IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 1 April 2013; revised 3 September 2013; accepted 21 October 2013. Date of publication 4 November 2013;
date of current version 21 January 2014.

Digital Object Identifier 10.1109/TETC.2013.2288275

Enhanced Network Coding to Maintain Privacy in Smart Grid Communication

HASEN NICANFAR[1] (STUDENT MEMBER, IEEE), PEYMAN TALEBIFARD[1] (STUDENT MEMBER, IEEE), AMR ALASAAD[2] (MEMBER, IEEE), AND VICTOR C. M. LEUNG[1] (FELLOW, IEEE)

[1] WiNMoS Laboratory, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada
[2] National Center for Electronics, Communications and Photonics, King Abdulaziz City for Science and Technology, Riyadh 11442, Saudi Arabia

CORRESPONDING AUTHOR: H. NICANFAR (hasennic@ece.ubc.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada under Grant STPGP 396838, and by the National Center for Electronics, Communications, and Photonics at King Abdulaziz City for Science and Technology in Saudi Arabia.

ABSTRACT Cyber-physical systems (CPS) are aimed at combining the physical system with the cyber ones to provide a better control and improve the management of physical systems around us. Recently, the CPS and its applications, e.g., health-care and smart grid, have gained attention of the research community. In this paper, we consider the privacy aspect of users in a CPS, particularly in smart grid system as our use-case, and provide a mechanism that utilizes the advances in network coding to maintain data privacy. We address privacy issues associated with gathering metering information of clients in a smart grid system. In smart grid systems, wireless multi-hop communications are mainly used to gather metering information through exchanging data and control messages between smart meters and the utility. We argue that any communication paradigm used in a smart grid should support all aspects of privacy such as anonymity, unlinkability, unobservablity, and undetectablity. We propose innovative schemes for traffic routing and encryption that benefit from the enhanced network coding technology. Our analysis shows that our schemes maintain privacy of users despite the possibility of detecting metering data by an adversary. In addition, our scheme has extra favorable features such as less computation complexity, reliable, and robust communication.

INDEX TERMS Anonymity, unlinkability, undetectability, unobservability, network coding, privacy, smart grid.

I. INTRODUCTION

Rapid developments in the computer science, and information and communication technology along with the control advances in physical systems have emerged into a new direction of multi-disciplinary engineering systems called Cyber-Physical Systems (CPS) [2]–[4]. This revolutionary section of the science enables humans to interact with and control the environment more efficiently and effectively. "*CPSs will transform how humans interact with and control the physical environment to the greater benefit of society*" [4]. Regardless of having a fully or semi-auto controlling system, the system relies on collecting data to make the controlling decisions for the physical and controlling interactions, or as part of the system feedback loop [5]. Normally, the fine-grained data gathered/sensed by the sensing devices, e.g. sensors or metering devices [6], are transferred to the monitoring/controlling parties for further actions, e.g. get processed and make the controlling decisions. There are many example of the CPS applications such as health-care [3], manufacturing automation, energy (smart grid), agriculture, defense and transportation [4], [6]–[9] to name a few. In this paper, we describe our scheme and designs specifically for the case of smart grid.

Smart grid system is aimed at improving power generation, transmission, distribution and consumption through contribution and collaborations of different stockholders such as utility sector, service providers and consumers [10], [11]. In all systems and applications that follow demand-response

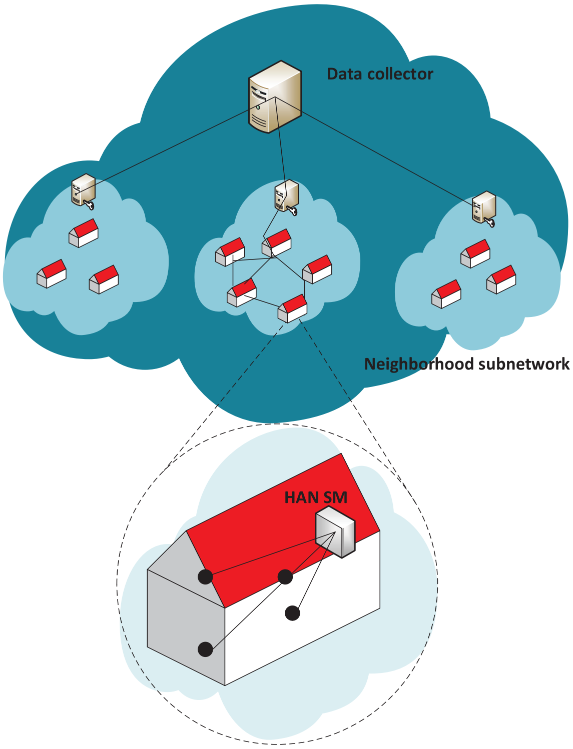


FIGURE 1. **Smart grid network architecture.**

architecture such as the advanced metering infrastructure (AMI) used in a smart grid system, information about the actual or planed power consumption are key elements [12]. In this case, smart meters are used to periodically collect live metering data from end-users, e.g. home area networks (HANs). This information is then transmitted to the utility via AMI to be used for billing purposes. Also, this information is used by the service provider as a reference to efficiently plan service delivery [13]. Furthermore, this fine-grained information is used by the energy management system to provide users with real-time price (tariff) of the power upon which the consumers can take advantage of the low price times. This motivates consumers to move their power demands to off-peak hours so as to efficiently use the power and decrease their monetary costs [10].

Different communication technologies have been proposed for the AMI such as power line communication and wireless communication [14]. In North America, wireless multi-hop communication technologies (e.g., ad-hoc and mesh networks) are proposed to be used for exchanging data and control messages over the AMI between smart meters or gateways of HANs and the utility [1], [13]–[17]. In this case, data traffic is transmitted from a smart meter to the utility and vice versa over multi-hop wireless links with intermediate network nodes forwarding traffic (Figure 1).

Privacy in the smart grid is identified as one of the biggest concern by the research community, considering the uncertainty in the environment [7]. Due to the broadcast nature of wireless transmissions in the AMI, an attacker can overhear communication between any adjacent wireless nodes. This enables the attacker to detect valuable information, which can compromise privacy of the clients. Even if the transmitted packets were encrypted, the attacker may correlate the amount of traffic transmitted by a particular user at different times to infer private information about the user by applying a user behavior model. Thus, having well defined security and privacy system are preliminary demands for implementation readiness of the smart grid system. Although it may be tempting to try to patch existing protocols such as random paths and anonymous routing to provide some level of privacy [18], the privacy of the users in the smart grid system needs to consider more precise specifications such as anonymity, unobservability, unlinkability, and undetectability. This requires different designs of traffic routing in order to meet the required privacy properties. For example, when using anonymous routing protocols, an adversary may detect data traffic generated by an individual smart meter to infer information about appliances existed in a HAN (by monitoring trends of power consumed by different appliances), and information about behavior of the users (by monitoring amount of power usage in the HAN). Although a trivial scheme that generates dummy packets may solve the unobservability problem, it fails to address anonymity, unlinkability and undetectability while introducing high amount of the overhead to the system. We refer to the Pfitzmann-Hansen definitions of the privacy [19], which we describe in Section II.

Contribution: Our proposed schemes address the problem of preserving privacy of users in a smart grid system by maintaining all necessary features required for privacy in such a system including anonymity, unlinkability, undetectability and unobservability communications.

None of the existing schemes in the literature simultaneously address all these properties together. We identify five privacy measures for the CPS communication such as hiding source, destination, path, traffic volume and content. We address this problem using an enhanced network coding technique. Our proposed schemes basically benefit from the capability of the network coding in encoding transmitted linear combination of packets.

We review our definition of privacy in the smart grid context and provide a background for network coding in Section II followed by literature review in Section III. Our proposed schemes are presented in Section IV, while we analyze the performance of our proposed schemes in Section V. We conclude the paper in Section VI.

II. BACKGROUND

A. DEFINITION OF PRIVACY

There are different proposed definitions for the privacy. Bob Blakley defines privacy as "*The ability to lie about yourself and get away with it*" [20], or "*The right to be left alone*". The latter definition has been adopted by NIST [21].

Pfitzmann and Hansen provided six features for the privacy [19] as follows:

1) ANONYMITY

The most used feature in the literature for the privacy is anonymity. "*Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set*" [19]. The main goal of the anonymity is to make a party anonymous from others, even a peer. There are two defined forms for the anonymity: *Sender Anonymity* and *Receiver Anonymity*.

2) UNLINKABILITY

The situation of not being able to distinguish relationship between two items in a system is referred to as unlinkability. Unlinkability is required for different items in the smart grid such as smart device, smart meter, controller of a HAN, Building Area Network or Neighborhood Area Network, aggregator, system/sub-system (located in cloud or in any of the smart grid servers) or group (like multicast group).

3) UNDETECTABILITY

Undetectability of an item (entity, application or process) from an adversary's perspective means that the adversary is not able to sufficiently distinguish whether the item exists or not.

4) UNOBSERVABILITY

Unobservability of an item (entity, application or process) means that first of all, undetectability of the item against all subjects uninvolved in it. In addition and at the same it means the anonymity of the subject(s) involved in the item even against the other subject(s) involved in that item.

5) PSEUDONYMITY

"*A pseudonym is an identifier of a subject which is different from the subject's real names*". For instance, a smart meter can have multiple identities known by whom the smart meter is communicating with. Pseudonym can be defined as person pseudonym, role pseudonym, relationship pseudonym, role-relationship pseudonym, transaction pseudonym, with respect to the relationship and link between the pseudonym and its holder.

6) IDENTITY MANAGEMENT

Entities of a system that follows pseudonymity approach have multiple identities. Each identity can be based on one or some attributes of the entity. Managing the identities in terms of assigning and controlling them in a way that makes the item unidentifiable by any unauthorized party is the task of identity management.

B. NETWORK CODING

Network coding has been widely used to improve the robustness and bandwidth efficiency of multicast routing in special network topologies. However, the inherit feature of packet encryption in the network coding can be exploited to provide privacy for users in a smart grid. Furthermore, the distributed nature of the network coding increases its robustness against possible attempts of attackers. The simplest coding scheme is linear coding [22], [23]. Linear network coding treats a block of data as a vector over a certain base field of coefficients. Each intermediate node performs a linear transformation and achieves a linear combination of the incoming edges before delivering them to the next node(s).

Network coding is used in communication to target maximizing throughput, minimizing energy per bit and Minimizing delay [24]. A linear combination of received packets at the encoding nodes is transmitted with a linear coding coefficient vector or Local Encoding Vector (LEV). The GEV is used to form the transfer matrix for the entire system. Practical instances of the network coding constitute the following: (i) Random coding [25] which allows the encoding to be done in a distributed fashion, (ii) Packet tagging of each packet with LEV allows the decoding to be done in a distributed manner, and (iii) Buffering which is required for asynchronous packet arrivals and departures with arbitrarily varying rates, delay, and loss.

Let us assume an acyclic network (V, E, c) with unit capacity edges $c(e) = 1$ for all $e \in E$. Let $x_1, x_2, ..., x_h$ be the h packets that our graph, from an over all point of view, wishes to carry. Bringing the coefficients of all nodes $v \in V$ into account and in short, if we assume an "$h \times h$" model, (1) shows the relationship between received packets (y_is) and sent packets (x_is). Matrix T presented by (2) is called transfer matrix of the network, therefore, receiver(s) can use (3) to extract the original x_i out of y_i. T is based on each node coefficient and should be an invertible matrix, which having a random coefficient guarantees that.

$$\begin{bmatrix} y_1 \\ \vdots \\ y_h \end{bmatrix} = \begin{bmatrix} t_1(e_1) & \dots & t_h(e_1) \\ \vdots & \ddots & \vdots \\ t_1(e_h) & \dots & t_h(e_h) \end{bmatrix} \times \begin{bmatrix} x_1 \\ \vdots \\ x_h \end{bmatrix} \tag{1}$$

$$T = \begin{bmatrix} t_1(e_1) & \dots & t_h(e_1) \\ \vdots & \ddots & \vdots \\ t_1(e_h) & \dots & t_h(e_h) \end{bmatrix} \tag{2}$$

$$\begin{bmatrix} y_1 \\ \vdots \\ y_h \end{bmatrix} = T \times \begin{bmatrix} x_1 \\ \vdots \\ x_h \end{bmatrix} \Rightarrow \begin{bmatrix} x_1 \\ \vdots \\ x_h \end{bmatrix} = T^{-1} \times \begin{bmatrix} y_1 \\ \vdots \\ y_h \end{bmatrix} \tag{3}$$

Depicted by Figure 2, and since transfer matrix T is not fix due to dynamic and randomness of the coefficients, a receiver requires to calculate T^{-1} each time based on received tags. To improve the calculations of (3), [26] proposes using sub-graph in order to handle different sources' traffics to different destination. More specifically, the main graph is divided to parallel sub-graphs, and packets from a source to a destination traverse in only one sub-graph. The aim in [27] is finding the minimum cost multicast sub-graph, where delay values

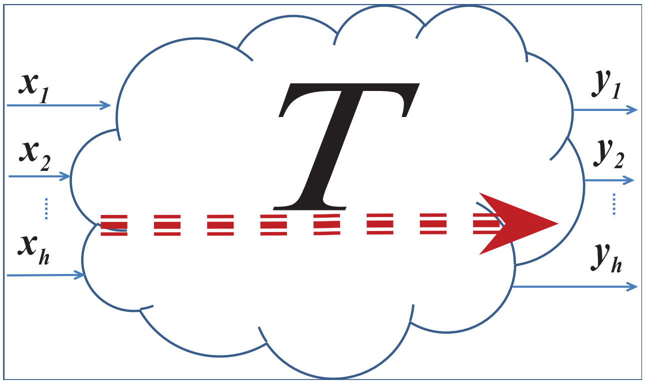


FIGURE 2. **Matrix of transfer.**

associated with each link, limited buffer-size of the intermediate nodes and link capacity variations over time are taken into account.

III. RELATED WORK

Wayne Wolf proposed the concept of the cyber-physical systems. He mentioned that understanding and using of computer needs to change, "*Cyberphysical systems actively engage with the real world in real time and expend real energy. This requires a new understanding of computing as a physical act, a big change for computing*" [2]. The challenges of the CPS design and deployment are studied in [3]. The authors mentioned that global warming coupled with energy shortage and the aging of the population are the objects of the CPS, and they identified the research challenges for the CPS as real-time system abstractions, robustness of CPS, quality of service composition, and knowledge engineering. In [4], the CPS is studied as a combination of multiple fields of science such as computing, communication and control systems. The author compared the evolution of the CPS to the Internet, and provided some applications of the CPS in real world, e.g. smart grid for the power sector. He also mentioned that privacy should be preserved by the CPS: "*These CPSs will have embedded and distributed intelligence, operating dependably, securely, safely, and efficiently in real time, while satisfying privacy constraints*". The author also presented advances of the CPS, such as fully autonomous vehicles, smart power grids and extreme-yield agriculture, as well as the impact of the CPS on society and education. Modeling the CPS is studied in [5], where authors provided challenges of the CPS caused by heterogeneity, concurrency, and sensitivity to timing of CPSs, by modeling the dynamics considering the evolution of a system state over time.

A survey on the CPS in [7] presents a number of CPS and their features. The authors also described state-of-the-art CPS researches in energy control, secure control, transmission and management, control technique, system resource allocation, and model-based software design. Authors also described the research CPS challenges in the area of control and hybrid systems, sensor and mobile networks, robustness, reliability, safety, and security, abstractions, model-based development, and verification, validation, and certification.

The work in [6] considers the case of smart grid as an application of the CPS, which is related to the scope of our work in this paper. The research work presented in [8] considers security of the smart grid. Author discussed the security aspects of the cyber-physical controls required to support the smart grid, which takes into account the power application. They analyzed the security from the risk point of view, and address the security concerns in control systems of the generation, transmission and distribution of the power in the smart grid. Furthermore, they studied the security of the infrastructure support and devices as well as security management and intrusion detection systems, followed by list of research challenges in this area. In this paper, however, we focus on the privacy aspect of the smart grid in this paper. To the best of our knowledge, we are the first to propose comprehensive schemes to address all features required to preserve privacy of clients in a smart grid system.

The scope of the work in [9] is the smart grid as well, in which the authors presented a security-oriented cyber-physical state estimation system. Their proposed system identifies the compromised set of hosts in the cyber network and the maliciously modified set of measurements obtained from power system sensors, at each time instant. They used the concept of the IDS, which utilizes stochastic information fusion algorithms and merges sensor information from both the cyber and electrical infrastructures. The innovation of their proposed work is using the IDS system to monitor the cyber infrastructure for malicious or abnormal activity, in conjunction with knowledge about the communication network topology. Similarly in [28], the authors concentrated on the effect of intrusion detection and response on the reliability of a CPS. They considered a CPS system comprises of sensors, actuators, control units, and physical objects for controlling and protecting a physical infrastructure. Their developed model is based on stochastic Petri nets to emulate the behavior of the CPS in the presence of both malicious nodes exhibiting a range of attacker behaviors. They also proposed an intrusion detection and response system for detecting and responding to malicious events at runtime.

The scope of the work in [29] is data center from the CPS point of view, in which the authors considered the controlling system of data centers versus the ITC system. Precisely, the proposed model considered a computational network representing the cyber dynamics and a thermal network representing the physical dynamics as two coupled networks in a control oriented model. In [30], safety, security and sustainability (S3) of the CPS is the target of the study, in which they proposed a formal framework for representing cyber-physical interactions in a CPS. Authors also studied the challenges that are applicable to this framework. In [31], the authors provided a review of the historical technology developed to the CPS systems, as well as applications of the CPS along with the new research challenges and directions.

M. Stegelmann *et al.* proposed a scheme, wherein smart meter sends the metering data to a local aggregator, and then the aggregator applies the anonymity before sending the data to service providers. Although data for the billing is not anonymous, the same data is anonymous when it is sent to the service provider for the planning [32]. However, this scheme provides only source anonymity in portion of the data deliveries. The presented system in [33] aimed at anonymity of the smart meters by combining the data collected by each smart meter with an *ortho code*, in a ring architecture, to the utility via an aggregator. The utility, without realizing the identification of each smart meter, can obtain the meters by summation information processed by aggregator. As the authors mentioned as well, they only provided anonymity of the sender (smart meter).

A Secured routing protocol for ad-hoc network is presented in [34], which enables anonymity of the source, destination and path. In this protocol, a source initiates and broadcasts a path request including a path sequence number and the encrypted destination address. The relay nodes only rebroadcast the path request after recording it. The destination responds back (unicast) to the path request, and nodes along the path reserve the path by matching information about the previous and next hops. However, this protocol is vulnerable to the flow tracing attack.

In [35], a network coding based scheme is used for privacy preserving, which extends the work in [34] by providing source anonymity. The scheme forwards a random-based linear vector encrypted Global Encoding Vector (GEV) at each intermediate node in which only the destination is capable of decrypting the GEV. The receiver has to undergo the decryption of the tags, forming transfer matrix, and heavy process of the reverse matrix calculation. The scheme presented in [36] also utilizes network coding to support security and privacy.

In [37], the linear network coding is used to maintain privacy of the mobile nodes in a wireless mesh network environment. The proposed mechanism is aimed at flow untraceability and movement untraceability of the nodes. However, the proposal mainly pay attention to the flow of the information of the mobile nodes, and does not preserve anonymity of the nodes, especially when an attacker is listening to the first mesh router that receives the data/packet from the mobile node.

The proposal scheme in [38] aimed at flow anonymity of the data to provide the anonymity of the communicating parties by tacking advantage of mixing characteristic of the coding. Although the scheme concentrates on anonymity of the source and destination by hiding the flow identifies causes by mixing the flows, it does not address other aspects of the privacy.

IV. SYSTEM DESIGN

In this section, we first describe our assumptions. we then present our proposed enhanced the network coding mechanism and describe our privacy-preserving scheme.

A. ASSUMPTIONS AND SYSTEM SETUP

Our assumption are as follows:

- Public key encryption system that has a private key generator (PKG) responsible for the key management. The detail of the encryption system can be found in the literature, e.g. [17].
- Nodes have already performed an authentication scheme. They have also received their private key as well as the system parameters from the PKG.
- Topology is almost static: For instance in case of the smart grid, the maximum movement of nodes are within a HAN, although the smart meter of the HAN is static.
- A smart grid server, which can be in charg eof the PKG duties as well, is aware of the topology and graph of the network.

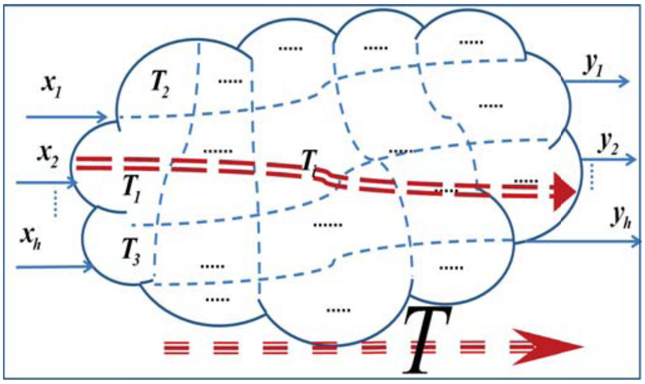


FIGURE 3. Matrix of transfer, with sub-graphs.

B. ENHANCED NETWORK CODING

As shown in Figure 3, the system administrator divides the main topology/graph G into "m" sub-graphs $SubG_i$ (he may consider the proposed solution in [27] for sub-graphing) and forms sub-graphs set $\widetilde{SubGS}$ such that:

$$\begin{cases} \widetilde{SubGS} = \{SubG_i \mid i = 1, 2, \ldots, m\} & \text{(4a)} \\ G = \bigcup_{i=1}^{m} SubG_i = \bigcup_{SubG_i \in \widetilde{SubGS}} SubG_i & \text{(4b)} \end{cases}$$

In each sub-graph $SubG_i$, system administrator selects n_s nodes to be the network coding nodes, which perform the network coding activities such as encoding. Furthermore, system administrator nominates one of the nodes to be head cluster of the sub-graph, which can be shown by HC_i.

We consider transfer matrices set $\widetilde{TS}$, which T_i represents transfer matrix of $SubG_i$ such that:

$$\widetilde{TS} = \{T_i \mid i = 1, 2, \ldots, m\} \tag{5}$$

Similarly, we consider inverse of transfer matrices set $\widetilde{TRS}$, which TR_i represents inverse of the transfer matrix of the sub-graph $SubG_i$, such that:

$$\widetilde{TRS} = \{TR_i | i = 1, 2, ..., m\} \tag{6}$$

Furthermore, we introduce a new parameter "α_i" as follows:

$$\alpha_i = \begin{cases} 1\ , & data\ crosses\ SubG_i & (7a) \\ 0\ , & data\ does\ not\ cross\ SubG_i & (7b) \end{cases}$$

Finally, we define "$h \times h$" transfer matrix $\widehat{T}$ which converts an input data matrix $\widehat{X} = \left[x_1\ x_2\ \cdots\ x_h\right]^T$ to the output data matrix $\widehat{Y} = \left[y_1\ y_2\ \cdots\ y_h\right]^T$, following (8a) and (8b).

$$\begin{cases} \widehat{T} = \prod\limits_{T_i \in \widetilde{TS}\ \&\ \alpha_i = 1} T_i, \quad i = 1, 2, \ldots, m & (8a) \\ \widehat{Y} = \widehat{T} \times \widehat{X} & (8b) \end{cases}$$

Similarly and at the receiver side, (9a) and (9b) are used to decode $\widehat{X}$ out of $\widehat{Y}$. Note that $\widehat{TR} = \widehat{T}^{-1}$.

$$\begin{cases} \widehat{TR} = \prod\limits_{T_i \in \widetilde{TS}\ \&\ \alpha_i = 1} T_i^{-1}, \quad i = 1, 2, \ldots, m & \\ \quad\ \ = \prod\limits_{TR_i \in \widetilde{TRS}\ \&\ \alpha_i = 1} TR_i, \quad i = 1, 2, \ldots, m & (9a) \\ \widehat{X} = \widehat{TR} \times \widehat{Y} & (9b) \end{cases}$$

C. PRIVACY-PRESERVING SCHEME

Referring to Section II, a receiver requires the LEVs of a graph (over which the data has passed through) in order to compute the transfer matrix. In a linear network coding, there are two parameters that can be changed, such as network topology (path) and coefficient factors (LEVs). One solution is having one of these two values to be fixed and the other one changes dynamically (or, in some cases both of them can be dynamic). To be more precise, we can keep the topology (path) static, and randomly choose the coefficients, which in this case the coefficients information should be transferred (some how, and securely) to the receivers to make the receiver capable of decoding the data. On the other hand, we can fix the coefficients and randomly choose the path, which in this case information about the path, or the network coding nodes (that have performed network coding operation/encoding), should be transferred to the receiver.

Note that LEV is a function of the coefficient factors [24]. Without loss of generality:

$$T_i = Function(LEV_{SubG_i}), \quad i = 1, 2, ..., m \tag{10}$$

Since we keep the sub-graph structure fix, only knowing coefficients is missing to compute the transfer matrix(ces) of the sub-graphs, which the server is capable of doing it. From an abstract point of view, in our system, we keep the topology, nodes coefficients and structure of the sub-graphs fix, although the sub-graphs that the data is crossing is being selected randomly. Our mechanism phases are as follows:

Algorithm 1 System setup

```
Define:
$PrvK_{ID_j}$ : Private key of node $ID_j$.
$Coef_{ID_j}$ : Coefficient factor of node $ID_j$.
$PKG$ : Private Key Generator.
$F_{coef}(.)$ : Shared hash function.
$SubG_i$ : "$i^{th}$" sub-graph in sub-graph set $\widetilde{SubGS}$.
$T_i$ : Transfer matrix of the sub-graph $SubG_i$.
$\widetilde{TRS}$ : Set of inverses of transfer matrices of the sub-graphs.

Algorithm:
$PKG \leftarrow ID_j$
$PKG :\ (PrvK_{ID_j}\ ,\ F_{coef}(.)\ ,\ i) \rightarrow ID_j$ {$PKG$ calculates the private key}
$Coef_j \leftarrow F_{coef}(PrvK_{ID_j})$ {Perform by $PKG$ and $ID_j$}
$\widetilde{SubGS} = \{SubG_i |\ i = 1, 2, ..., m\}$ {Defined by system administrator}
$PKG \leftarrow \widetilde{SubGS}$ {Receive from the system administrator}
$T_i^{-1} \leftarrow T_i \leftarrow (SubG_i\ ,\ Coef_j\ s.t.\ ID_j \in SubG_i)$ {Performed by $PKG$}
$\widetilde{TRS} = \{T_i^{-1} | i = 1, 2, ..., m\} = \{TR_i | i = 1, 2, ..., m\}$
$\widetilde{TRS} \rightarrow Destination$
```

1) PHASE I: SETUP

Firstly (Algorithm 1), PKG provides a *One-Way* hash function $F_{coef}(.)$ to the nodes. Each node applies $F_{coef}(.)$ to its own private key to obtain its coefficient (11):

$$Node\_Coefficient = F_{coef}(Node\_PrivateKey) \tag{11}$$

In a PKI-based system, only PKG and each node know the private key of the node. System administrator provides all information about the topology and graph consists of the participating nodes in each sub-graph to PKG. PKG calculates T_i and T_i^{-1} of each $SubG_i$ and provides the T_i^{-1}s to a destination.

Note that a private key can be considered as a random-based secret value managed by PKG. For instance, in an identity-based cryptography approach, like [39], the private key of a node is multiplication of a secret random value generated by PKG and the public key of the node. Since the coefficient is a function of the private key (11), the randomness is implied for the coefficient as well, and referring to [24], T_i is invertible.

Since $F_{coef}(.)$ is a *One-Way* function, even if any of the receivers acts maliciously, an attacker would not be able to utilize matrix T_i^{-1} and performs a reverse operation to obtain the private keys of the nodes. We discuss more about this in Section V. Furthermore, a private key is a dynamic value [17], therefore, transfer matrices T_i (and T_i^{-1}) are also dynamic. Note that the PKG is responsible to maintain and update the matrices and informing the receivers, for instance in case of the smart grid, the smart grid servers, which collect the data, should be notified by this server (PKG).

2) PHASE II: GENERATING AND SENDING THE PACKETS

Presented by Algorithm 2, a sender chooses a nonce and assigns it to the *TAG*, and a nonce random identity for the *TAG*, which we show it as ID_{TAG}. Then, the sender chooses

Algorithm 2 Generating and sending the packets

```
Define:
$PubK_{ID_a}$ : Public key of node $ID_a$.
$PrvK_{ID_a}$ : Private key of node $ID_a$.
$NSG_{ID_s}$ : Set of next optional sub-graphs to the destination for sender $ID_s$.
$e_{ek}(.)$ : Encrypting with key $ek$.
$sign_{ek}(.)$ : Signature of data using key $ek$.
$X$ : “$1 \times h$” size matrix of plain packets to be sent.
$\widehat{X}$ : “$1 \times h$” size matrix of encrypted packets to be sent.
$TAG$ : “$m$” bit size vector; each bit represent one sub-graph.
$ID_{TAG}$ : A nonce value represents the identification of the $TAG$.
$F_{nc}(k)$ : A nonce generator function in “$k$” bits size.

Algorithm:
{$ID_s$ chooses one $SG_i$ out of $\widetilde{NSG}_{ID_s}$ with an equal probability}
$MyNSG \leftarrow Random(\widetilde{NSG}_{ID_s})$ Random choosing a sub-graph out of $\widetilde{NSG}_k$ set
$TAG \leftarrow F_{nc}(m)$ {Encryption of the tag. “$m$” is total number of sub-graphs}
$ID_{TAG} \leftarrow F_{nc}(m)$ {Choosing a nonce vale for the tag identification}
$DataH \leftarrow (ID_s, ID_r, TAG, ID_{TAG})$ {Data header}
$SgnH \leftarrow sign_{PrvK_{ID_s}}(DataH)$ {Signing the data header}
{$ID_s$ encrypts data (packet by packet) using public key of the receiver}
for ($l = 1 \rightarrow h$) do
    $\widehat{X}.[1, l] \leftarrow e_{PubK_{ID_r}}(X.[1, l])$ {Encryption}
end for
$(\widehat{X}, e_{PubK_{ID_r}}(DataH), SgnH, TAG, ID_{TAG}) \rightarrow MyNSG$ {Sending encrypted data, data header, signature of the header, $TAG$ and $ID_{TAG}$ to the next sub-graph}
```

Algorithm 3 Relaying the packets

```
Define:
$NSG_i$ : A set of next optional sub-graphs to the destination for “$i^{th}$” sub-graph.
$\widehat{Y}_i$ : Input “$1 \times h$” size data matrices at sub-graph $SubG_i$.
$\widehat{X}_i$ : Output “$1 \times h$” size data matrices at sub-graph $SubG_i$.

Algorithm:
$SubG_i \leftarrow (\widehat{Y}_i, DataH, SngH, TAG, ID_{TAG})$ {Receiving data, data header, signature, tag and tag ID}
if ((Looks up $ID_{TAG}$) == NO) then
    $\widehat{X}_i \leftarrow SubG\_Function(\widehat{Y}_i)$ {The result of $SubG_i$ internal process}
    $SHFT\alpha_i \leftarrow 2^{i-1}$ {Shift “$\alpha_i$” to the “$i^{th}$” bit position}
    $TAG \leftarrow (TAG \otimes SHFT\alpha_i)$ {Record “$\alpha_i$” into $TAG$}
    Records $ID_{TAG}$
end if
$MyNSG \leftarrow Random(NSG_k)$ {Choosing $SubG_k$ out of $\widetilde{NSG}_k$ set}
$(\widehat{X}_i, DataH, SngH, TAG, ID_{TAG}) \rightarrow MyNSG$ {Sending data, tag, tag ID and data header to the next sub-graph}
```

one of the adjacent sub-graphs with equal probability to send the data. Then, the sender forms the data header including the nonce values and address of the receiver. Furthermore, the sender signs the header with its own private key in order to preserve the source authentication as well as the data header integrity. Finally, the sender sends the encrypted data (packets) and data header, signature of data header and plain form of the tag and its ID to the next sub-graph toward the receiver.

Note: *TAG* is an array that traverses with the data. Each bit of the *TAG* represents α_i of a sub-graph ((7a) and (7b)). To be more precise, the i^{th} bit of the array is converted to one if the data passes through $SubG_i$. Therefore, initially *TAG* consists of only zeros ($TAG = 0$). Since *TAG* is sent in a plain format, we load it with a nonce value, and forward the nonce (encrypted) to the destination. Then, in each sub-graph, the head cluster only reverses the value of the i^{th} bit. In other words, we *XOR* this bit with α_i. Consequently, at the destination only needs to *XOR* the result with the original nonce value to decrypt the tag and obtain list of the sub-graphs that the data has passed through. Comparing to the network coding operation, especially at the receiver, changing one bit per sub-graph is negligible overhead added cost by our mechanism.

Note: Referring to our discussion in Section II about the network coding, normally the coefficient that each network coding node use to handle the coding process, needs to be sent to the receiver for encoding process (by receiver). In our design, we eliminate sending this overhead data (coefficients) in cost of sending the tag and tag identity. In fact, tag ID is similar to the flow ID that is being used by the network coding, and our additional overhead cost is the tag itself. The overhead cost of sending the tag is much less than sending the coefficients, since in network coding there is one coefficient per network coding node, and we only have one tag from source to destination.

3) PHASE III: RELAYING THE PACKETS

As it is shown in Algorithm 3, we consider a situation that our data is entering to the $SubG_i$. The data passes through $SubG_i$ concerning the defined connections and coefficient values of the nodes (network coding nodes are already identified by the administrator). The head cluster of the sub-graph needs to record α_i into *TAG* by changing the i^{th} bit of *TAG*. Similar to the previous step (sending data), the head cluster of the sub-graph $SubG_i$ randomly selects one of its neighbour sub-graphs to transfer the data to toward the receiver.

Note: Since the next sub-graph is chosen randomly, the data may get entered to the same sub-graph more than once. In order to prevent this looping situation, the identity of the tag (ID_{TAG}) is referred by the header of the sub-graph (HC_i). Indeed, HC_i keeps a record of the ID_{TAG} that is processed by the sub-graph, in addition to IDs the sub-graphs that it is received from and is sent to, for some time in order to prevent processing it twice. The reasonable expiry time of keeping the record can be same as smart meters periodic collecting time, e.g. 15 minutes. In this case, the assumption is that the data will be received and decoded by the receivers during 15 minutes. Therefore, first of all, HC_i does not lead the processed (coded) information to be sent to the same sub-graph that is coming from. Secondly, if it receives the same data (ID_{TAG}) from another sun-graph, it will forward the data as-is and without coding it again, to the next randomly chosen sub-graph excluding the sub-graphs that are received from as well as the data has been sent previously to. It is obvious that in a worse case scenario, the data will reach the destination after being processed by the entire sub-graphs only once.

4) PHASE IV: RECEIVING AND DECODING THE PACKETS

Presented by Algorithm 4, when a receiver receives the data:

- Utilizes its own private key to decrypt the header to obtain addresses of the sender and receiver, and the nonce.

Algorithm 4 Receiving and decoding the packets

```
Define:
$\widehat{T}$ : Transfer matrix from source to destination.
$\widehat{TR}$ : Inverse of the transfer matrix from source to destination.
$y$ & $x$ : Received packet and sent packet.
$\widehat{Y}$ : Matrix of the received packets with size of "$1 \times n$".
$\widehat{X}$ : Matrix of the sent packets with size of "$1 \times n$".
$e_{ek}(.)$: Encrypting with key $ek$.
$d_{dk}(.)$: Decrypting with key $dk$.

Algorithm:
$Receiver \leftarrow (\widehat{Y}, DataH, SgnH, TAG, ID_{TAG})$ {Receiving packets, data header, signature, tag and tag ID}
$OrgNonceEnc \leftarrow DataH$
$OrgNonce \leftarrow d_{PrvK_{ID_r}}(OrgNonceEnc)$
Verify $Sgn$ {If verification result is positive, proceed}
$TAG \leftarrow (TAG \otimes OrgNonce)$ {XOR with the original nonce for decryption}
$\widehat{TR} \leftarrow I$ {$I$ is identical matrix}
for $(i = 1 \rightarrow m)$ do
    if $(TAG.[i] == 1)$ then
        $\widehat{TR} \leftarrow (\widehat{TR} \times TR_i)$
    end if
end for
$\widehat{X} \leftarrow \widehat{TR} \times \widehat{Y}$
for $l = 1 \rightarrow h$ do
    $X.[1, l] \leftarrow d_{PrvK_{ID_r}}(\widehat{X}.[1, l])$ {Decryption}
end for
```

- Referring to the sender address, verifies the signature, and if it is valid, *XOR*es the nonce with the received tags for decryption.
- Referring to the bit values of *TAG*, selects T_i^{-1} (TR_i) of sub-graphs that data has passed through, and multiplies them together to obtain the reverse value of the path transfer matrix $\widehat{TRS}$ via (9a).
- Obtains original packets sent by the sender via (9b).

V. SYSTEM EVALUATION

In this section, we present our analysis from privacy and system performance point of views. First we propose two adversary models, then compare our delivered privacy factors comparing to the literature, and finally in the communication and network performance subsection, we discuss complexity and reliability of our design.

A. ADVERSARY MODELS

We refer to Dolev-Yao model [40] to design our two adversary models including external and internal adversaries, in case of the smart grid system.

1) EXTERNAL ADVERSARY

In this case, the adversary is an external party and is not an entity of the system.

Objectives: The adversary objective is obtaining information about the HAN occupancy and its resident behaviour.

Initial capabilities: The adversary knows the detail information about the initial security system as well as our proposed privacy mechanism. For instance, the adversary knows public keys of the entire parties and has the detail knowledge about the network topology, graph and sub-graphs. Furthermore, the adversary knows the detail design of our mechanism including algorithms shown by Algorithm 1–4. Finally, the adversary has enough technical knowledge and is fully-equipped to be able to listen to the channels and analyze the traffic.

Capabilities during the attack: The adversary receives all of the packets entering to a HAN (smart meter of HAN) and departure from the HAN. Beside, the adversary can listen to the channel of any other entity of the system like PKG and any destination, to collect their receiving data.

Note: By using the term *data*, we mean and refer to the exact data that is in the channels (encrypted and/or encoded).

Discussion: Refer to our assumption, a HAN gateway (smart meter) acts as relay node in a mesh-based topology. We also implement and perform enhanced network coding that mixes the packets utilizing sub-graphs. Since source and destination addresses are encrypted inside the header, our scheme delivers the anonymity and undetectability, which yields to unobservability. If the adversary listens to entering and departing data from a HAN, he does not gain any useful information, since the entering packets plus HAN packet are encoded into one packet, which hides the HAN packet. If the origin of a packet is an appliance, listening to the channel does not help the adversary to obtain anything about the existence of the appliance (undetectability over appliances). In the proposed schemes in the literature (Section I), he can understand HAN is generating a packet by listening to the first node, so, mostly those schemes only make a private path.

The packets entering a smart meter to be relayed, also do not have the source address, and are entering to the sub-graphs randomly. Therefore, the adversary cannot trace back the packets or monitor flow of the data, so unlinkability is delivered since he cannot observe direction of the data.

Last position for the adversary is at receiver side and listening to the receiving data. Considering above discussion about the hidden address of the receiver, he only obtain the flow of information to the destination. Indeed, since the data travels through random chosen sub-graphs to reach the destination, he cannot trace back the data. Consequently, our scheme maintains anonymity and unlinkability here too.

Note that in any of the above situations, gaining access to *TAG* does not help the adversary. Indeed, encoding *TAG* with a random nonce makes sub-graphs capable of inserting α_i without decoding *TAG*. He does not obtain anything by having an encoded *TAG*, even at the first or last sub-graphs.

2) INTERNAL ADVERSARY

Adversary is an internal party, e.g., he has access to one of the HANs and can particularly monitor gateway of the HAN or analyze the gateway information.

Objectives: Gaining access to the neighbour HANs information by receiving their data for relay.

Initial capabilities: The malicious node is already authenticated and receives the system parameters and its own private key, so our adversary has these information.

Capabilities during the attack: The malicious node is under control of the adversary and performs the Algorithm 3.

TABLE 1. Delivery of the privacy measures.

Scheme	[18]	[32]	[34]	[35]	[36]	[33]	[37]	[38]	Our proposal
Anonymity	✔	✖ & ●	✔	✔	✔	✔	●	●	✔
Unlinkability	●	✖ & ●	●	●	●	✔	✖	●	✔
Undetectability	✖	✖	●	●	●	✖	✖	✖	✔
Unobservability	✖	✖	✖	✖	✖	✖	✖	✖	✔

Discussion: Having access to a malicious node only improves the adversary situation on modifying its HAN data. The relay nodes only mix the packets and do not perform any encryption and decryption. Furthermore, the data that he receives does not show any sign of the source or destination. Consequently, his capability and behave is almost same as the previous scenario.

B. PRIVACY PERFORMANCE ANALYSIS

Referring to Sections II and III as well as our proposal in Section IV, TABLE 1 presents performance of our scheme comparing to the discussed schemes in Section I. We consider two types of the attackers such as a neighbour and a relay node. Some of the schemes may deliver the anonymity in case of relay nodes; however, the data is not anonymous for a neighbour. We also use the following symbols to describe each deliverable:

- "✖": Does not deliver the measure.
- "●": Delivers the measure only against relay nodes.
- "✔": Delivers the measure against all nodes.

C. COMMUNICATION AND NETWORK PERFORMANCE ANALYSIS

In this subsection, we provide an analysis and evaluation on the aspects of probability of success and complexity as well as intrusion success likelihood, and reliability for the proposed approach. Throughout the discussion we consider a square grid network topology. The communication performance evaluation of our proposed coordinated method is evaluated against the random network coding approach of [41] where authors claim a throughput performance gain over no coding. However, while there are advantages to network coding approaches, the success of these methods highly depends on the characteristics of topology. In this method, nodes continuously replicate and forward messages to newly discovered nodes.

1) COMPLEXITY

One of the overheads with the network coding is that nodes must have the processing capability to perform arithmetic operations over finite fields in real time. This processing will determine whether a decoded content chunk is innovative and makes a decision to either encode, forward, or decode. The processing complexity involved in operations over fields depends on the size of each generation h, and size of the field n. It takes $O(h^2)$ operations in F_{2^n} for linear operations with generations of size h. Multiplications and inversions over field F_{2^n} is of complexity $O(n^2)$. Furthermore, matrix inversions and Gaussian elimination to solve the system takes $O(h^3)$.

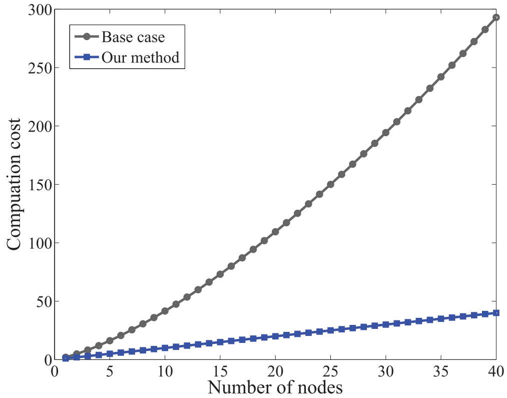


FIGURE 4. Cost of computing.

As shown in Figure 4, the cost of computing in our method is lower since the transfer metric at the receiver is implied and need not to be recalculated every interval. The computational cost in our algorithm is reduced because enhanced network coding is performed on a selected set of nodes within each cluster.

2) RELIABILITY

Our method aims at minimizing the number of nodes that shall perform the network coding operations. Therefore, we can take advantage of opportunities for fixed the network coding where possible. It is intuitive that as the system size increases, random network coding on large number of node compromise the overall computational complexity and degrades the overall probability of success.

The probability that a random network coding problem is solvable depends on whether the global coding vector has a full rank. If the coefficients are randomly chosen from a field F_q, then probability for a generation to be invalid is at most $\frac{|T|}{|q|}$. The extension of the *Schwartz-Zippel* theorem yields the probability of success at each random coded node as follows:

$$Pr(success) = (1 - \frac{|T|}{q})$$

where $Pr(success)$ is the probability of success within the cluster of random network coding. The following theorem from [25] states the probability of success by a valid network code.

Theorem 5.1: The probability of a random network code with coefficients from field F_q being valid and being successfully decoded in a multicast connection problem with $|T|$ number of receivers and $|S|$ number of sources is $(1 - \frac{|T|}{q})^\eta$ where $q > |S|$ and η is the number of intermediate links with associated random coefficients.

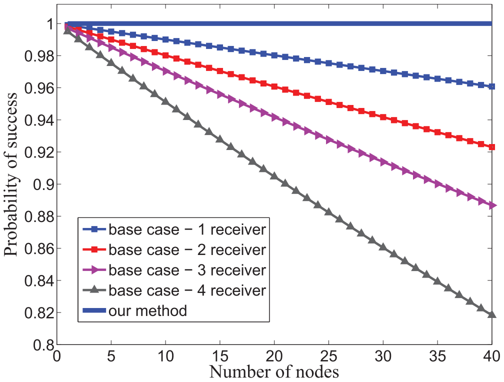


FIGURE 5. **Probability of success.**

As depicted by Figure 5, in contrast to the base case scenario, where random network coding is used, our proposed method utilizes a fixed network coding approach where the coefficients are dependent on the private key. Therefore, the uncertainty about the existence of a solution for the system is being resolved.

VI. CONCLUSION

In this paper, we have proposed a privacy-preserving approach for the smart grid system, an application of the cyber-physical system. We developed an enhance network coding technique for packet routing to hide source, destination, path, traffic volume and content information of the packets. We introduced concept of the sub-graphing the network for this purpose, and used a subset of the sub-graphs to transfer the data, which improve the energy consumption and system complexity. Also, we eliminated sending the coefficients of the network coding nodes to the receiver for performing the decoding process, which saves the bandwidth. We have shown that our scheme maintains multiple favourable privacy preserving metrics such as anonymity, unlinkability, undetectability and unobservability for communications over the advanced metering infrastructure. We evaluated the performance of our scheme using both simulation and analytical analysis. Our result show that our proposed schemes provide reliability to the system without adding much complexity.

REFERENCES

[1] H. Nicanfar, P. TalebiFard, A. Alasaad, and V. C. Leung, "Privacy-preserving scheme in smart grid communication using enhanced network coding," in *Proc. IEEE ICC*, Jun. 2013, pp. 1–3.

[2] W. Wolf, "Cyber-physical systems," in *Proc. Comput., Embedded*, 2009, pp. 88–89.

[3] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *Proc. Mach. Learn. Cyber Trust*, 2009, pp. 3–13.

[4] R. Rajkumar, "A cyber–Physical future," *Proc. IEEE*, vol. 100, no. 13, pp. 1309–1312, May 2012.

[5] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.s

[6] H. Li, L. Lai, and H. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1097–1107, Jul. 2012.

[7] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proc. Int. Conf. WCSP*, Nov. 2011, pp. 1–6.

[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[9] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[10] (Sep. 2010). NIST Smart Grid, Cyber Security Working Group. *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, Gaithersburg, MD, USA [Online]. Available: http://www.nist.gov/smartgrid

[11] T. M. Chen, "Survey of cyber security issues in smart grids," *Proc. SPIE*, vol. 7709, pp. 1–11, Apr. 2010.

[12] A. Rossello-Busquet, "G.hnem for AMI and DR," in *Proc. ICNC*, Feb. 2012, pp. 111–115.

[13] P. Kulkarni, S. Gormus, Z. Fan, and F. Ramos, "AMI mesh networks—A practical solution and its performance evaluation," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1469–1481, Sep. 2012.

[14] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, *et al.*, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, Jan. 2013.

[15] H. Gharavi and B. Hu, "Multigate communication network for smart grid," *Proc. IEEE*, vol. 99, no. 6, pp. 1028–1045, Jun. 2011.

[16] J. Wang and V. Leung, "A survey of technical requirements and consumer application standards for IP-based smart grid AMI network," in *Proc. ICOIN*, Jan. 2011, pp. 114–119.

[17] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, to be published.

[18] V. Mohanty, D. Moliya, C. Hota, and M. Rajarajan, "Secure anonymous routing for MANETs using distributed dynamic random path selection," in *Proc. Intell. Security Inf. Pacific Asia Workshop*, 2010, pp. 65–72.

[19] A. Pfitzmann and M. Hansen, (2010). *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management* [Online]. Available: http://dud. inf. tu-dresden. de/literatur/Anon_Terminology_v0

[20] B. Blakley, (2006, Oct. 23). *What is Privacy, Realy* [Online]. Available: http://podcast.burtongroup.com/ip/2006/10/what_is_privacy.html

[21] *National Institute of Standard and Technology* [Online]. Available: http://www.nist.gov/

[22] S. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[23] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[24] P. A. Chou and Y. Wu, "Network coding for the internet and wireless networks," *IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 77–85, Sep. 2007.

[25] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, *et al.*, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[26] P. Bao-xing, Y. Lu-ming, W. Wei-ping, and X. Xiao, "Linear network coding construction for multi-source multicast network," in *Proc. 1st Int. Workshop ETCS*, vol. 3. 2009, pp. 114–118.

[27] H. Ghasvari, M. Raayatpanah, B. Khalaj, and H. Bakhshi, "Optimal subgraph selection over coded networks with delay and limited-size buffering," *IET Commun.*, vol. 5, no. 11, pp. 1497–1505, 2011.

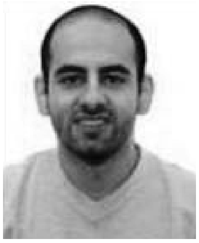
[28] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.

[29] L. Parolini, B. Sinopoli, B. H. Krogh, and Z. Wang, "A Cyber–Physical systems approach to data center modeling and control for energy efficiency," *Proc. IEEE*, vol. 100, no. 1, pp. 254–268, Jan. 2012.

[30] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012.
[31] K.-D. Kim and P. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, no. 13, pp. 1287–1308, Jan. 2012.
[32] M. Stegelmann and D. Kesdogan, "GridPriv: A Smart metering architecture offering k-anonymity," in *Proc. IEEE 11th Int. Conf. Trust, Security Privacy Comput. Commun.*, Jun. 2012, pp. 419–426.
[33] S. Li, K. Choi, and K. Chae, "An enhanced measurement transmission scheme for privacy protection in smart grid," in *Proc. ICOIN*, 2013, pp. 18–23.
[34] X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, "ASR-PAKE: An anonymous secure routing protocol with authenticated key exchange for wireless Ad Hoc networks," in *Proc. IEEE ICC*, Jun. 2007, pp. 1247–1253.
[35] Y. Fan, Y. Jiang, H. Zhu, J. Chen, and X. S. Shen, "Network coding based privacy preservation against traffic analysis in multi-hop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 834–843, Mar. 2011.
[36] J. Wang, J. Wang, C. Wu, K. Lu, and N. Gu, "Anonymous communication with network coding against traffic analysis attack," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1008–1016.
[37] J. Wang, K. Lu, J. Wang, and C. Qiao, "Untraceability of mobile devices in wireless mesh networks using linear network coding," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 270–274.
[38] A. O. Fathy Atya, T. ElBatt, and M. Youssef, "On the flow anonymity problem in network coding," in *Proc. 9th IWCMC*, Jan. 2013, pp. 225–230.
[39] H. Nicanfar and V. C. Leung, "EIBC: Enhanced identity-based cryptography, a conceptual design," in *Proc. IEEE Int. Syst. Conf. (SysCon)*, Mar. 2012, pp. 1–7.
[40] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[41] C. Gkantsidis and P. Rodriguez, "Network coding for large scale content distribution," in *Proc. IEEE Comput. Commun. Soc. 24th Annu. Joint Conf.*, vol. 4. Mar. 2005, pp. 2235–2245.

HASEN NICANFAR (S'11) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of British Columbia, the B.A.Sc. degree in electrical engineering from the Sharif University of Technology in 1993, and the M.A.Sc. degree in computer networks from Ryerson University in 2011. From 1993 to 2010, he was involved in different positions such as an IT/ERP Manager, a Project Manager, and Business and System Analyst. His research interests are in the areas of trust, security and privacy in wireless communication, computer network, and cloud computing.

PEYMAN TALEBIFARD (S'08) received the B.Eng. degree with high distinction in communications engineering from Carleton University in 2006, and was awarded the Senate Medal for high academic achievements. He attended graduate school at the University of British Columbia (UBC) and received the M.A.Sc degree in electrical and computer engineering in 2008. He is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, UBC. His research includes design and analysis of architectures, protocols, and management, control and solutions for interworking of heterogeneous wireless access networks and next generation networks for reliable, efficient, and cost effective communications in telecommunication and computer networks.



AMR ALASAAD (S'09–M'13) is an Assistant Professor with the National Center for Electronics, Communications and Photonics, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia. His research interests are in the broad areas of wireless networks and mobile system, P2P resource sharing protocols, routing and scheduling in wireless mesh networks, content sharing and replication schemes. He received the Ph.D. degree in electrical and computer engineering from the University of British Columbia, the M.S. degree in electrical and computer engineering from the University of Southern California, and the B.Sc. degree in electrical engineering from King Saud University in 2000, 2005, and 2013, respectively.

VICTOR C. M. LEUNG (S'75–M'89–SM'97–F'03) is a Professor of electrical and computer engineering and holds the TELUS Mobility Research Chair at the University of British Columbia. He has contributed more than 600 technical papers and 25 book chapters in the areas of wireless networks and mobile systems. He was a Distinguished Lecturer of the IEEE Communications Society. He has been serving on the editorial boards of the IEEE Transactions on Computers, the IEEE Wireless Communications Letters and several other journals, and has served on the organizing and technical program committees of numerous conferences. He was a winner of the 2012 UBC Killam Research Prize and the IEEE Vancouver Section Centennial Award.