 42 percent (c.f. http://bit.ly/1Sz8w2O). In 2013, the Spamhaus/Cyberbunker attack clogged servers with dummy internet traffic at a rate of about 300 gigabits per second. This happened 13 years after the publication of best practices on preventing Distributed Denial of Service (DDoS) attacks, and motivated cyber-security professionals to search for novel approaches to IoT security.

In *IoT4Industry*, we specifically explore a game-theoretic setting for interaction among benign and malicious users. Therefore, we start by examining the recent work on using Game Theory (GT) for both the IoT and Wireless Sensor Networks. Game Theory is a mathematical method with the potential to describe both cooperation and conflicts between rational decision-makers [SWKC12]. It can be used to analyze system operations in decentralized and self-organizing networks, and describe the behavior of players involved in a game. For example, GT addresses problems where multiple players with different objectives compete and interact with each other. From the perspective of Wireless Sensor Networks (WSNs) and the IoT, GT has been proved to be useful in improving WSN performance objectives caused by the limited capabilities of sensor nodes in terms of computation, communication, and energy (e.g., GT can maximize sensing coverage, extend operation periods, or improve security aspects via adequate mathematical generalization). Furthermore, GT mechanisms can be used to monitor behavior of sensor nodes and evaluate reputation of each node based on collected observations. Reputation can be further used to predict the future behavior of other nodes in WSN.

There is already a plethora of research papers describing GT approach to WSNs: [KASI04] [KAIY04] [URBG03] [FEHB06] [BUHS05] [WALI06]. In addition, Machado and Tekinay summarize 29 publications with the focus on the use of GT approaches to formulate problems related to security and energy efficiency [MATE08]. Shen et al. in [SYCY11] summarize another 30 publications of the existing GT approaches to strengthen WSN security.

Commonly used GT methods to solve problems in WSNs can be classified as follows:

- **cooperative GT** - a class of games that studies the behavior of cooperative players and considers the utility of all the players involved in the game. This category of games is also known as **coalitional GT**, and in WSN particularly, allows for a

reduction of power consumption by forming coalitions. For example, some nodes in WSN can form a coalition by transferring data coordinately with the aim to minimize energy consumption;

- **non-cooperative GT** - a class of games that studies behavior of non-cooperative, competing players, and focuses on each user's individual utility, rather than on the utility of the whole network. Mechanism design in non-cooperative GT helps to find the right incentives and ensures that the participants tell the truth (agent obtains maximum profit only by submitting a real bid/ true value);
- **repeated GT** - a class of dynamic games, in which a game is played for numerous times and the players can observe the outcome of the previous game before attending the next repetition [OWEN01]. The interaction between sensor nodes can be modeled by using repeated GT, to prevent the problem of dropping packets attacks in WSN [YAMC08], or prevent passive DoS attacks at routing layer in WSN [AGDA07], etc.
- **evolutionary GT**, and more.

Hackers could attack WSN, and sensitive corporate or private data could be easily compromised. Hence, WSN need to be designed to prevent DoS attacks and detect intrusions, provide secure localization, etc. The authors in [SWKC12] survey the recent developments in the area of GT and GT-based applications in WSNs, such as: routing protocol design, topology control, power control and energy saving, packet forwarding, data collection, spectrum allocation, bandwidth allocation, quality of service control, coverage optimization, and other sensor management tasks (task scheduling, etc.).

Shen et al. in [SYCY11] classify current GT approaches in WSN security into four categories: (i) preventing DoS attacks, (ii) detecting intrusion, (iii) strengthening security, and (iv) coexistence with malicious sensor nodes that is based on signaling games described in [WACK09]. Shen et al. pointed out on several future research areas for ensuring WSN security based on GT, including Base Station credibility, Intrusion Detection System (IDS) efficiency, WSN mobility, WSN QoS, real-world applicability, energy consumption, sensor nodes learning.

In the rest of this section, we present the above mentioned categories of GT methods for WSN security.

2.2.4.1 Preventing DoS Attacks

Denial of Services (DoS) attacks can be passive and active [AGDA07]. In passive attacks, selfish sensor nodes use the network, but do not cooperate with other sensor nodes in order to save battery life for their own communications. In that way, they do not intend to damage other nodes, while in active attacks, malicious nodes damage other nodes by causing network outage by partitioning. The existing non GT mechanisms to prevent DoS attacks in sensor networks are suggested in [AGDA07]:

- **Watchdog scheme**: it identifies misbehaving nodes [MGLB00] using two concepts:
    - *Watchdog* (every node implements constant monitoring). The disadvantage of the Watchdog scheme is that it doesn't solve the collision between malicious nodes [HUSH03]), and
    - *Pathrater* (rates the transmission reliability of all alternative routes to a particular destination node).
- **Rating scheme**: the neighbors of any single node collaborate in rating the node, based on how well the node execute requested functions [MIMO02a] [MIMO02b] [MIMO02c]. The disadvantages of this approach are that evaluated node may be able to cheat easily and the result of the function may require significant overhead to be communicated to the evaluating node [HUSH03].
- **Virtual currency**: This scheme introduces a special type of selfish nodes called *nuglets* [BBCG01] [BUHU01]. The disadvantages of this scheme are that intermediate nodes are able to take out more *nuglets* than they are supposed to, and overhead [HUSH03].
- **Route DoS prevention**: It attempts to prevent DoS in the routing layer via cooperation of multiple nodes [BUBO02].

Apart non-GT mechanisms to prevent DoS attacks in sensor networks, there are GT-based models such as:

- **non-cooperative game** [AGBD05a] [AGBD05b] [SAEP09],
- **cooperative game** [AGBD04], and
- **repeated game** [AGDA07] [YAMC08].

The authors in [AGDA07] present a protocol based on repeated GT, which achieves the design objectives of truthfulness by recognizing the presence of nodes that agree to forward packets but fail to do it (passive DoS). The jamming and anti-jamming attacks are

modeled as a zero-sum stochastic game in [LILQ11], designed to defend DoS attack. Dong et al. [DLLX09] established an attacking-defending game model for detecting active DoS attacks, in which the strategy space and payoff matrix are given to both the Intrusion Detection System (IDS) and the malicious nodes.

2.2.4.2 Intrusion Detection

Research in the area of IDS for WSN has a relatively short history [PAPA06]:

- Marti et al. in [MGLB00] introduce the concept of *Watchdog* and *Pathrater* to identify routing misbehavior;
- Buchegger & Boudec in [BUBO2] extend the work of Marti et al. by replacing the Watchdog with a *Neighborhood Watch* paradigm. They also introduce a Trust Manager, a Reputation System and a Path Manager paradigms;
- Zhang & Lee in [ZHLE00] propose a general intrusion detection and response mechanism for the Mobile Ad hoc NETwork (MANET), in which each IDS agent participates in the intrusion detection and response independently;
- Huang et al. in [HFLY03] extend the work done by Zhang & Lee, by analyzing the routing activities and improving the anomaly detection process by providing more details about the attack types and attack sources;
- Sun et al. in [SUWP03] proposed a Markov chain-based anomaly detection approach for MANETs.

The use of mobile agents in the context of intrusion detection has been explored in both the LIDS project [PPCJ03] and the SPARTA project [KRTO02]. Kachirski & Guha in [KAGU02] propose distributed IDS for the MANET environment [MINP04]. Several GT frameworks for modeling IDS has been presented in [KOLA03] (based on sampling in communications networks), [ALBA04], [PAPA06] (the interaction between an attacker and a host-based IDS is analyzed as a **dynamic two player non-cooperative game**). Reddy in [REDD09] discusses currently available IDS techniques, models attacks using GT and proposes a framework to detect malicious nodes by using **zero sum approach** for nodes in the forward data path. Reddy & Srivathsan in [RESR09] developed a framework to detect malicious nodes using zero sum game approach and selective node acknowledgements in the forward data path. A GT-based scheme is introduced to find out the vulnerable areas in WSN [AGBD04] [AGDB04]. Mohi et al. [MOMZ09] models the interaction of nodes in WSN

and IDS as a **Bayesian game** and use the same concept to make a secure routing protocol. Finally, Michiardi et al. [MIMO02] use **cooperative and non-cooperative GT** to develop a reputation based architecture to enforce cooperation. **Non-cooperative GT-based** schemes could assist detection schemes in improving their performance as well as an efficiency [XHTP11]. Qiu et al. in [QICX10] propose an active defense model for WSN in which the nodes have limited rationality of evolutionary learning ability based on **evolutionary GT.** The nodes can achieve the most effective defense by adjusting their defensive strategies active and dynamic. Jing & Ruiying in [CHDU09] analyze the cooperation stimulation and security in self-organized WSN under a GT framework.

2.2.4.3 Strengthening Security

GT-based approach to strengthening security considers auction theory [AGBD06] and coalitional game [LILY08], as presented in [SYCA11].

Auction Theory for Strengthening Security. There are four major auction formats: English, Dutch, First-Price and Second-Price sealed auctions. The authors in [AGBD06] propose a *Secure Auction-based Routing (SAR) protocol* using the First-Price auction format. Here, the bidder with the highest bid wins the auction and reaches equilibrium, and thereafter the truth bidding becomes a dominant strategy for sensor nodes. Both malicious and truthful sensor nodes compete against each other in order to forward incoming packets and, by doing so, each sensor node improves its reputation among other sensor nodes. *"The payoff of each sensor node is calculated based on battery power and reputation. The authors consider communication and computation of sensor nodes when computing the required power for each sensor node. If a sensor node saves its power by not forwarding incoming packets or dropping them for its selfishness, then it will be isolated from the network and get a bad reputation; otherwise, it will get a good reputation. As a result, sensor nodes prefer to participate in forwarding incoming packets and gaining reputation. Experiment results show that the SAR protocol can guarantee more reliable delivery, and can observe the behavior of sensor nodes and isolate suspicious sensor nodes by defining an acceptable threshold for reputation of sensor nodes."* [AGBD06]

Coalition Game for Strengthening Security. The authors in [LILY08] study how to strengthen security in WSNs by using coalitional game. They propose a throughput characteristic function that describes the expected gain of a coalition from the cooperation. For finding a reliable routing path, a coalition to a weighted and directed graph is

formulated. The number of routing paths is related to the size of the coalition. In order to fairly distribute the gains among all sensor nodes, the authors in [LILY08] consider Shapley value method and prove that it is applicable to the payoff allocation inside coalitions given their proposed throughput characteristic function. Some game rules are defined as follows:

- A sensor node will join into a coalition only if it can create more payoff than being alone;
- A sensor node will deviate from the current coalition and join another coalition only if it can create more payoff in the future than current;
- A coalition will refuse a sensor node if the sensor node cannot increase the total payoff of the coalition;
- A coalition will exclude a sensor node if the sensor node can not benefit the coalition;
- Sensor nodes failing to join into any coalitions will be denied from the WSNs.

Under the above rules, the selfish sensor nodes that do not forward others' data packets will hardly be admitted into coalitions because of their poor reputation. In such rules, sensor nodes are enforced to participate in a coalition and those that cannot join into any coalitions are under high suspicion of being malicious.

The coalitional game model can be integrated with various routing protocols; for example, AODV routing protocol presented in [PBRD03]. However, as noted in [SYCY11], there is a lack of simulation experiments for validating the performance of coalitional game integrated with the routing protocol, such as AODV and DSR [JOHM07].

2.2.4.4 Coexistence with Malicious Sensor Nodes

Malicious and regular sensor nodes can coexist as long as the destruction they bring is less than the contribution they make [SYCY11]. For example, the authors in [WACK09] study interactions between a malicious and a regular sensor node in WSN, defining two separated sets of sender's and receiver's strategies:

- The set of strategies of the sender is **{Attack, Forward}**. Attack means the sender is malicious, while Forward means the sender is regular or a malicious sensor node disguises itself;
- The set of strategies of the receiver is **{Monitor, Idle}**, which means the receiver monitors the sender or not, respectively.

The authors in [WACK09] additionally formalize the interaction between sensor nodes into

two games. The first game, called ***malicious sensor node detection game***, is a signaling game that is a special category of Bayesian game with imperfect information. The second game, called ***post-detection game***, is played when the regular sensor node knows confidently that its opponent is a malicious sensor node. Based on various combinations of the strategies used, the net utility is calculated. As noted in [SYCY11], the authors do not mention where their simulations are done and how the simulation environment has been configured. This is what motivates our research in *IoT4Industry*.

3. Industrial Requirements w.r.t. IoT Security, Privacy and IPR/ Data Protection

The Industrial Internet (of Things) brings new opportunities, along with new risks, to business and society in general. Many questions about the Industrial Internet still remain open; for example, how it will impact business models, policies, interaction, protection. To answer these questions and their impacts facing business and government leaders, the World Economic Forum's IT Governors launched ***the Industrial Internet initiative*** at the Annual Meeting 2014 in Davos, Switzerland. This initiative conducted a series of research activities, including in-person workshops, virtual working group sessions, interviews of key thought leaders, and a survey of innovators and early adopters. The summary on this initiative is presented in the form of a study published in [WEF15], in which security and data privacy (data breaches, attacks, espionage) has been recognized as one of the most important hurdles to solve in order to realize the full potential of the Industrial Internet. The authors in [WEF15] conclude that cybersecurity for the IoT requires "*new security frameworks that span the entire cyber physical stack, from device-level authentication and application security, to system-wide assurance, resiliency and incidence response models.*" Figure 2 summarizes the greatest barriers that largely inhibit industries from adopting the Industrial Internet in EU, North America, and the rest of the world. Security and privacy concerns are ranked amongst major inhibitors. Therefore, ***the Industrial Internet Reference Architecture (IIRA)***, as presented in its first published version in [IIRA15] "*...initiates a process to create broad industry consensus to drive product interoperability and simplify development of Industrial Internet systems that are better built and integrated with shorter time to market, and at the end better fulfill their intended uses.*" With a special focus on major architecture question in Industrial Internet, IIRA gives privacy and security a

strong emphasis. For example, it integrates the business viewpoint (the RoI for security), the usage viewpoint (transparent security to the user), the functional viewpoint (security for the system as a whole) and the implementation viewpoint (common architecture patterns and system components).

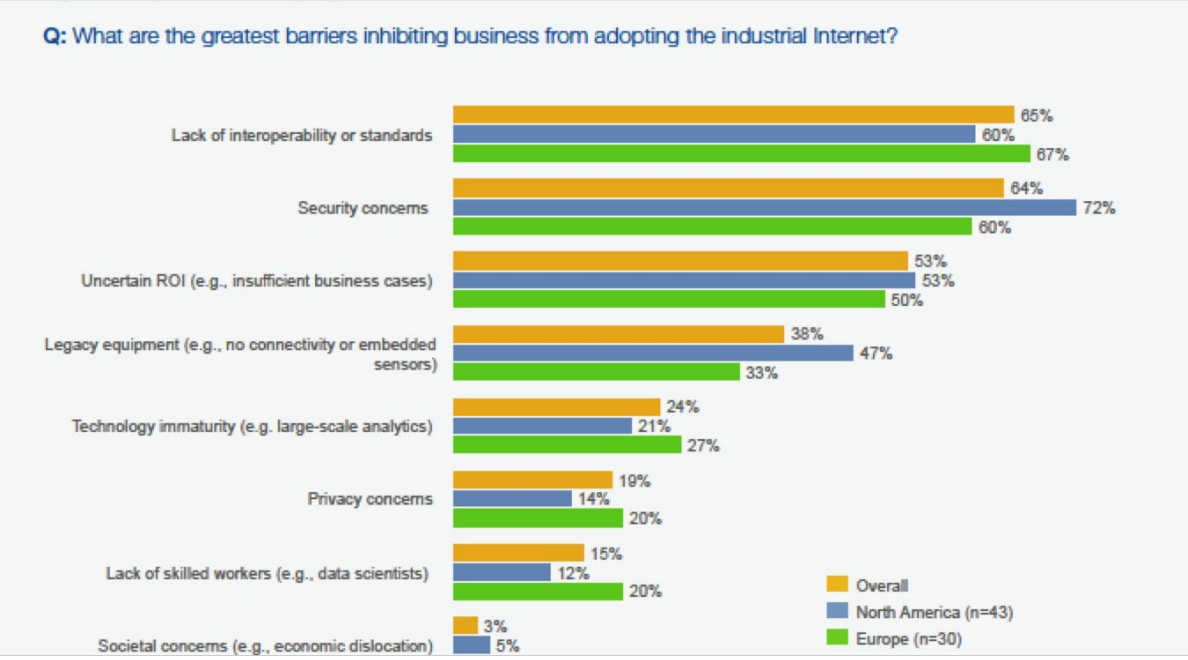

Figure 2. The greatest barriers that largely inhibit business from adopting the Industrial Internet (source [WEF15])

Furthermore, common security activities are described below [IIRA15]:

- ***Security monitoring*** gathers and analyzes security-related data continuously as activities are performed. It may take different forms depending on the context of operations and on security events. For example, different tasks are appropriate before, during and after an attack.
- ***Security auditing*** collects, stores and analyzes security information.
- ***Security policy management*** manages both automated and human-driven administrative security tasks by documenting their usage and constraints.
- ***Cryptographic*** support management consists of globally interoperable key management, secure credential storage and revocation.

To secure an Industrial Internet System, the authors in [IIRA15] outline a number of important and common security issues to be addressed in its implementation:

- ***End-to-end security***: the implementation of an IIS must provide: protected device-to-device communications, confidentiality and privacy of the data collected, remote security management and monitoring, simultaneously addressing both existing technologies as well as new technologies, and seamlessly spanning both information technology (IT) and operational technology (OT) subsystems and processes without interfering with operational business processes.
- ***Securing legacy systems***: the use of security gateways is an approach to secure legacy endpoints and their protocols. A security gateway acting as proxies for the legacy endpoints bridges the legacy protocols supported by the legacy endpoints and their counterparts used by new endpoints. A security gateway isolates the attack surface introduced by the legacy endpoints and their protocols to the links from these endpoints.
- ***End-point security***: it provides embedding security capabilities and policy enforcement directly in end-point devices. The end-point should have the ability and autonomy to defend itself and must remain resilient even when disconnected from the external security management systems.
- ***Information exchange security***: Communication and data exchanges within an IIS must be protected for authenticity, confidentiality, integrity and non-repudiation.
- ***Management and monitoring security*** of both the endpoints and the communication mechanisms, involves the following areas: identity management, provisioning and commissioning, security policy management, situational awareness, remote update, credential management, etc.
- ***Data distribution and secure storage***, including data security, data centric policies, data analysis and privacy, etc.

Our analysis of industrial requirements for IoT security, privacy and IPR/data protection in *IoT4Industry*, is additionally based on the RAMI (Reference Architecture Model Industry 4.0), as well as the SCISSOR project (Horizon 2020 N644425, February 2015 - January 2018) and its project report "*Technological assessments, scenarios and requirements*". Salzburg Research is the project partner in SCISSOR. In Task 2.1, the project examines the real-world expertise of the consortium partners related to the ICS (Industrial Control System) technologies, devices, and network infrastructure. It considers the requirements related to security services, including a wide range of possible deployment and solutions,

from industrial control processes, pipelines, power generation, nuclear plants, water distribution, ambient control, etc.

Industrial infrastructures are often built on top of complex and heterogeneous systems (in sense of heterogeneous protocols in use), with many features strictly connected to the specific activity sectors, and strategically deployed, to manage their complexity. For example, literature on Smart Grid refers on Advanced Distribution Automation (ADA), which goal is to provide the real-time adjustment of the distribution system to changing loads, generation, and failure conditions, usually without operator intervention. In order to achieve real-time performances, many control applications will play a central role covering the full automation of all the controllable equipment and functions in the distribution system [EPRI04] [SCISSOR15a].

In order to achieve the goals of ADA, new applications and technology are expected to be developed, such as Fault Detection Isolation and Restoration (FDIR), Topology Processor (TP), Distribution Power Flow (DPF), Integrated Voltage/Var Control (IVVC), Optimal Feeder Configuration (OFC), Distribution Contingency Analysis (DCA), Distribution State Estimation (DSE), Distribution Load Forecasting and Estimation (DLF/DLE), etc. Intelligent Electronic Devices (IED) are key enablers of these applications, by receiving and sending data from/to electronic multifunction meters, digital relays, controllers, etc. [EPRI04] In addition, it is expected that ADA will bring new sophisticated algorithms, providing more intelligence and coordination at the central SCADA/DMS systems, as well as distributed control capabilities of the grid.

The evolution of the smart grids is based on the Advanced Metering Infrastructures (AMI), which heavily depends on Automated Meter Reading (AMR) devices, which support the following functionality [SCISSOR15a]:

- Measure power usage in real-time;
- Monitor and inform the Distributed System Operator (DSO), the customer and third parties about power quality;
- Track and keep a record about customer usage parameters;
- Remotely connect and disconnect customers from the power grid;
- Send out alarms to the DSO in case of technical issues and failures;
- Energy prepayment;
- Remotely receive and install firmware upgrades to incorporate new functionality;
- Anti-tampering and fraud detection;

- Remotely customizable load limit feature.

Despite broad use of SCADA systems for running critical industrial processes (such as, railway signaling systems, food production, wind turbines, oil refineries, etc.), SCADA has not been designed for security, which consequently might lead to intellectual property theft, loss of visibility of the system sensor readings, data integrity, loss of control of the plants, etc. Hence, the authors in [SCISSOR15a] survey SCADA literature related to security:

- threats analysis (physical threats, human threats, network incident taxonomy [HOLO98] [BLAC09] [HAHU03], SCADA attacks taxonomy [ZHJS11]),
- protection methods and tools (e.g. network monitoring, IDS),
- security risks (e.g. ICT network, or DSS control center compromised; modification, deletion, or disclosure of customer private data; shutdown of the corporate LAN).

In addition, the authors in [SCISSOR15a] perform the security risk analysis, with the aim to define possible attacks in smart grids and ICS/SCADA systems, and to find ways to protect these systems within the existing constraints.

Finally, our analysis of the industrial requirements for security, privacy and IPR/data protection takes into consideration findings from the interviews and presentations given by the network of IoT experts, industrial leaders and IoT early adopters in Austria, that we met during *IoT Salzburg* meetups held in March 10, 2015 and May 19, 2015, in Salzburg.

4. Conclusion

This report presents our first results on IoT technology tracking, plus the investigation of the major industrial requirements for security, privacy and IPR/ data protection in the IoT. The activities carried during the project follow up (1) *IoT Salzburg* meetups, and our discussions with the experts from several production companies in Austria, which help us understand the expectations and security needs of the industrial practitioners. (2) We additionally consult the report "*Technological assessments, scenarios and requirements*" of the SCISSOR project (Horizon 2020 N644425, February 2015 - January 2018), particularly its Task 2.1 that examines the real-world expertise of the consortium partners related to the ICS (Industrial Control System) technologies, devices, and network infrastructure. SCISSOR considers the requirements related to security services. (3) Finally, we base our investigation on the relevant literature from the areas such as privacy, security, IPR and

data protection in the IoT. We explore the main privacy and data protection challenges in the IoT, security challenges (security vulnerabilities, detection and prevention of attacks in IoT, data provenance, game-theoretic algorithmic approach to IoT security), and finally, security concerns and requirements from the side of the industrial practitioners.

In parallel with the requirements gathering, we also tracked developments in the technical and scientific fields. Our summary on emerging IoT platforms, over the course of the project is summarized in the additional report: "*Report on emerging IoT platforms for Industrial Internet*".

Appendix 1: Interview with Industrial Experts in Austria

This is a template prepared to support the Interview with Industrial Experts in Austria, to identify major expectations about Industry 4.0 and their security needs related to the IoT. It has been created to serve as a basis for the discussion with the industrial experts in Austria, during *IoT Salzburg* meetups.

(*IoT4Industry* project; full name of the project: Secure, Privacy-Preserving Agents for the Industrial Internet, project website: http://iot4industry.salzburgresearch.at/)

Interviewee: _____

Date: _____

1. Which of the following barriers are the main inhibitors of adoption of the Industrial Internet in your company? Please rank from 5 (least relevant) to 1 (most relevant).

☐ Security concerns

☐ Privacy concerns

☐ Technology immaturity

☐ Interoperability, or lack of standards

☐ _____ (e.g. lack of skilled workers, lack of education in the area, lack of business models (or how do company profit from the IoT))

2. What is likely to be the primary M2M protocol used in your company for the IoT in 5 years?

_____

_____

3. What are your major privacy concerns?

☐ Loss of control over data

☐ Inferences derived from the data

☐ Repurposing of original data processing

☐ Bringing out behavior patterns and user profiling

☐ Remaining anonymous when using IoT based services

☐ Quality of the user's consent (lack of information about the use of the data)

☐ _____

☐ _____

4. What are your major security concerns?

☐ Security weaknesses of any hardware and IoT devices

☐ Security vulnerabilities (e.g. insecure Web interface, insecure network services)

☐ Security attacks

☐ Insufficient authentication/authorization

☐ Lack of transport encryption

☐ Insecure mobile interface

☐ Insecure cloud interface

☐ Poor physical security

☐ Insecure software / firmware

☐ _____

☐ _____

5. Have you experienced any of the following security attacks (please, ignore this question if you find it being sensitive information)

☐ Selective forwarding

☐ Sinkhole attacks

☐ Sybil attacks

☐ Wormholes

☐ HELLO flood attacks

☐ Acknowledgement spoofing

References

[ABLF04] M. Atallah, M. Bykova, J. Li, K. Frikken, and M. Topkara, 2004. "Private collaborative forecasting and benchmarking," in ACM workshop on Privacy in the electronic society, Washington DC, USA, 2004.

[AFKM05] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu, 2005. Approximation algorithms for k-anonymity. In Journal of Privacy Technology (JOPT).

[AGBD04] A. Agah, S.K. Das, K. Basu, 2004. A game theory based approach for security in wireless sensor networks. In Proceedings of 2004 23rd IEEE International Performance, Computing, and Communications Conference, Phoenix, AZ, USA, 15–17 April 2004.

[AGBD05a] A. Agah, K. Basu, S.K. Das, 2005. Enforcing security for prevention of DoS attack in wireless sensor networks using economic modeling. In Proceedings of 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems, Washington, DC, USA, 2005.

[AGBD05b] A. Agah, K. Basu, S.K. Das, 2005. Preventing DoS attack in sensor networks: A game theoretic approach. In Proceedings of 2005 IEEE International Conference on Communications, Seoul, South Korea, 16–20 May 2005.

[AGBD06] A. Agah, K. Basu, and S. K. Das, “Security enforcement in Wireless Sensor Networks: A framework based on noncooperative games,” Pervasive and Mobile Computing, vol. 2, Apr. 2006, pp. 137-158.

[AGDA07] A. Agah, S.K. Das, 2007. Preventing DoS attacks in wireless sensor networks: A repeated game theory approach. Int. J. Network Security 2007, 5, 145–153.

[AGDB04] A. Agah, S.K. Das, K. Basu, 2004. “A non-cooperative game approach for intrusion detection in sensor networks.” In Proceedings of 2004 IEEE 60th Vehicular Technology Conference. VTC2004-Fall, Los Angeles, CA, USA, 26–29.

[ALBA04] T. Alpacan & T. Basar, 2004. “A game theoretic approach to decision and analysis in network intrusion detection," in Proceedings of 43rd IEEE Conference on Decision and Control, (Piscataway, NJ, USA), IEEE Press.

[BAAG05] R.J. Bayardo Jr. and R. Agrawal, 2005. Data privacy through optimal k-anonymization. In ICDE, pages 217–228.

[BADI06] R. S. Barga and L. A. Digiampietri. Automatic generation of workflow provenance. In Proceedings of the International Provenance and Annotation Workshop (IPAW), pp 1–9, 2006.

[BBCG01] L. Blazevic, L. Buttyaan, S. Capkun, S. Giordano, J.P. Hubaux, J. LeBoudec, 2001. “Self-organization in mobile ad hoc networks: the approach of terminodes,” IEEE Commun.Mag., vol. 39, no. 6, 2001, pp:161-174.

[BENA94] J. Benaloh, 1994. "Dense Probabilistic Encryption," in Proceedings of the

Workshop on Selected Areas of Cryptography Kingston, ON, 1994, pp. 120-128.

[BERG85] J. O. Berger. Statistical decision theory and Bayesian analysis. Springer, 1985.

[BHLX04] B. Bhargava, L. Lilien and D. Xu, 2004. “Private and Trusted Interactions,” slides, 5th Annual Info. Security Symp. "Energizing the Enterprise: Cyber Security in Context," CERIAS, Purdue University. http://www.cs.purdue.edu/homes/llilien/priv_trust_int.pdf

[BHRB01] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi, 2001. “Secure pebblenets,” In ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), pp. 156–163.

[BITR01] J. Binkley and W. Trost, “Authenticated ad hoc routing at the link layer for mobile systems,” Wireless Networks, vol. 7, no. 2, pp. 139–145.

[BLAC09] C. Blackwell, 2009. A security architecture to protect against the insider threat from damage, fraud and theft. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, page 45. ACM.

[BOYD05] E. Bertino, B.C. Ooi, Y. Yang, and R.H. Deng, 2005. Privacy and ownership preserving of outsourced medical data. In ICDE, pages 521– 532.

[BRNI10] H. Brenner and K. Nissim. Impossibility of differentially private universally optimal mechanisms. In Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on, pages 71-80. IEEE, 2010.

[BRNI11] F. Brunton and H. Nissenbaum. Vernacular resistance to data collection and analysis: A political theory of obfuscation. First Monday, 16(5), 2011. Online: http://firstmonday.org/article/view/3493/2955

[BROE10] G. Broenink et al., 2010. “The Privacy Coach: Supporting Customer Privacy in the Internet of Things,” Proc. Workshop on What Can the Internet of Things Do for the Citizen?. Online: http://dare.ubn.ru.nl/bitstream/2066/83839/1/83839.pdf.

[BRSH08] J. Brickell and V. Shmatikov. The cost of privacy: Destruction of data-mining utility in anonymized data publishing. In Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '08, pages 70{78, New York, NY, USA, 2008. ACM.

[BUBO02] S. Buchegger & J. L. Boudec, 2002. “Nodes bearing grudges: toward routing security, fairness and robustness in mobile ad hoc networks,” Proceedings of the 10th Euronicro Workshop on parallel, Distributed and Network-based Processing, Spain..

[BUBO02] S. Buchegger and J.-Y. L. Boudec, 2002. “Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks,” in Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing. Canary Islands, Spain: IEEE Computer Society, pp. 403–410.

[BUHS05] Buttyán, L., Holczer, T., Schaffer, P., 2005. Spontaneous cooperation in multi-domain sensor networks. In Proceedings of 2005 2nd European

Workshop on Security and Privacy in Ad-Hoc and Sensor Networks, Visegrad, Hungary, 13–14 July 2005.

[BUHU01] L. Buttyaan, J. P. Hubaux, 2001. “Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks, ” TR DSC/2001/001, Department of Communication Systems, Swiss Federal Institute of Technology.

[BUKT00] P. Buneman, S. Khanna, and W. C. Tan. Data provenance: Some basic issues. In FST TCS 2000: Proceedings of the 20th Conference on Foundations of Software Technology and Theoretical Computer Science, pages 87–93, London, UK, 2000. Springer-Verlag.

[BUKT01] P. Buneman, S. Khanna, and W. C. Tan. Why and where: A characterization of data provenance. Lecture Notes in Computer Science, 1973:316–330, 2001.

[CBBG12] Compton, M., Barnaghi, P., Bermudez, L., Garcia-Castro, R., Corcho, O., Cox, S., Graybeal, J., Hauswirth, M., Henson, C., Herzog, A., Huang, V., Janowiczj, K., Kelsey, W., Phuoc, D.L., Lefort, L., Leggieri, M., Neuhaus, H., Nikolov, A., Page, K., Passant, A., Sheth, A., Taylor, K.: The SSN ontology of the W3C semantic sensor network incubator group. Journal of Web Semantics: Science, Services and Agents on the World Wide Web 17 (2012)

[CEBM13] Corsar, D., Edwards, P., Baillie, C., Markovic, M., Papangelis, K., Nelson, J.: Short paper: Citizen sensing within a real time passenger information system. In Proceedings of the 6th International Workshop on Semantic Sensor Networks. vol. 1063, pp. 77-82. CEUR Workshop Proceedings (2013)

[CEBM13] Corsar, D., Edwards, P., Baillie, C., Markovic, M., Papangelis, K., Nelson, J.: Short paper: Citizen sensing within a real time passenger information system. In Proceedings of the 6th International Workshop on Semantic Sensor Networks. vol. 1063, pp. 77{82. CEUR Workshop Proceedings (2013)

[CHCH11] D. Chen, G. Chang et al, 2011. “TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things”, Computer Science and Information Systems, Volume 8, Issue 4,pp.1207-1228.

[CHDU09] Chen, J.; Du, R. Fault tolerance and security in forwarding packets using game theory. In Proceedings of the 2009 International Conference on Multimedia Information Networking and Security (MINES 2009), Hubei, China, 2009.

[CHPA08] K. Chatzikokolakis, C. Palamidessi, and P. Panangaden. Anonymity protocols as noisy channels. Information and Computation, 206(2-4):378{401, 2008.

[CHSV10] Chong, S., Skalka, C., Vaughan, J.: Self-identifying sensor data. In Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks. pp. 82-93. IPSN '10, ACM, New York, NY, USA (2010)

[CKVL02] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, 2002. "Tools for privacy preserving distributed data mining," SIGKDD Explore. Newsletter. Vol. 4, pp. 28-34.

[COCT14] M. Compton, D. Corsar, K. Taylor, 2014. Sensor Data Provenance: SSNO and

PROV-O Together at Least. In Proceedings of the 7th International Workshop on Semantic Sensor Networks (October 2014). Online: http://knoesis.org/ssn2014/paper_9.pdf

[COTH00] C. Collberg and C. Thomborson, “Watermarking, tamper-proofing, and obfuscation—tools for software protection,” Tech. Rep. 2000-03, Department of Computer Science, University of Arizona, 2000.

[CRAN03] L. Cranor, “P3P: Making privacy policies more useful,” IEEE Security and Privacy, Nov./Dec. 2003, pp. 50–55.

[DLLX09] R. Dong, L. Liu, J. Liu, X. Xu, 2009. Intrusion detection system based on payoff matrix for wireless sensor networks. In Proceedings of 2009 3rd International Conference on Genetic and Evolutionary Computing (WGEC 2009), Guilin, China, 14–16 October 2009.

[DSCP03] C. Diaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In Privacy Enhancing Technologies, pages 54-68. Springer Berlin Heidelberg, 2003.

[DUAT01] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: a review and open problems," in Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico, 2001.

[EPRI04] EPRI. Technical and system requirements for advanced distribution automation, 2004.

[FEHB06] Fèlegyhazi, M., Hubaux, J., Buttyán, L., 2006. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. IEEE Trans. Mobile Comput. 2006, 5, 463–476.

[FRAL06] K. Frikken, M. Atallah, and J. Li, 2006. "Attribute-Based Access Control with Hidden Policies and Hidden Credentials," IEEE Trans. Comput., vol. 55, pp. 1259-1270.

[FRAZ05] K. Frikken, M. Atallah, and C. Zhang, 2005. "Privacy-preserving credit checking," in Proceedings of the 6th ACM conference on Electronic commerce, Vancouver, BC, Canada, 2005.

[FRBO01] J. Frew and R. Bose. Earth system science workbench: A data management infrastructure for earth science products. In SSDBM ’01: Proceedings of the Thirteenth International Conference on Scientific and Statistical Database Management, pp. 180, Washington, DC, USA, 2001. IEEE Computer Society.

[FTC15] The Federal Trade Commission Report on IoT: “FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks”. Online: http://prn.to/1A0eT3s

[FVWZ02] I. T. Foster, J. Vockler, M. Wilde, and Y. Zhao. Chimera: A virtual data system for representing, querying, and automating data derivation. In SSDBM ’02: Proceedings of the 14th International Conference on Scientific and Statistical Database Management, pages 37–46, Washington, DC, USA, 2002. IEEE Computer Society.

[GHRS09] A. Ghosh, T. Roughgarden, and M. Sundararajan. Universally utility-maximizing

privacy mechanisms. In Proceedings of the 41st annual ACM symposium on Theory of computing, pages 351-360. ACM, 2009.

[GHRS12] A. Ghosh, T. Roughgarden, and M. Sundararajan. Universally utility-maximizing privacy mechanisms. SIAM Journal on Computing, 41(6):1673-1693, 2012

[GOLB06] J. Golbeck. Combining provenance with trust in social networks for semantic web content filtering. In Proceedings of the International Provenance and Annotation Workshop (IPAW), pages 101–108, 2006.

[GOLD97] S. Goldwasser, 1997. "Multi party computations: Past and Present," in Proceedings of the sixteenth Annual ACM Symposium on Principles of Distributed Computing, Santa Barbara, California, United States.

[GÜTD11] Gürses, S., Troncoso, C., and Diaz, C. 2011. Engineering privacy by design. Paper presented at CPDP 2011, Belgium, 2011.

[HAHU03] S. Hansman & R. Hunt, 2003. A taxonomy of network and computer attack methodologies. Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand.

[HASA05] R. Hasan, Z. Anwar, W. Yurcik, L. Brumbaugh, and R. Campbell. A survey of peer-to-peer storage techniques for distributed file systems. In ITCC ’05: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’05) - Volume II, pages 205–213, Washington, DC, USA, 2005. IEEE Computer

[HASW07] R. Hasan, R. Sion, M. Winslett, 2007. Introducing Secure Provenance: Problems and Challenges. In Proceedings of the StorageSS’07, October 29.

[HESN13] Hensley, Z., Sanyal, J., New, J.: Provenance in sensor data management. Queue 11(12), 50:50-50:63 (2013)

[HEWB06] H. Hexmoor, S. Wilso, Sandeep Bhattaram, 2006. “A theoretical inter-organizational trust-based security model”, The Knowledge Engineering Review, pp.127-161.

[HFLY03] Y. Huang, W. Fan, W. Lee, and P. S. Yu, 2003. “Cross-feature analysis for detecting ad-hoc routing anomalies," in Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS 2003:), pp. 478-487.

[HGZZ14] W. Han, Y. Gu, Y. Zhang, L. Zheng, 2014. Data Driven Quantitative Trust Model for the Internet of Agricultural Things. In Proceedings of teh 4th International Conference on IoT, MIT, USA.

[HOLO98] J.D. Howard & T. A. Longsta, 1998. A common language for computer security incidents. Sandia National Laboratories.

[HUBC01] J. Hubaux, L. Buttyan, and S. Capkun, 2001. “The quest for security in mobile ad hoc networks,” in Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001).

[HUJP02] Y.-C. Hu, D. B. Johnson, and A. Perrig, 2002. “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), pp. 3–13.

[HUPJ01] Y.-C. Hu, A. Perrig, and D. B. Johnson, 2001. “Ariadne: A secure on-demand

routing protocol for ad hoc networks," Department of CS, Rice University, TR01-383.

[HUPJ02] Y.C. Hu, A. Perrig, and D. B. Johnson, 2002. "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384.

[HUSH03] F. Hu & N. K. Sharma, 2003. "Security considerations in ad hoc sensor networks," Ad Hoc Networks, 2003.

[IIRA15] Industrial Internet Reference Architecture. Version 1.7, Industrial Internet Consortium. 04.06.2014. Online available: www.iiconsortium.org/IIRA-1-7-ajs.pdf

[IMWB14] S. Ioannidis, A. Montanari, U. Weinsberg, S. Bhagat, N. Fawaz, and N. Taft. Privacy tradeoffs in predictive analytics. arXiv preprint arXiv:1403.8084, 2014.

[IYEN02] V.S. Iyengar, 2002. Transforming data to satisfy privacy constraints. In Proc. of ACM SIGKDD'02, pages 279–288.

[JACO10] Janowicz, K., Compton, M.: The Stimulus-Sensor-Observation Ontology Design Pattern and its Integration into the Semantic Sensor Network Ontology. In: 3rd International workshop on Semantic Sensor Networks. Vol. 668. CEUR-WS (2010)

[JCST14] S. Jha, K. Chatterjee, S.A. Seshia, S. Tripakis, 2014. "Game-Theoretic Secure Localization in Wireless Sensor Networks". In *Proceedings of the 4th International Conference on the Internet of Things (IoT)*.

[JOHM07] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC 4728, Feb. 2007.

[KAGU02] O. Kachirski and R. K. Guha, 2002. "Intrusion detection using mobile agents in wireless ad hoc networks," in Proceedings of the IEEE Workshop on Knowledge Media Networking, (Piscataway, NJ, USA), pp. 153{158, IEEE Press.

[KAIY04] Kannan, R., Iyengar, S.S., 2004. Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks. IEEE J. Sel. Areas Commun. 2004, 22, 1141–1150.

[KASI04] Kannan, R., Sarangi, S., Iyengar, S.S., 2004. Sensor-centric energy-constrained reliable query routing for wireless sensor networks. Journal on Parallel Distributed Computing. 2004, 64, 839–852.

[KAWA02] Chris Karlof & David Wagner, 2002. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, Volume 1, Issue 2, Pages 293-315.

[KOLA03] M. Kodialam & T. V. Lakshman, "Detecting network intrusions via sampling : A game theoretic approach," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOMM 2003, (Piscataway, NJ, USA), pp. 1880{1889, IEEE Press, April 2003.

[KOOL05] G. M. Køien and V. A. Oleshchuk, 2005. "Location Privacy for Cellular Systems;

Analysis and Solution," in 5th Workshop on Privacy Enhancing Technologies (PET'05), 2005, pp. 40-58.

[KRTO02] C. Kruegel & T. Toth, 2002. "Flexible, mobile agent based intrusion detection for dynamic networks," in Proceedings of the European Wireless (EW2002).

[KUFK11] Kung, A., Freytag, J., and Kargl, F., 2011. Privacy-by-design in ITS applications. Proc. IEEE WoWMoM (2011), 1-6.

[KZLZ01] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in ICNP, pp. 251–260.

[LFMR10] Liu, Y., Futrelle, J., Myers, J., Rodriguez, A., Kooper, R.: A provenance-aware virtual sensor system using the open provenance model. In Collaborative Technologies and Systems (CTS); pp. 330-339 (2010)

[LHRM10] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor. Optimizing linear counting queries under differential privacy. In Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, pages 123-134. ACM, 2010.

[LHTB12] Lefort, L., Henson, C., Taylor, K., Barnaghi, P., Compton, M., Corcho, O., Castro, R.G., Graybeal, J., Herzog, A., Janowicz, K., Neuhaus, H., Nikolov, A., Page, K.: Semantic Sensor Network XG Final Report. W3C Incubator Report (2011), Available: http://www.w3.org/2005/Incubator/ssn/XGR-ssn-20110628/

[LIBH05] L. Lilien & B. Bhargava, 2005. A Scheme for Privacy-Preserving Data Dissemination. IEEE Transactions on Systems, Man and Cybernetics. Part A; Systems and Humans, 36(3).

[LILQ11] H. Li, L. Lai, R.C. Qiu, 2011. A denial-of-service jamming game for remote state monitoring in smart grid. In Proceedings of 2011 45th Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 23–25 March 2011.

[LILY08] X. Li and M. R. Lyu, "A novel coalitional game model for security issues in wireless networks," Proc. IEEE Global Telecommunications Conference (GLOBECOM 2008), 2008, pp. 1-6.

[LIZY11] X. Li, F. Zhou, X. Yang, 2011. "A multi-dimensional trust evaluation model for large-scale P2P computing", Journal of Parallel and Distributed Computing, pp.837-847.

[LKMS04] J. Li, M. Krohn, D. Mazières, and D. Shasha. Secure untrusted data repository (sundr). In OSDI'04: Proceedings of the 6th conference on Symposium on Opearting Systems Design & Implementation, pages 9–9, Berkeley, CA, USA, 2004. USENIX Association.

[LNHM05] Ledlie, J., Ng, C., Holland, D., Muniswamy-Reddy, K., Braun, U., Seltze, M.: Provenance-aware sensor data storage. In Proceedings of the 1st IEEE International Workshop on Networking Meets Databases (NetDB) (2005)

[LSGB14] Lebo, T., Sahoo, S., McGuinness, D., Belhajjame, K., Cheney, J., Corsar, D., Garijo, D., Soiland-Reyes, S., Zednik, S., Zhao, J.: PROV-O: The PROV ontology. W3C Recommendation (2013), available at

http://www.w3.org/TR/prov-o/ (last accessed April 2014)

[MATE08] R. Machado, S. Tekinay, 2008. A survey of game-theoretic approaches in wireless sensor networks. Comput. Network 2008, 52, 3047–3061.

[MCFF11] Moreau, L., Cliord, B., Freire, J., Futrelle, J., Gil, Y., Groth, P., Kwasnikowska, N., Miles, S., Missier, P., Myers, J., Plale, B., Simmhan, Y., Stephan, E., Van den Bussche, J.: The open provenance model core specification (v1.1). Future Generation Computer Systems 27(6), 743-756 (2011)

[MCKY03] D. J. MacKay. Information theory, inference and learning algorithms. Cambridge university press, 2003.

[MGLB00] S. Marti, T. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM) 2000.

[MGLB00] S. Marti, T. J. Giuli, K. Lai, and M. Baker, 2000. “Mitigating routing misbehavior in mobile ad hoc networks,” in Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255–265.

[MIMO02] P. Michiardi & R. Molva, 2002. “Core: A collaborative reputation mechanism to enforce node co-operation in mobile ad hoc networks," in Proceedings of the 6th IFIP Communications and Multimedia Security Conference.

[MIMO02a] P. Michiardi, R. Molva, 2002. “Core: A Collaborative Reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Communications and Multimedia Security Conference.

[MIMO02b] P. Michiardi, R. Molva, 2002. “Prevention of denial of service attack and selfishness in mobile ad hoc networks,” Research Report RR-02-063, Institute Eurecom, France, 2002.

[MIMO02c] P. Michiardi and R.Molva, “Simulation-based analysis of security exposures in mobile ad hoc networks,” in European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services and Applications, Florance, Italy, February 2002.

[MINP04] A. Mishra, K. Nadkarni, and A. Patcha, 2004. “Intrusion detection in wireless ad hoc networks," in IEEE Wireless Communications, vol. 11, (Piscataway, NJ, USA), pp. 48-60, IEEE Press.

[MOMZ09] Mohi, M., Movaghar, A., Zadeh, P. A “Bayesian game approach for preventing DoS attacks in wireless sensor networks.” In Proceedings of 2009 WRI International Conference on Communications and Mobile Computing, Kunming, China, 2009.

[MURE06] K.-K. Muniswamy-Reddy, D. A. Holland, U. Braun, and M. I. Seltzer. Provenance-aware storage systems. In USENIX Annual Technical Conference, General Track, pp. 43–56, 2006.

[MYER04] J. D. Myers, et al., 2004. A collaborative informatics infrastructure for multi-scale science.

[MZAB12] M. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux. Game theory meets network security and privacy. ACM Computing Surveys, 45(3), 2012.

[NACC98] D. A. S. J. Naccache, 1998. "A New Cryptosystem Based on Higher Residues,"

in Proceedings of the 5th ACM Conf. on Computer and Communication Security, 1998, pp. 59-66.

[OWEN01] Owen, G., 2001. Game Theory; Academic Press: New York, NY, USA.

[PAHA02] P. Papadimitratos and Z. Haas, 2002. “Secure routing for mobile ad hoc networks,” in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002).

[PAHE08] Park, U., Heidemann, J.: Provenance in sensornet republishing. In Freire, J., Koop, D., Moreau, L. (eds.) Provenance and Annotation of Data and Processes, Lecture Notes in Computer Science, vol. 5272, pp. 280{292. Springer Berlin Heidelberg (2008)

[PAIL99] P. Paillier, 1999. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in EUROCRYPT'99, 1999, pp. 223-238.

[PAPA06] A. Patcha & J.M. Park, 2006. A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks. International Journal of Network Security, Vol.2, No.2, PP.131–137, Mar. 2006

[PAPG05] Parno, B., Perrig, A., Gligor, V., 2005. "Distributed detection of node replication attacks in sensor networks," *Security and Privacy, 2005 IEEE Symposium on* , vol., no., pp.49,63, 8-11.

[PBRD03] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, July 2003.

[PPCJ03] R.S. Puttini, J.-M. Percher, O. Camp, R. T. S. Junior, C.J.B. Abbas, and L.J. Garca-Villalba, 2003. “A modular architecture for distributed ids in manet," in Proceedings of the 2003 International Conference on Computational Science and Its Applications (ICCSA). (V. Kumar, M. L. Gavrilova, C. J. K. Tan, and P. L'Ecuyer, eds.), vol. 2669 of Lecture Notes in Computer Science, pp. 91-113, Springer.

[PSHS10] Patni, H., Sahoo, S., Henson, C., Sheth, A.: Provenance aware linked sensor data. In Proceedings of the 2nd Workshop on Trust and Privacy on the Social and Semantic Web. Vol. 5 (2010)

[PSWC01] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, “SPINS: Security protocols for sensor networks,” in Proceedings of Mobile Networking and Computing 2001, 2001.

[QICX10] Qiu, Y.; Chen, Z.; Xu, L. “Active Defense Model of Wireless Sensor Networks Based on Evolutionary Game Theory.” In Proceedings of 2010 6th International Conference on Wireless Communications, Networking and Mobile Computing, Chengdu, China, 2010.

[RAMI15] Referenzarchitecturemodell Industrie 4.0 (RAMI4.0), APril 2015.

[REBE03] A. Rezgui, A. Bouguettaya and M. Eltoweissy, “Privacy on the Web: Facts, challenges, and solutions,” IEEE Security and Privacy, Nov./Dec. 2003, pp. 40–49.

[REDD09] Reddy, Y.B. “A Game theory approach to detect malicious nodes in wireless sensor networks.” In Proceedings of 2009 3rd International Conference on Sensor Technologies and Applications, Athens, Greece, 18–23 June 2009.

[RERG10] E. Rekleitis, P. Rizomiliotis, & S. Gritzalis, 2010.“A Holistic Approach to RFID Security and Privacy,” Proc. 1st Int’l Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory. Online: www.nics.uma.es/seciot10/files/pdf/rekleitis_seciot10_paper.pdf.

[RESR09] Reddy, Y.; Srivathsan, S. Game theory model for selective forward attacks in wireless sensor networks. In Proceedings of 2009 17th Mediterranean Conference on Control and Automation (MED), Thessaloniki, Greece, 24–26 June 2009.

[RONL11] R. Roman, P. Najera, J. Lopez, 2011. “Securing the Internet of Things”. In IEEE Computer, Vol. 44, No. 9, pp. 51-58, September 2011.

[RUBI12] Rubinstein, I. Regulating Privacy by Design. Berkeley Technology Law Journal, (2012).

[SACA05] C. Sar and P. Cao. Lineage file system. Online: http://crypto.stanford.edu/ cao/lineage.html, January 2005

[SAEP09] Y.E. Sagduyu, A. Ephremides, 2009. A game-theoretic analysis of denial of service attacks in wireless random access. Wirel. Netw. 2009, 15, 651–666.

[SAGI09] A. Sarma & J. Girão, 2009. “Identities in the Future Internet of Things,” Wireless Personal Comm., pp. 353-363.

[SBGS09] Sahoo, S., Barga, R., Goldstein, J., Sheth, A., Thirunarayan, K.: Where did you come from...where did you go? An algebra and RDF query engine for provenance. Tech. rep., Kno.e.sis Center, Wright State University (2009)

[SCISSOR15a] Technological assessments, scenarios and requirements. Horizon 2020 N644425. April 2015.

[SEDA03] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In Privacy Enhancing Technologies, pages 41-53. Springer Berlin Heidelberg, 2003.

[SEN11] J. Sen, 2011. “Privacy Preservation Technologies in Internet of Things,” Proc. Int’l Conf. Emerging Trends in Mathematics, Technology, and Management, 2011; http://arxiv.org/ftp/arxiv/papers/1012/1012.2177.pdf.

[SHBA05] J. Shi, G. Bochmann, C. Adams, A Trust Model with Statistical Foundation, Formal Aspects in Security and Trust, IFIP International Federation for Information Processing, vol 173, pp.145-158.

[SHOK15] R. Shokri, 2015. Privacy Games: Optimal User-Centric Data Obfuscation. In Proceedings on Privacy Enhancing Technologies 2015 (2), 1-17.

[SIPG05] Y. L. Simmhan, B. Plale, and D. Gannon, 2005. A survey of data provenance in e-science. SIGMOD Rec., 34(3):31–36, September 2005.

[SPCR09] Spiekermann, S. and Cranor, L. F., 2009. Engineering Privacy. IEEE Trans Software Engineering 35, 1 (2009) 67-82.

[SRUM13] V.B. Srinivas and S. Umar, 2013. “Spoofing Attacks in Wireless Sensor Networks”. IJCSET 2013, Vol. 3, Issue 6, 201-210.

[SSAK11] Stasch, C., Sven Schad, S., Alejandro Llaves, L., Krzysztof Janowicz, K., Broring, A.: Aggregating linked sensor data. In Taylor, K., Ayyagari, A., De Roure, D. (eds.) Proceedings of the 4th International Workshop on Semantic

Sensor Networks. Vol. 839, pp. 55-68 (2011)

[SSGB12] Shebaro, B., Sultana, S., Gopavaram, S., Bertino, E.: Demonstrating a lightweight data provenance for sensor networks. In Yu, T., Danezis, G., Gligor, V.D. (eds.) Proceedings of the 2012 ACM Conference on Computer and Communications Security. pp. 1022-1024. ACM (2012)

[STAN99] F. Stajano and R. J. Anderson, 1999. "The resurrecting duckling: Security issues for ad-hoc wireless networks," in Seventh International Security Protocols Workshop, pp. 172–194

[STBH11] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux. Quantifying location privacy. In Proceedings of the IEEE Symposium on Security and Privacy, 2011.

[STHA12] F. Stutzman, W. Hartzog, 2012. Obscurity by Design: An Approac to Building Privacy into Social Media. In Proceedings of the CSCW'12, Seattle, USA.

[STTH12] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec. Protecting location privacy: optimal strategy against localization attacks. In Proceedings of the ACM conference on Computer and communication security, 2012.

[SUWP03] B. Sun, K. Wu, and U. Pooch, 2003. "Routing anomaly detection in mobile ad-hoc networks," in Proceedings of the 12th International Conference on Computer Communications and Networks (ICCCN03), (Piscataway, NJ, USA), pp. 2531, IEEE Press.

[SWEE02] Latanya Sweeney, 2002. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5):557–570, 2002.

[SWKC12] Hai-Yan Shi, Wan-Liang Wang, Ngai-Ming Kwok, Sheng-Yong Chen, 2012. "Game Theory for Wireless Sensor Networks: A Survey". Sensors (Basel) 2012; 12(7): 9055–9097. Published online 2012 July 2. doi: 10.3390/s120709055.

[SYCY11] S. Shen, G. Yue, Q. Cao, F. Yu, 2011. A survey of game theory in wireless sensor networks security. Journal of Networks, 2011, 6, 521–532.

[UMBR12] Umuhoza, D., Braun, R.: Trustworthiness assessment of knowledge on the semantic sensor web by provenance integration. In: Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA). pp. 387-392 (2012)

[URBG03] Urpi, A., Bonuccelli, M., Giordano, S., 2003. Modelling cooperation in mobile ad hoc networks: A formal description of selfishness. In Proceedings of WiOpt Workshop, Sophia-Antipolis, France, 3–5 March 2003.

[VIPL06] N. N. Vijayakumar and B. Plale. Towards low overhead provenance tracking in near real-time stream filtering. In Proceedings of the International Provenance and Annotation Workshop (IPAW), pages 46–54, 2006.

[WACK09] W. Wang, M. Chatterjee, and K. Kwiat, "Coexistence with malicious nodes: A game theoretic approach," Proc. International Conference on Game Theory for Networks (GameNets '09), 2009, pp. 277-286.

[WALI06] Wang, W., and Li, X., 2006 Low-cost routing in selfish and rational wireless ad hoc networks. IEEE Trans. Mobile Comput. 2006, 5, 596–607.

[WAWU10] K. Wang, M. Wu, 2010. Cooperative communications based on trust model for mobile ad hoc networks, Information Security, IET, Volume 4, Issue 2, pp.68-79.

[WEF15] World Economic Forum, 2015. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services.

[WIDO05] J. Widom, 2005. Trio: A system for integrated management of data, accuracy, and lineage. In Proceedings of the Second Biennial Conference on Innovative Data Systems Research (CIDR'05), January 2005.

[WP29-14] Data Protection Working Party: "Opinion 8/2014 on the Recent Developments on the Internet of Things", 16 September 2014. Online: http://bit.ly/11S3Kcq

[XHTP11] Xie, M.; Han, S.; Tian, B.; Parvin, S. Anomaly detection in wireless sensor networks: A survey. J. Netw. Comput. Appl. 2011, 34, 1302–1325.

[YAMC08] L. Yang, D. Mu, X. Cai, 2008. Preventing dropping packets attack in sensor networks: A game theory approach. Wuhan Univ. J. Nat. Sci. 2008, 13, 631–635.

[ZAPA01] M. G. Zapata, 2001. "Secure ad-hoc on-demand distance vector (SAODV) routing," IETF MANET Mailing List, Message-ID: 3BC17B40.BBF52E09@nokia.com, ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail.

[ZGSB04] J. Zhao, C. A. Goble, R. Stevens, and S. Bechhofer. Semantically linking and browsing provenance logs for e-science. In ICSNW, pages 158–176, 2004.

[ZHHA99] L. Zhou and Z. Haas, 1999. "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6.

[ZHJS11] B. Zhu, A. Joseph, and S. Sastry, 2011 A taxonomy of cyber attacks on scada systems. In Internet of things (iThings/CPSCom), 2011 International conference on and 4th international conference on cyber, physical and social computing, pages 380--388. IEEE.

[ZHLE00] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in Proceedings of the 6th annual international conference on Mobile computing and networking (MOBICOM 2000), (New York, NY, USA), pp. 275{283, ACM Press, 2000.