# Trust infrastructures for future energy networks

N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti

***Abstract*—Efficient use and distribution of energy in future energy infrastructures largely depend on distributed control, metering and accounting functionalities. Thus, essential parts of the infrastructure will be placed under possibly hostile end-user's control. Consequently, their dependency as well as security directly relies on the trust established among all involved stakeholders and the proper functioning of devices. This short paper discusses some of the open issues and introduces the vision of a security infrastructure for energy networks built on hardware security anchors.**

***Index Terms*—Future energy networks, dependability, cyber security**

## I. Introduction

FUTURE energy infrastructures are characterized by the distribution of control, metering and accounting functionalities to the possibly hostile end-user's control. Their QoS depends directly on the trust established among all involved stakeholders and the proper functioning of devices. Current designs for Smart Grids and converging ICT and energy networks disregard the additional security and dependability issues arising from these advanced approaches. In the following sections this paper first reviews trends in energy networks and their rather obvious need for dependability and security, then several more concrete issues are discussed in more detail and finally the vision of a trust infrastructure using hardware trust anchors is introduced.

## II. Trends in Future Energy Distribution

A system is called distributed if its components are relatively autonomous entities which work together to achieve some overall objective and if its components are at different sites with no or limited coordination [26]. Distributed and embedded systems integrate in many areas tasks whose functionality is regarded as critical by both operators and end users. Distributed energy generation and intelligent energy distribution mechanisms are examples for such critical systems as they depend on a large number of small and independent devices connected in a Smart Grid (see Figure 1[1]). In this context many things are affecting the way energy is managed. For example so called "Micro cogeneration" [18] (microCHP) as part of distributed energy resource (DER) concepts requires IT infrastructures systems supporting the supervisory control and data acquisition (SCADA). Also the introduction of renewable energy resources [8], such as wind power, requires a robust control to manage the energy they produce. Other concepts include hybrid vehicles to provide for temporal resources in case of peaks in the load or storage capability in case of energy production surplus. In contrast to existing approaches these microCHP devices, vehicles or other consumers are not within the physical control of the operators as they are located, e.g., in the households of the end customers. This independence of action has consequences both from the control standpoint and security standpoint. From the control perspective the new infrastructure is characterized by a multi-layer decision architecture. From the security standpoint, while classical metering technology was protected by physical means, this is no longer possible for intelligent devices with different communication interfaces. Furthermore, attacks on these devices can create large financial losses or, when executed in a large scale, can even bring down complete energy networks. Therefore, new approaches for security management are required.

Facing the challenges that arise from the global change of climate, advances in control and metering systems for energy consumption are a promising step. So-called smart, or advanced, meters, can provide instant, automated information on electricity consumption to both users and transmission and distribution companies. These advanced meters are being rapidly installed in many jurisdictions throughout North America and Europe. In a pilot project undertaken by Ontario utility Hydro One, participating homeowners with such real-time displays decreased their electricity use by nearly 10 per cent.[2] The European Union committed itself to the EU Triple-20 targets by 2020 stating that energy consumption and greenhouse gas emissions are to be reduced by 20 % and energy from renewable sources increased by 20 %. National aims, e.g., of the UK are heading for 80 percent reduction by 2050.

Other factor in the development towards so called Smart Grids is the interest of the network operators to influence the load of the end users according to the load of the network on the one hand and to offer new services on the other. Toeholds on the end user's side are considered to establish certain "run levels" of the grid by interacting with the end users devices. This intelligent environment also allows for innovative services to the end users as they now can be part of incentive schemes or use home automation functionalities.

Due to the situation of the past, classical metering technology was protected by physical means. The utilities used for energy generation their estimated load profiles and levelled the difference through control energy provided by few exclusively selected generating plants which only purpose was the provision of control energy. In this context there was only a certain amount of communication network needed which was solely in

N. Kuntze, and C. Rudolph are with the Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany.

M. Cupelli, J. Liu, and A. Monti are with the E-ON Energy Reserch Center, Aachen, Germany.

[1] http://vtsenvirogroup.wordpress.com/2009/05/19/you-think-youre-so-smart-grid/

[2] http://www.climatechangecentral.com/publications/c3-views/january-2009/smart-meters-could-help-reduce-electricity-use

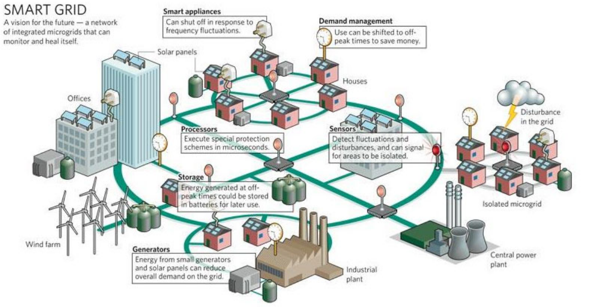
SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.
Smart appliances
Can shut off in response to frequency fluctuations.
Demand management
Use can be shifted to off-peak times to save money.
Solar panels
Houses
Offices
Disturbance in the grid
Processors
Execute special protection schemes in microseconds.
Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.
Storage
Energy generated at off-peak times could be stored in batteries for later use.
Isolated microgrid
Wind farm
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.
Industrial plant
Central power plant

Fig. 1. Smart Grid example

the hand of the utilities. Due to the regulatory laws and with the emergence of Smart Grids and the immense amount of actors in different locations it won't be possible to maintain a closed proprietary communication network anymore. Any utility/company which is interested in participating in the future market has to accept the fact that it has to reach its participant over a potentially insecure communication network where its messages could easily be intercepted and manipulated. Any interception and manipulation of messages where the energy infrastructure is part of it could in the wrong hands harm cause potentially significant damage in the whole energy network.

An extension of the hitherto existing control infrastructure with security aspects put on top of it cannot be easily done. This will result in huge rag rug which will be under constant patching of security holes. Here comes the need of a new approach for control incorporated by design with security. From the control theory perspective all that means that we are moving towards a new system architecture characterized by a set of intelligent operators working as peers in a distributed environment. Obviously, varying requirements w.r.t. the trustworthiness and privacy exist for the operations performed in such systems.

## III. Dependability and security issues in future energy networks

### A. Control Requirement for Smart Grids

The new control requirements for Smart Grids represent a major change in the way Energy grids are managed. These changes are supposed to mostly affect Distribution Network. Historically, Distribution Networks have been operated as passive network with minimal local energy generation. In the future, thanks to Distributed Energy Resources (DER) the situation is supposed to significantly change the grid topology, control systems, security measurements, etc [27], [14]. Through all these changes an additional amount pressure will be put on the power grid during a time where power is one of the most important commodities for economical, industrial and everyday activities. The distribution grid transforms from a star topology into a meshed reconfigurable system. Where the power flow is bi-directional. Which has to be accounted by the infrastructure. With these change follows also in a change in the information flow where it will also become bi-directional [23]. To successful accomplish this changes there is the need of additional monitoring on the medium and low voltage levels with state-estimation, which is a key enabler for Smart Grid applications on the distribution system [6], [7]. Furthermore, the on-going changes in the business models of the utility mostly related to the de-regulation are making clear that a centralized approach to the energy management is not anymore possible. From the control theory perspective all that means that we are moving towards a new system architecture characterized by a set of intelligent operators working as peers in a distributed environment. This situation also determines a much more dynamic operation of the systems where communication plays a significant role both for the stability and the security. Furthermore, the integration in the control infrastructure also of the private households introduces a new level of complexity in the architecture.

### B. Security requirements of Smart Grids

*The heritage that future energy systems have to deal with is the large amount of heterogeneous SCADA-Systems which were designed from a security standpoint as island solutions with no security incorporates a serious problem for distributed Control.*

Obviously, varying requirements w.r.t. the trustworthiness and privacy exist for the operations performed in such systems. The system consists of the power grid itself including communication networks and the devices controlling the processes [16]. One of the requirements concerns with compliance with respect to billing data of the produced capacities and consumed energy carrier. Another aspect is the requirement that the operator can determine the compliance of the state of operation of the overall system, which requires a trustworthy reporting technology for each operating device. These demands create new challenges for the state of the art of existing infrastructures concerning, e.g., non-repudiation of the derived data. Additionally, in many cases it is important to authentically report the current state of the system to third parties.

Common to all energy infrastructures is that it is desirable to establish a common metering infrastructure to be established at the households of the end users [25]. With this approach a interface from the utility towards the house infrastructure is introduced. This interface will then be used by the so called Smart Energy Box which provides a unified Home Area Network (HAM) connecting all devices operating in the household [1]. The metering instruments are owned by the respective network operators but installed at the households of the paying customers the environment is not to by assumed as safe. The system should monitor and protect against attacks on the customer instruments.

Privacy issues have to be covered w.r.t. the derived consumption data as they are created in each metering device. Consumption data contains detailed information that can be used to gain insights on the user behaviour.

### C. Controlling devices in malicious environments

Several activities can be identified in the international context heading into the direction of flexible and adaptable energy creation and distribution systems. One example is the US

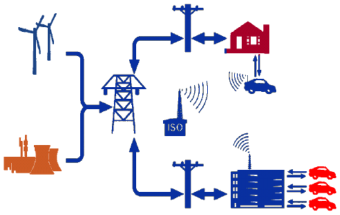

Fig. 2. US "Electric Vehicle to Grid" concept [24]

American "Energy Independence and Security Act (EISA)" which promotes the development of so called Smart Grids providing as one aspect certain security and trustworthiness properties. The IEEE Standards Association (IEEE-SA) is launching a Smart Grid initiative [4] for the power engineering, communications and information technology industries with the creation of the *IEEE Standard 2030 Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS) and End-Use Applications and Loads*. Also on an international level led by the IEC activities are started ensuring the interoperability of the concepts chosen. These activities extend the functionalities of today's SCADA systems and require a higher distribution of these systems. Thus, essential parts of the systems are applied in potentially hostile environments prone to attacks with direct physical access to hardware.

Remote maintenance and control are of special interest. Central authorities should be able to alter the properties of the system without direct physical access to the individual components and to validate the compliance of them. One example are software updates. From the perspective of IT security it has to be guaranteed that only authorised entities are allowed to modify the state of the system. Trust in the system can be defined in this case as the reproduceability of a certain behaviour and the degree with which security requirements are met.

### D. Reliable location information

Current energy networks are mainly static. In future Smart Grids the exact location of parts of the grid become relevant. This is particularly important for moving parts (e.g., batteries of electronic private and public transport vehicles or hydrogen production in vehicles), mobile communication devices used in the grid, or elements with increased distribution as e.g. for phase synchronisation (see Figure 2).

The Hybrid or Electric Vehicles, which can be assimilated to moving batteries, constitute a new challenge for prediction models. As a highly dynamic component of the grid, the energy demand cannot be accurately predicted if its displacement patterns are not known and integrated in the prediction model. In a world in the near future in which hybrid and fully electric vehicles will represent a significant proportion of the total vehicles on the road, the demand created by commuters returning from work in the evening and plugging the vehicle to the grid for example could locally overload the network. In its Draft Publication on Smart Grid Interoperability Standards, the NIST mentions the requirement of geographic data for many Smart Grid applications and proposes the OGC GML standard for the exchange of location-based information.

Further, incentive schemes may prove as one promising way to motivate private households and industry customers to support energy saving technologies. However, the realisation of such schemes requires to enforce contracts negotiated between the parties. With respect to electronic vehicles, for example, incentives in such contracts may also include parameters as for example the location of energy consumption and energy provision to the grid. The exact location of devices or access points to the Smart Grid are very relevant in these scenarios.

By using customer related location data as an element in the Smart Grid even privacy related aspects of the end users are involved. The Smart Grid infrastructure needs to be prepared to tangle even the users demand on the protection of his movement and consumption profile.

### E. Risk assessment

Malicious behaviour is considered a minor threat for classical energy distribution networks and utilities. It is assumed that physical or technical attacks mostly result in a relatively small financial loss and in temporary failures in small parts of the network causing minor disruptions of energy supply. The situation gets much more complex in Smart Grids. Bidirectional flow of energy as well as information, different types of communication interfaces, coupled with other infrastructures (e.g., for communication) results in new attack vectors. Co-ordinated and distributed attacks well-known from ICT networks become feasible in energy networks. Such attacks could result in majour destabilisation of the network and large financial losses of the different stakeholders.

## IV. Multi-layer security and trust infrastructures for energy distribution networks

The radical new designs of future energy networks call for a multi-layered architecture. The growth of the electrical network resulted in a plentifulness of power system software applications, developed in many different computer languages and platforms. Extending old applications or developing new ones usually involves integrating legacy systems. Therefore approaching the dependability and security of future energy networks cannot be done with a complete new start using the so called Greenfield deployment or Big-Bang deployment. In parallel to the development of the energy networks themselves also introducing a complete and monolithic security infrastructure is not a viable option. Multi-layer architecture, advanced control methodologies and dependable software infrastructure as well as device protection mechanisms and hardware security anchors will have to be specified at the same time. Advanced control approaches will have to include predictive and self-adaptive intelligence at higher level and cross-layer mapping to the different technical layers. The dependable software infrastructure will have to be designed to identify and isolate higher-layer independent applications as well as to secure cross-layer communications. With such an architecture we have the flexibility of incorporating parts of already existing infrastructure with the generation of frontiers and interfaces to adjacent systems. Furthermore, the architecture needs the flexibility to interchange or update the part systems in a secure way at a later stage due to new laws and regulations or new developments in the energy market.

Research on control of future energy network with distributed generation towards Smart Grids has been carried out. The Multi-Agent Systems (MAS) technology has been proposed as a potential approach to control the future energy network [15]. This technology was also recognized as being able to overcome the problem of integrating legacy systems by encapsulating them into autonomous agents for interoperability within a larger infrastructure [9]. Moreover, control issues considering the stability, voltage control and power flow with integration of renewable resources have been widely investigated [13][28]. New control challenges arisen by integrating PHEV into future Smart Grids have to be addressed [10]. Smart metering can serve as a powerful tool to improve the network operation in terms of control and monitoring [12][3]. In the last couple of years a great amount of papers was published which investigated MAS based approaches to power system problems [22], [29], [5], [20], [21] and see significant potential in them for contributing to power systems problems in distributed computing, communications, and data integration. All these papers have as a common denominator, that they did not incorporated security as system component in the design phase of their architecture. However, as mentioned before the control architecture and methodology requiring communications have to be addressed together with the development of dependable security infrastructure. In a first step towards a multi-layer security and trust infrastructure the following paragraphs briefly discuss three possible layers.

*a) Smart devices in un-controlled environments:* Current energy network hardware in un-controlled environments relies on physical security for protections. Such mechanisms are not sufficient if smart meters, control systems etc. are connected to open communication networks. Therefore, additional protection mechanisms are necessary. As software solutions are in principle vulnerable to active attacks, worms, viruses, etc. hardware security mechanisms should be considered. One example is the so-called trusted Platform Module TPM that was specified by the Trusted Computing Group and is currently mainly deployed in PCs, laptops or servers. Such hardware security anchors can be used to check the status of the software running on the device during run-time, regularly check the configuration and generate and securely store cryptographic keys. They provide security levels similar as Smart Card chips but integrated into the devices. Based on such hardware trust anchors a lean security infrastructure can be build.

*b) Communication security:* A large variety of secure communication protocols exist. Standardised secure protocols should be used to establish secure channels for the communication between the different entities of the Smart Grid. However, energy networks consists of millions of long-living devices. Thus, topics like key management, update of cryptographic algorithms, identification of devices are not trivial. Some of the issues can be solved by using hardware trust anchors for key generation and storage of keys (i.e. binding keys to particular platforms). However, a variety of open issues exist particularly for efficient, economic and societal acceptable management processes.

*c) Certification and trust authorities:* In a security infrastructure a variety of tasks have to be assigned to entities that are more-or-less trusted. Someone needs to decide on policies for the valid status of devices in the network, certificates for cryptographic keys have to be issued, access policies for the networks and also for sub-networks (e.g. parts of the network in control of the end-user or enterprise energy networks) need to be managed and controlled by different entities. A multi-layer security infrastructure needs to take into account all these different issues. Many open questions remain even when existing technologies are used and a lean architecture for the infrastructure is designed.

*d) Operations of Smart Grid applications:* Control of applications in Smart Grids has to combine many individual local control loops. The novelty for future applications stems from adapting the classical control architectures that are used in static and stable scenarios to highly dynamic networks that constitute a Smart Grid. Individual control loop have to be combined into one or several higher level control loops.Higher level control loops will have to include features for predictive and self-adaptive behavior. They get input from *virtual sensors* and act on *virtual actuators*. A precise definition of these higher level control loops will be necessary for realisations of dependable and secure Smart Grids. Such a precise definition shall involve (i) the specification of the mapping of the artefacts of the high level control loops onto the artefacts of the individual control loops and (ii) the specification of the model of the high level control loop itself. This model has to include the features for predictive and self-adaptive behavior.

## V. Trusted Computing

As shown in section IV protection of the node's identity is an important security requirement. Furthermore, the lack of control on the physical access to the node induces strong requirements on the protection level. One possibility is to root security mechanisms in strong hardware security anchors. Trusted Computing (*TC*) [17] offers such a hardware root of trust providing certain security functionalities. In this section these functionalities are introduced.

TC as defined by the Trusted Computing Group (TCG) are computer systems extended by additional components which shall bring trust to the computing environment. Trust means that components of the system always work as implemented. To achieve this goal, the TCG has published and is still working on specifications describing architectures, affecting system components at any level from hardware to the operating system.

Most important hereby is the specification of the Trusted Platform Module (TPM). This module is mostly realized as a hardware chip hard-wired to the computer platform. It implements basic cryptographic functionality like SHA-1 calculation, message digest creation, random number generation, creation of 2048 bit RSA key pairs, and a RSA engine for encryption and signing purposes. Realized as an independent hardware module, it can provide protected capabilities allowing to shield secret data efficiently. This implementation also allows for in depth testing and validation of the soft- and hardware. The TCG defines three different roots of trust. These are components on which the trust to the whole system is built on.

The Core Root of Trust for Measurement (CRTM) [19] is implemented e.g. as an extension of the BIOS. Its duty is to perform measurements of system components involved in the boot process. Measured components then can perform measurements of other components involved in the next stage of booting. Through this principle of transitive trust, trust in the correctness of the measurement values can be passed on to the OS and the software executed in user space. All components together form a so called Trusted Building Block (TBB) if all components are measured. Through this architecture it shall be guaranteed that a computer system always starts in an authenticated state that can be verified by an external entity and therefore to spur the establishment of trust.

The second root of trust is the Root of Trust for Reporting (RTR). One of the aims of TC is to enable computer systems to proof to other platforms that it is in a trusted state. Therefore the results of measurements of system components have to be presented to the remote platform. To guarantee the genuineness of these data, they are signed. For this purpose every TPM contains a 2048 bit RSA key pair, the Endorsement Key (EK), which is generated before shipping. The EK, together with an EK Credential, represents the identity of the platform. Pseudonymous representatives of the EK, so called Attestation Identity Keys (AIK) are used for signatures, for example of measurement results used by the remote party to verify the correctness of the desired state (Remote Attestation or Direct Anonymous Attestation) [2].

The third root of trust is the Root of Trust for Storage (RTS) with the purpose to establish a secure storage for cryptographic keys and other sensitive data. The RTS is implemented by introducing the Storage Root Key (SRK), a second 2048 bit RSA key pair stored in the non-volatile memory of the TPM. The SRK never leaves the shielded location of the TPM. That allows building a hierarchy of keys, with the SRK as the root, in which direct successors are protected by encryption with the SRK. These keys on their part can protect any number of other keys. Thus, trust is bequeathed from the SRK. Any key, following up the SRK can be stored off-chip, not least because memory in TPM is limited, but the number of possible TPM-generated keys is not. Keys never leave the TPM in clear; they are always encrypted by parent keys. The benefit from this is the possibility to work with encryption keys, which in the end are under protection of a hardware module and with this the possibility to encrypt data based on a hardware module. These keys allow to bind data to a device or even to a particular state of the device.

## VI. Application of TC in Smart Grids

Smart Grid development can benefit from trusted Computing technologies in various ways. The most obvious application of TC in the grid is where devices live in (possibly) malicious environements. The following paragraphs highlight some of the advantages of supporting cyber security in Smart Grids with TC technology or other similar hardware-based security mechanisms.

### A. *Secure identification of devices*

Currently, computers in IP-based networks are ususally identified by their MAC address. As this identification is not secure, additional mechanisms need to be used to prevent malicious devices to access the network. Many of these additional security measures involve the user (e.g. by asking for passwords). A Smart grid requires clear distinctions between device identification and users. furthermore, additional parameters like the location can become important. Trusted Computing can provide secure hardware-based identities (or pseudonymous identification if required) and data or netwrok access can be bound to a particular identity.

### B. *Integrity of executable software and configurations*

For secure operations the status of a device is relevant with respect to the executable software running on the device and the configuration of the device. Attacks on cyber security often involve the manipulation of software or installation of additional executable code (e.g. trojans, viruses, bot-nets, worms). TC technology can be used to stop critical components of the Smart Grid from executing malicious code or to regularly report the status of the component to other parts of the grid in order to enable fast reactions to attacks. Such information can also be used in security information management processes. In addition to these cyver-security issues for the Smart Grid itself, also end-users can benefit as manipulations on devices controlling appliances in the house or local energy production have the potential to create financial loss for the end-user.

### C. *Economic and efficient security*

Trusted Platform Modules provide an integrated solution for many security-related functionality, such as generation of cryptographic keys, secure storage, shielded locations, or platform integrity measurement. It is very useful to consider security early in the design process. Standardised interfaces and functionalities already on the lowest level of hardware provide a clear security design space that can be a basis of the treatment of cyber security in Smart grid development. from an economic point of view it is much better to already include the security viewpoint in early prototypes and operational field tests. By using standardised security modules such as the TPM this early integration can be done in a very efficient and econimic way.

### D. *Privacy protection*

Privacy relevant data is generated and processed mainly in the metering devices locate in the houses of the end users and as part of the vehicular use case. In the scenario concerning the stationary metering equipment Trusted Computing allows for a trustworthy computation environment that allows for privacy protection by precomputing certain aggregated data sets. Mobile scenarios are involving also location data and interactions with e.g. gas stations revealing privacy relevant details. Trusted Computing approaches allow for the introduction of (one time) pseudonyms or even anonymous credentials for the establishment of a trust relationship. Schemes similar for example to [11] are allowing for privacy aware solutions.

## VII. Conclusions

Security and dependability requirement are obviously critical for the energy infrastructure. Nevertheless, this issue has not raised to attract the deserved attention. In our view, it is highly inefficient to consider security as simply added on top of control. We foresee that an integrated approach could bring significant benefits to the system operation. This paper highlights some of the arising (and partly already existing) issues and proposes some ways to continue with research and development work towards security and trust infrastructures for future energy networks.

## References

[1] Nist framework and roadmap for smart grid interoperability standards release 1.0 (draft). Technical report, NIST, September 2009.

[2] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 132–145. ACM New York, NY, USA, 2004.

[3] S. Bruno, S. Lamonaca, M. L. Scala, G. Rotondo, and U. Stecchi. Load control through smart-metering on distribution networks. In *IEEE Proceeding PowerTech, Bucharest*, 2009.

[4] R. DeBlasio and C. Tom. Standards for the Smart Grid. *Atlanta*, 17:18, 2008.

[5] A.L. Dimeas and N.D. Hatziargyriou. Operation of a multiagent system for microgrid control. *IEEE Transactions on Power Systems*, 20(3):1447–1455, 2005.

[6] R. Gelagaev, P. Vermeyen, and J. Driesen. State estimation in distribution grids. In *Harmonics and Quality of Power, 2008. ICHQP 2008. 13th International Conference on*, pages 1–6, 28 2008-Oct. 1 2008.

[7] Frdric Gorgette, Olivier Devaux, and Jean-Luc Fraisse. Possible roadmaps for new requirements for french distribution control and automation. In *19th International Conference on Electricity Distribution(CIRED)*, 21-24 May 2005.

[8] T. Gul and T. Stenzel. Variability of wind power and other renewables: Management, options and strategies. Technical report, IEA, Paris, 2005.

[9] V. Honavar, L. Miller, and J. Wong. Distributed knowledge networks. In *Information Technology Conference, 1998. IEEE*, pages 87–90, Sep 1998.

[10] C. Hutson, Venayagamoorthy G.K., and K.A. Corzine. Intelligent Scheduling of Hybrid and Electric Vehicle Storage Capacity in a Parking Lot for Profit Maximization in Grid Power Transactions. In *Energy 2030 Conference*, 2008.

[11] Nicolai Kuntze, Dominique Mähler, and Andreas U. Schmidt. Employing trusted computing for the forward pricing of pseudonyms in reputation systems. In *Axmedis 2006, Proceedings of the 2nd International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution, Volume for Workshops, Industrial, and Application Sessions*, 2006.

[12] P.K. Lee and L.L. Lai. A practical approach of smart metering in remote monitoring of renewable energy applications. In *Power & Energy Society General Meeting*, 2009.

[13] M. N. Marwali and A. Keyhani. Control of Distributed Generation Systems – Part I Voltages and Currents Control. In *IEEE Transcations on Industrial Electronics, VOL. 19, NO. 6, pp. 1541–1550*, 2004.

[14] S. Massoud Amin and B.F. Wollenberg. Toward a smart grid: power delivery for the 21st century. *Power and Energy Magazine, IEEE*, 3(5):34–41, Sept.-Oct. 2005.

[15] S. D. J. McArthur, E. M. Davidson, V.M. Catterson, A. L. Dimeas, N.D. Hatziargyriou, F. Ponci, and T. Funabashi. Multi-Agent Systems for Power Engineering Applications – Part I and Part II. In *IEEE Transactions on Power Systems, Vol. 22, Issue 4, pp. 1743–1759*, 2007.

[16] P. McDaniel and S. McLaughlin. Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy*, pages 75–77, 2009.

[17] C. Mitchell et al. Trusted Computing. *Trusted computing*, page 1, 2005.

[18] AD Peacock and M. Newborough. Impact of micro-CHP systems on domestic sector CO2 emissions. *Applied Thermal Engineering*, 25(17-18):2653–2676, 2005.

[19] S. Pearson. Trusted computing platforms, the next security solution. *HP Labs*, 2002.

[20] L. Phillips, M. Link, R. Smith, and L. Weiland. Agent-based control of distributed infrastructure resources. Technical Report SAND2005-7937, Sandia National Laboratories, Jan 2006.

[21] M. Pipattanasomporn, H. Feroze, and S. Rahman. Multi-Agent systems in a distributed smart grid: Design and implementation. In *Proc. Proc. IEEE PES 2009 Power Systems Conference and Exposition (PSCE09)*, 2009.

[22] T. Rigole, K. Vanthournout, and G. Deconinck. Distributed control systems for electric power applications. In *Proceedings 2nd Workshop on Networked Control Systems, Rende, Italy*, 2006.

[23] Jan Ringelstein and David Nestle. Application of bidirectional energy management interfaces for distribution grid services. In *Electricity Distribution, 2009 20th International Conference and Exhibition on*, pages 1–4, June 2009.

[24] J. Tomić and W. Kempton. Using fleets of electric-drive vehicles for grid support. *Journal of Power Sources*, 168(2):459–468, 2007.

[25] A. Treytl, N. Roberts, and GP Hancke. Security architecture for power-line metering system. In *2004 IEEE International Workshop on Factory Communication Systems, 2004. Proceedings*, pages 393–396, 2004.

[26] Amjad Umar and C. W. Fraser. *Distributed computing: a practical synthesis of networks, client-server systems, distributed applications, and open systems*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1993.

[27] E. Valigi and E. di Marino. Networks optimization with advanced meter infrastructure and smart meters. In *20th International Conference and Exhibition on Electricity Distribution*, 2009.

[28] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright. Distributed MPC Strategies With Application to Power System Automatic Generation Control. In *IEEE Transactions on Control Systems Technology, Vol. 16, No. 6, pp. 1192–1206*, 2008.

[29] Z. Zhang, J. D McCalley, V. Vishwanathan, and V. Honavar. Multiagent system solutions for distributed computing, communications, and data integration needs in the power industry. In *Proceedings of IEEE Power Engineering Society General Meeting*, volume 1, page 4549, 2004.