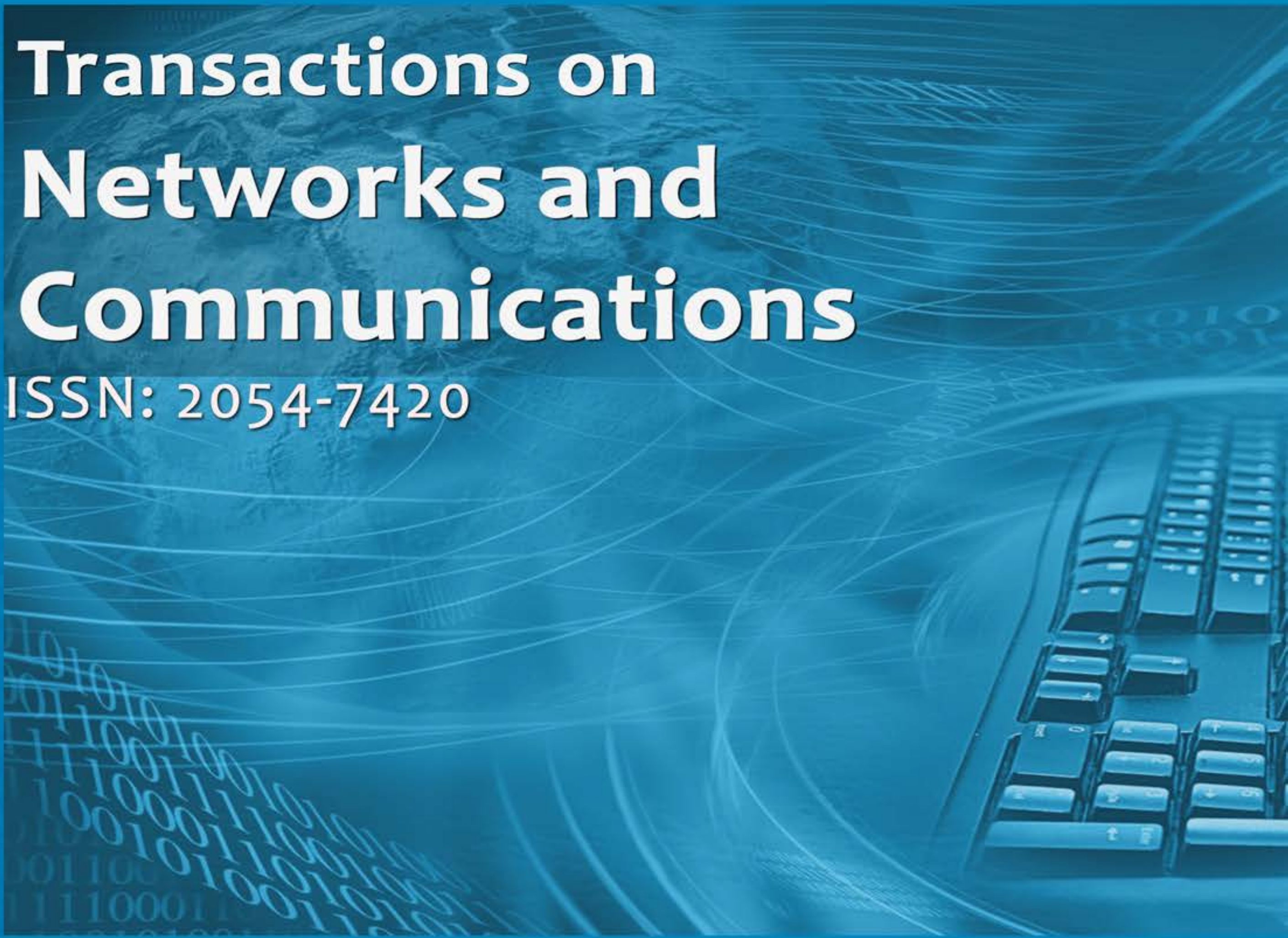
Volume 4 No. 5, October 2016



Transactions on Networks and Communications

ISSN: 2054-7420

Society for Sciences and Education - United Kingdom

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone’s views or feelings etc.

Society for Science and Education
United Kingdom

TNC Transactions on Networks and Communications

Volume 4, Issue 5
ISSN: 2054 -7420

An Energy Efficient Data Aggregation for Random Sensor Networks

M. Shanmukhi[1] and O.B.V. Ramanaiah[2]
[1]Associate Professor, Malla Reddy College of Engineering, JNTUH, Hyderabad, Telangana, India.
[2]Professor, College of Engineering, JNTUH, Hyderabad, Telangana, India
shanmukhi.m@gmail.com; obvramanaiah@gmail.com

ABSTRACT

Energy-efficient computing is the thrust area of research in an energy-constrained Wireless Sensor Network (WSN). Comb Needle Model (CNM) exists in literature for energy efficient data aggregation in regular (grid-based) WSNs. Clustering concept is added to CNM to reduce the energy consumption further. Besides, basic CNM is extended for randomly deployed WSNs. In this paper, the extended CNM for random WSNs is augmented with clustering mechanism. When clustering is added to the Extended CNM, it will aggregate the data at Cluster Head and minimizes the number of data transmissions, and thereby extends the network life span. The CNM uses the push-pull data distribution approach. It may overload certain sensor nodes, and lead to hotspots, which causes excess amount of energy loss. We extend the CNM with clustering in random network to overcome these issues and perform energy efficient processing. This paper makes the simulation based comparative analysis of the Extended CNM with clustering with that of without clustering. The performance metrics considered are energy consumption, communication cost, delay, packet loss, packet delivery ratio, and throughput. It is empirically observed that the network life span is improved substantially.

Keywords: Wireless Sensor Network, Cluster based comb needle model, Communication cost, energy efficiency.

1 Introduction

Wireless Sensor Networks (WSNs) are widely deployed in recent era because they extend our ability to control and monitor physical environment from far away. They improve the accuracy of sensing by using distributed processing of large quantities of sensed information (e.g., high resolution images, seismic data, and acoustic data). When sensors are networked they can aggregate such data to provide the different views of the environment. Several difficulties need to overcome to deploy a good WSN. These difficulties may arise from the limited computation power, limited energy and communication resources available for the sensors in the WSN [1-3]. Figure 1 shows the wireless sensor network architecture for a military application [4].

DOI: 10.14738/tnc.45.2223
Publication Date: 28th September 2016
URL: http://dx.doi.org/10.14738/tnc.45.2223

Energy: Sensor nodes have limited battery power, if they deployed in the sensing field their battery cannot be replenished, that is the reason, WSN require energy efficient protocols for computation and communication.

Computation: sensors are small devices they have limited computational ability, so they cannot run complex network protocols.

Communication: The sensed data should be communicated to sink otherwise it is useless. If all the sensor nodes try to send data to sink it consumes more power. So the data should be aggregated and only useful data should be communicated to sink. Hence we require efficient data aggregation techniques in WSN [5, 6].

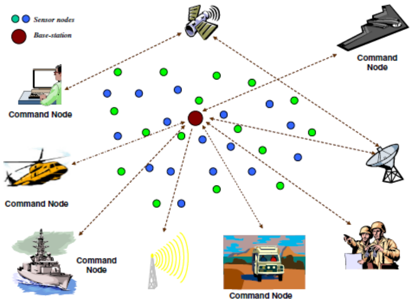


Figure1. Wireless Sensor Network Architecture for Military Applications [Taken from 4]

Many civilian and military applications have taken advantage of WSN. The advantage is its ability to perform operation in unattended harsh environments, where working of human beings is difficult and risky. In such cases sensor networks produce efficient results.

In large WSN hundreds or thousands of sensor nodes may involve to meet the civilian application requirements. To design and operate such large WSN would require scalable architecture and management strategies.

If we consider three key factors- Energy, computation and communication in a sensor node, designing energy-aware and efficient computing algorithms becomes an added advantage for WSN to extend the lifetime of sensors.

Clustering also plays important role in minimizing energy. So many clustering methods have been developed by research community to achieve the objective such as network scalability. Every cluster will be having a group of nodes with a group leader called cluster head (CH). Many clustering algorithms have been developed in literature for ad-hoc networks [7-11]. Recently, many number of cluster algorithms are specifically designed for WSNs [12-16]. The proposed clustering algorithms vary from one another in terms of network architecture, node deployment, network operation model, and the features of the CH nodes.

This paper proposes cluster based scheme for data aggregation mechanism by using Comb Needle Model (CNM), which is applied in random sensor networks.

In the Extended CNM for random networks [17], when an event occurs, all the sensor nodes present on the comb participate in transmitting the reply to the base station (See Figure 2). This may result in lot of communication cost and energy consumption, which depletes nodes energy and, it may lead to hotspot problem in the WSN. To overcome this issue clustering has been added for data gathering in extended CNM for random networks.

There are some assumptions in this research about the network and application as given below:

- Any time and any where an event may occur
- Any node may get query from its neighbor
- All nodes knows their location

Remaining paper organization is as follows: Related work is explained in Section 2. Section 3 elaborates the proposed method. The analytical evaluation of the proposed method is given in Section 4. Experimentation has been done using Network Simulator NS2, and the results obtained are presented in Section 5. Section 6 concludes the paper.

2 Existing Work on Data Aggregation in WSN

Data aggregation plays a vital role in the WSN for conserving energy [18]. Several characteristics associated with the aggregation have been discussed by researchers in literature. For example several energy efficient algorithms to perform data aggregation are studied [18]. To perform data aggregation scheduling algorithm for maximizing throughput and reducing delay were discussed in [19], and aggregation based routing protocol was demonstrated in [20].

Apart from data precision or data quality, delay, energy efficient algorithm also a significant performance outlook of data aggregation. The trade-off between energy efficiency and quality of data aggregation is first detected by Pharm et al. [21]. Afterwards, Zhu et al. [22] had analyzed the quality of service in the data aggregation of the wireless sensor networks for estimating the exact precision needed for completely specific task. Later on, Xu and Tang [23] had illustrated about the data precision gathered from various sensor nodes for improving network life span and minimizing the energy consumption. There are various similar papers, which aim to improve the data quality within the given life span or energy for the data aggregation [24].

Tang et al. [25] had proposed an energy-efficient protocol in the MAC layer for reducing the energy consumption in the nodes by altering the senders to detect the receiver’s wake up time. For achieving data transmission optimization with a static routing strategy, sensor nodes transfer the larger data to other nodes, which may consume the high energy at the earlier stage, it may create hotspots. To neglect the issues of the hotspots so many steps had been taken in the last decade. The previous methods are generally classified into two types: (i) Using the node-stage context for energy-aware data distribution strategy and (ii) exploiting the clustering methods for energy efficient management.

Hou et al. [26] had proposed a data protocol in wireless sensor networks. The protocol utilized adaptive network coding to minimize broadcast traffic for the function of codes updation in the wireless sensor networks. This protocol is further analyzed and developed by Shwe et al. [27], introduced an efficient neighbor discovery protocol to detect out all the nearby nodes for minimizing the power consumption in the wireless sensor networks. Later on, Lun et al. [28] have proposed a random linear network coding scheme that accomplishes the packet-stage capacity for both the unicast and multicast connections in wireless sensor networks.

Data classification, a prominent tool for data analysis, is widely used in variety of applications, such as, image processing, pattern recognition, market analysis, social behavior study, data mining, and so on. McQueen et al. [29] has proposed the k-means algorithm, one of the most fundamental and popular algorithm for unsupervised classification (data clustering). It employs the Euclidean distance, as a pattern similarity measure. The k-means algorithm is extended with additional heuristics to govern the process of splitting and/or merging of clusters, and is well known as ISODATA (Iterative Self-Organizing Data Analysis Technique) algorithm proposed by Ball et al [30]. ISODATA is used as a benchmark for all data clustering algorithms. Based on ISODATA, OBV Ramanaiah et al. [31] has proposed a distributed version (D-ISODATA). It clusters the voluminous distributed databases 'in place', without the need for uploading to a central location. It eliminates the demerits associated with the centralized clustering of voluminous database, such as, communication costs, storage requirements, and administrative complexity. D-ISODATA algorithm is adapted for mobile environment, which we call m-ISODATA *m* stands for mobile) [31]. Two schemes, named as discard partition and use recent history, are proposed to cope with the disconnection of MHs participating in the distributed clustering process. The proposed concept uses the basic ISODATA algorithm.

X. Liu [32] proposed Comb Needle Model to perform data aggregation based on push and pull strategies. Shanmukhi et al [33] had demonstrated Cluster based Comb Needle Model for grid networks. It has minimized communication cost and maximized the throughput. Shanmukhi et al [17] had applied the Comb-Needle Model in simple random network and achieved best results. Shanmukhi et al [34], carried out survey on data aggregation techniques. The survey of the data aggregation and energy consumption process had analyzed their mechanism and the drawbacks, our proposed method would be efficient than all these methods and overcome these drawbacks.

3 Proposed Concept

The CNM was proposed by X. Liu et al [32] for regular network (grid deployment) to perform data aggregation. Clustering has been added to CNM for regular network [33] to perform efficient data aggregation with energy efficiency. The basic CNM is extended to support the data aggregation in *randomly deployed* sensor networks [17] as shown in Figure 2.

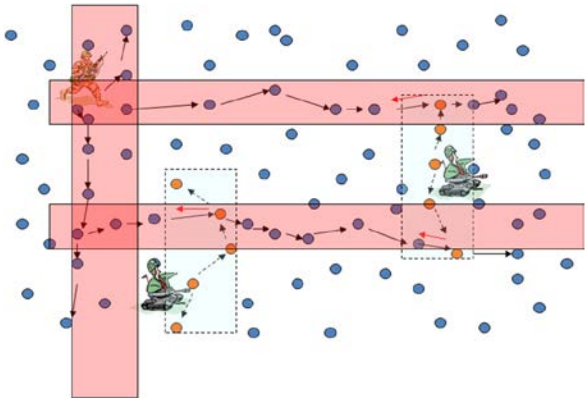


Figure 2. Basic Comb Needle Model in Random Network [Taken from 17]

Now in this work clustering is added to the extended CNM. The same is illustrated in Figure 3. See Table 1 for summarization of these works. When we add clustering to the Extended CNM, it helps to improve the data aggregation and decreases the energy consumption and improves the lifespan of network.

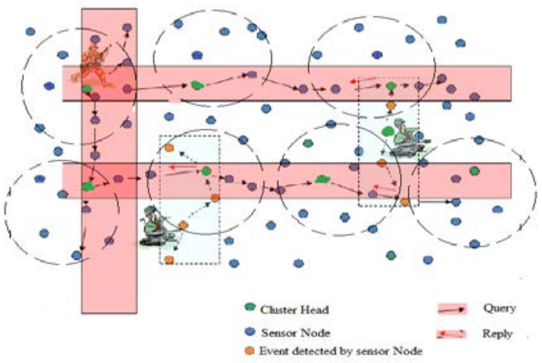


Figure 3. Proposed Cluster based Comb- Needle model with Cluster Heads

Table 1.Summarization of Our Works

Deployment Method	Basic CNM	Cluster-based CNM
Regular Network (Grid Deployment)	Combs, Needles, Haystacks: Balancing Push and Pull for Discovery in Large-Scale Sensor Networks [32]	Cluster-based Comb-Needle Model for Energy-efficient Data Aggregation in Wireless Sensor Networks [33]. *(Our Published Work)*
Randomly deployed Network	Extended Comb Needle Model For Energy Efficient Data Aggregation In Random Wireless Sensor Networks [17] *(Our Published Work)*	Now Proposed work is explained in this paper

3.1 Network Model

ASSUMPTIONS:

The following are the assumptions in the network model used for simulation as well as analysis:

(1) Wireless sensor network consists of *N* stationary and location-aware (using GPS or some other localization method) sensor nodes deployed randomly in the square field region of size *m* X *n*.

(2) Base station is in top left corner. (Multiple base stations may be available in network, each soldier is considered as base station)

(3) All the sensor nodes have the equal transmission power.

(4) All communication links are assumed to be symmetric.

(5) There are no transmission errors.

(6) Sensor node turns as an aggregator, if the size of the data is bigger than the certain limit.

(7) Clustering is done using ISODATA [31] scheme.

3.2 Applying ISODATA Clustering Algorithm

Many variants of k-means algorithm are available in literature. One such variant is the well-known ISODATA (Iterative Self-Organizing Data Analysis Technique) algorithm [30]. The variation employed is, splitting and merging of the resulting clusters of the k-means algorithm. In other words, ISODATA algorithm is based on the k-means algorithm with additional heuristics that govern the splitting and/or merging of clusters. Using these heuristics, it is possible to obtain the optimal partition starting from any arbitrary initial partitions, provided proper threshold values are specified. Splitting is done if a cluster has variance exceeding a threshold value, while merging is performed when the distance between a pair of cluster centroids is less than another threshold value. ISODATA is used as a benchmark for all unsupervised classification algorithms.

The application of ISODATA clustering in the proposed concept is as follows:

All the sensor nodes are initialized in 2D plane in random network, and then ISODATA algorithm is applied. How ISODATA algorithm works in our proposed concept is as follows: ISODATA has assigned initial cluster vector and it will take the sensor nodes positions into consideration to make them into clusters. The next step classifies each node to the closest cluster. Further new cluster mean vectors are calculated based on all sensor nodes in one cluster. The above two steps are repeated until the variation between the iteration is small. The variation is computed by the change in mean cluster vector iteratively. Clusters are merged if the number of sensor nodes in a cluster is less than a certain threshold value, or if the centroids of any two clusters are closer than a certain threshold. Clusters are split further into two different clusters if the cluster standard deviation exceeds another predefined value.

ISODATA ALGORITHM:

```
Input:  $N_C$: Initial number of clusters, M: Final (desired) number of clusters, CT: Convergence
threshold,
            $K$: No of clusters required
Output:  $M$ number of clusters along with their centroids.

  begin
            1. Select $N_C$ (< $M$) initial cluster centroids either arbitrarily or using some criterion;
            2. while (stopping criteria not satisfied)
                        2.1. repeat /* k-means Algorithm */
                                    Assign each pattern to the closest cluster centroid;
                                    Re-compute the cluster centroids using the current memberships.;
                              until (clustering converges) /* Convergence rate < CT */
                        2.2. Choose the clusters eligible for split and/or merge;
                        2.3. Update the number of clusters $N_C$ ;
                         2.4. Determine the current centroids.
  End
```

4 Analytical Evaluation

4.1 Analysis Of Comb Needle Model

It is considered that any node in the random networks can produce any event.

The following important performance metrics are determined as:

f_q = Query frequency

f_e = Event frequency

$f_d = \frac{f_e}{n^2}$ events occurs frequency in the sensor node

However, in our proposed mechanism, overall communication cost may be based on the broadcast or unicast, which utilized in the random networks. Here, we assume unicast for the analysis in the Extended Comb Needle Model. The cost of the developing the single comb needle for the length l is $l-1$.

We consider that frequency of Query f_q, The frequency of data event f_e is termed as ${}^{f_e}\!/_{f_q}$, which means that number of events produced for per query in a comb needle is $l-1(f_e/f_q)$. As $C_l = l-1$, then it would be modified and given as event produced for needle:

$$= C_l(f_e/f_q)$$

Complete Comb Needle Model analysis is given in our previous work [33].

4.2 Cluster Based Comb Needle Model for Random Networks

We consider the random network with *N* nodes located in plane at (x, y), where sensor node range is specified as 0<=*x*; *y*<*n*. The deployment area starts at (x, y) and the boundary is given as (x_n, y_m). Here, it is assumed that sensor nodes are uniformly distributed in the network.

We apply ISODATA [30] algorithm on randomly deployed sensor network, it will divide the sensor field into clusters called *i*. On top of the cluster region a CNM is applied.

The mathematical analysis for the proposed concept is as follows:

When a query is generated then the comb structure is formed in the network as shown in Figure 6. Let's assume that query node is located at (x, y). If the query is sent through the vertical direction from (x, y) to (x, y_m) and (x,0). Then the query is distributed at the horizontal lines from nodes (*x*,*y*+*s*),(*x*,*y*+*2s*) to (x_n,*y*+*s*), (x_n,*y*+*2s*). In this mechanism, *s* is used as combing degree or inter spike spacing. The resulting routing structure looks like a comb.

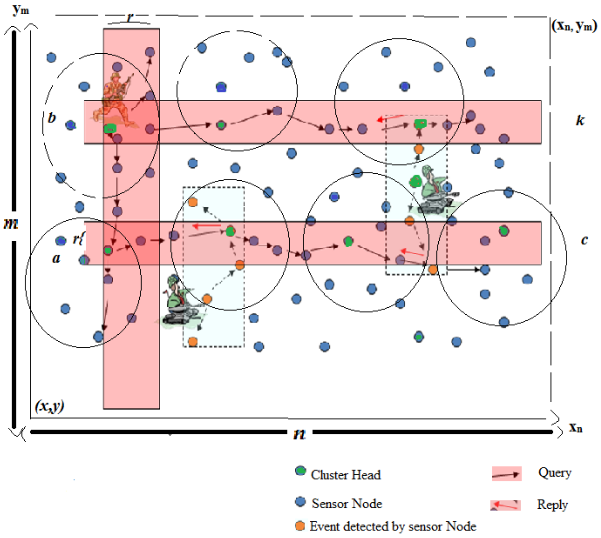


Figure 4. Definition of Comb base and spike for Extended Comb Needle Model

Let us assume that theoretical analysis of the random networks is given below:

$$(x,y+s) = a \tag{1}$$
$$(x,y+2s) = b \tag{2}$$
$$(x_n,y+s) = c \tag{3}$$
$$(x_n,y+2s) = k \tag{4}$$

From the equation (1) to (3) and (2) to (4) where the horizontal lines are formed, (x, y) to $(x,0)$ and (x,y) to (x,y_m) vertical lines are formed. While estimating the distance from the plane s.

$$s = (y_m\text{-}y_0)/3 \tag{5}$$

For illustrating the query response in horizontal direction $(x,y+s)$ and $(x,y+2s)$ are points generated for the horizontal response. Thus the push based query performance is operated while it is performing in the horizontal direction in the Figure 4. The comb structure has been developed. Then we need to specify the range of the comb needle model in the random network by using the following criteria, where r represents the range of the comb base and spike.

When the range is established for the random networks, it is demonstrated in the following equations

$$\text{Vertical range: } (x+r,y) \text{ to } (x+r,y_m)$$

Based on equation (1) and (3) horizontal range for spike *a* to *c* is

$$(a+\frac{r}{2},a-\frac{r}{2}) \text{ to } (c+\frac{r}{2},c-\frac{r}{2}) \tag{6}$$

Based on equation (2) and (4) horizontal range for spike *b* to *k* is

$$(b+\frac{r}{2},b-\frac{r}{2}) \text{ to } (d+\frac{r}{2},d-\frac{r}{2}) \tag{7}$$

The sensor nodes would pass the query depending on the Euclidean distance, which is used to consider the shortest path. The Euclidean distance is represented in the following equation:

$$\xi_{dist} = ((p,q)(u,v) = \sqrt{(p-u)^2 + (q-v)^2} \tag{8}$$

For example, consider the scenario as shown in Figure 5. e, f, and g are neighboring nodes on the spike. As per Euclidian Distance link is established in between *e* and *f*.

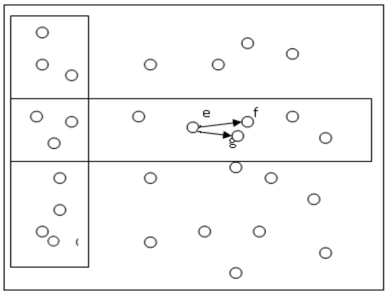


Figure 5. Establishing communication link in between neighbors

4.3 Analysis of Communication Cost

For analyzing the communication cost in both Grid (Regular) and random networks, the following scenario is considered:

Comb is assumed to be at the extreme left and needle at the extreme right. See Figure 6.

Case 1: Grid Network:
Number of hops for event notification = n hops as shown in Figure 7.

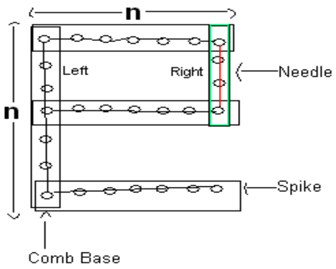


Figure 6. Comb and Needle in Grid Network

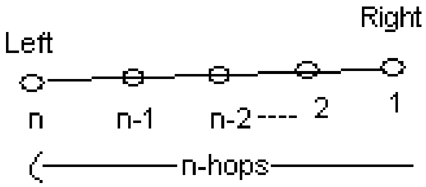


Figure 7. Communication using n hops in Grid Case

Case 2: Random Network:

Communication overhead depends on the way the nodes take their position at the time of random deployment as shown in Figure 2.

Best Case:

Nodes between two ends, Left and Right, take position as shown in Figure 7.

Number of hops required for event notification = n;

Increase in hops compared to Case1 (Grid network) = 0.

Worst Case:

In the worst case nodes take their position as shown in Figure 8

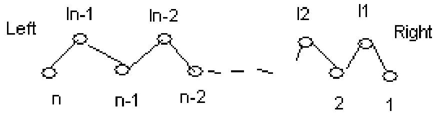


Figure 8. Communication in Random Network

Number of hops required for Event Notification = n+(n-1); (9)

Increase in hops compared to Regular deployment = (n-1); (10)

To calculate the Number of hops required for Event Notification in the average case, we consider the results of both the best and worst cases.

Therefore Increase in Number of hops for Event Notification in average case = 0+(n-1)/2

= (n-1)/2 (11)

This means that the communication overhead increases by 50% in case of random deployment.

When compared to regular deployment (Grid networks).

As per the reference [32] for CNM based grid networks Communication Cost Coptimal is

Coptimal = O(√n) (12)

When clustering is implemented in CNM based grid network [33]

Coptimal=O(√n/Nc) (13)

Since *Nc* is number of clusters

When CNM based random network is considered the Coptimal is *O (n)* (14)

When clustering is implemented in CNM based random network the Coptimal is as follows

Coptimal=O(n/Nc) (15)

5 Experimental Analysis

Experiment is conducted with the following simulation parameters given in Table 2. The performance of the Extended CNM with clustering is compared with Extended CNM without clustering.

5.1 Simulation Parameters

Simulation of the WSN with 50 nodes deployed randomly in an area of 20x10 square units is carried out using NS2. It is assumed that the wireless sensor nodes are distributed uniformly and independently. The MAC protocol is used is IEEE 802.11, number of nodes are 50 to 70. The radio propagation model is two ray ground reflection model.

NS2 has implemented three different propagation models (PM) to simulate the wireless channel: they are Free space model, Two-ray ground model and Shadowing model. Generally the propagation models are used to compute the received power. PM determines the attenuation between transmitter and receiver and computes received signal strength, when a packet is received. In Free space model, it assumes ideal propagation conditions and a single line-of-sight path between the transmitter and receiver. In two-ray ground reflection model, it considers both the ground reflection path and a direct path. In this model, both transmitter and receiver node are assumed to be in line-of-sight path. This model is more accurate in case of long distance line-of- sight path. Both the Free-space model and the two-ray model expect the received power as a deterministic function of the distance between the receiver and transmitter. The shadowing model will do deterministic path loss that predicts the received power from the distance between the receiver and transmitter nodes. The detailed information about NS2 propagation models can be found in the NS2 manual [35].

Table 2. Salient simulation parameters

Parameter	Value
Mac protocol	802.11
Number of nodes	50 to 70
Node deployment	Random
Radio propagation model	Two ray ground
Radio transmission range	200 m

5.2 Performance Metrics

The following metrics are used for evaluating the performance of proposed concept, which are defined as follows [17]:

a) Packet Delivery Ratio (PDR): It is determined as the ratio of overall packets received to the overall packets sent.

b) Throughput: It is determined as rate of successful message delivered over a communication channel in the random networks.

c) Average Delay: It means time difference between packets sent and packets received.

d) Energy consumption: It is determined as the average energy consumed on idle sleep, data processing, sensing, and data transmission.

e) Communication cost: It is determined as the number of packets transmitted and received for query and event notification.

5.3 Results And Discussion

The performance metrics are utilized to validate the proposed Cluster based CNM in random networks. The obtained results are demonstrated in [Figures 9 to 18]. From the obtained simulation results, it is clear that Cluster Based CNM in random network is significantly better than Extended CNM in simple random network.

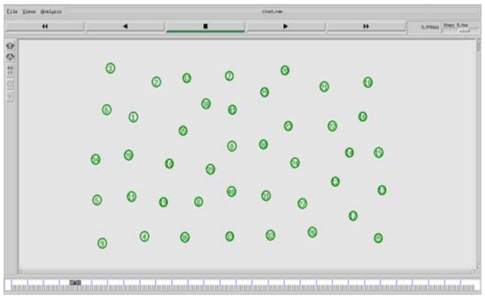


Figure 9. Simple Random Network

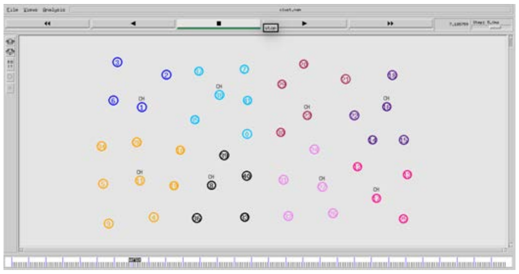


Figure 10. Clusters in Random Network

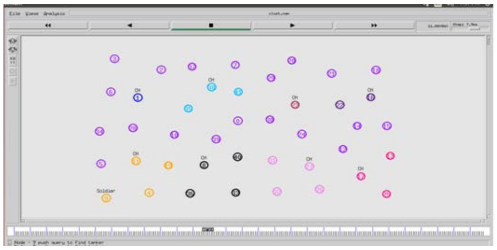


Figure 11. Cluster based Comb Needle Model (when query generated)

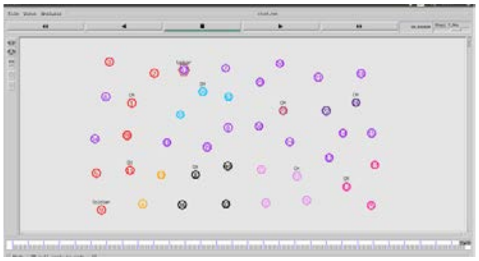


Figure 12. Cluster based Comb Needle Model With Needle (when Event found)

Figure 9 represents the network topology of the random network. The cluster network topology of the Cluster based CNM in the random network is demonstrated in Figure 10. Whereas Figure 11 shows the Comb structure in which base station sends the query in vertical fashion called comb base and horizontal spikes are formed for query forwarding in order to process information efficiently with minimum energy consumption. The result of query is shown in Figure 12 (i.e., when query received by node it sends event information to Cluster Head, Cluster Head aggregates data and sends back to soldier via the same path that is called Needle).

Hence, the simulation results are compared between the Cluster based CNM and Extended CNM in the random network. It is well understood from the obtained results graph that Cluster based CNM got higher performance than Extended CNM.

The performance analyzed in terms of communication cost, energy consumption, packet delivery ratio, packet loss, delay and throughput. They are represented in [Figures 13 to 18].

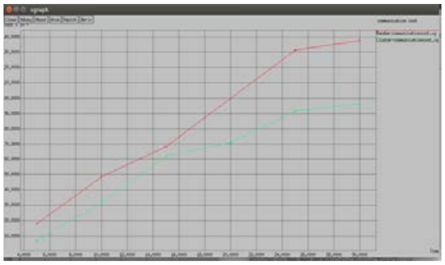


Figure 13. Communication Cost
*Red line indicates Extended CNM in random network. *Green line indicates Cluster based CNM

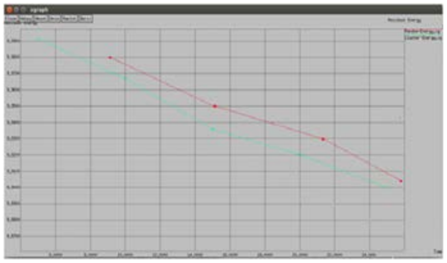


Figure 14. Energy Consumption
*Red line indicates Extended CNM in random network. *Green line indicates Cluster based CNM

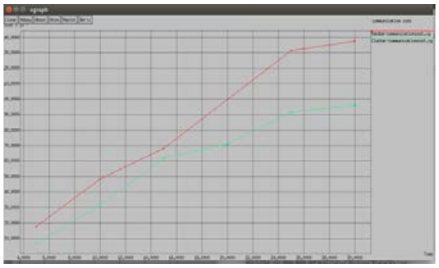


Figure 15. Packet Delivery Ratio
*Red line indicates Extended CNM in random network. *Green line indicates Cluster based CNM

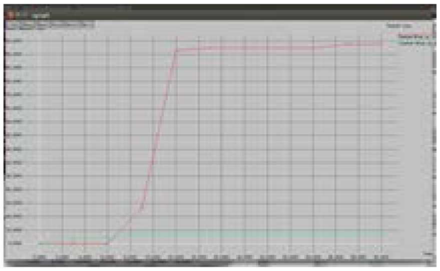


Figure 16. Packet Loss
*Red line indicates Extended CNM in random network. *Green line indicates Cluster based CNM

The graphs [Figures19 to 21] shows that efficiency of Cluster based Comb Needle Model in random networks and Extended Comb Needle Model in random networks

- Communication cost in Cluster based Comb Needle Model for Random Network is 30 % and in Extended Comb Needle Model for Random Networks is 58%. So 28% Communication Cost is decreased in our proposed model.

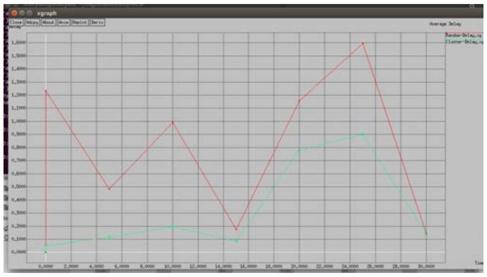


Figure 17. Delay
*Red line indicates Extended CNM in random network. *Green line indicates Cluster based CNM

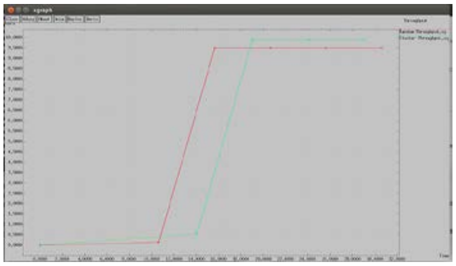


Figure 18. Throughput
*Red line indicates Extended CNM in random network. *Green line indicates Cluster based CNM

Average Energy Consumption in Cluster based Comb Needle Model for Random Network is 25 % and in Extended Comb Needle Model for Random Network is 41%. So 16 % energy is saved in our proposed model.

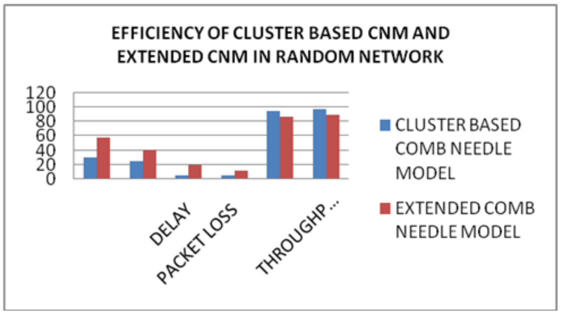


Figure 19. Efficiency of Cluster based CNM and Extended CNM in Simple Random Network

Delay in Cluster based Comb Needle Model for Random Network is 5 % and in Extended Comb Needle Model for Random Network is 20%. So 15% delay is reduced in our proposed model.

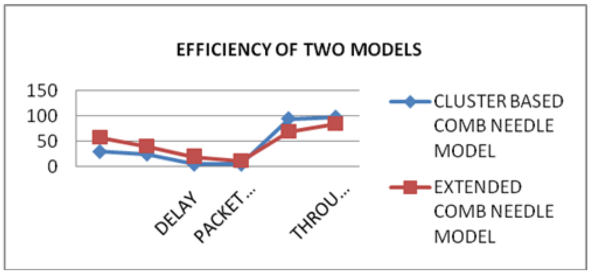


Figure 20. Efficiency of Two models

- Packet Loss is 5% in Cluster based Comb Needle Model for Random Network where as 12% in Extended Comb Needle Model for Random Network. So 7% is reduced in our proposed model.

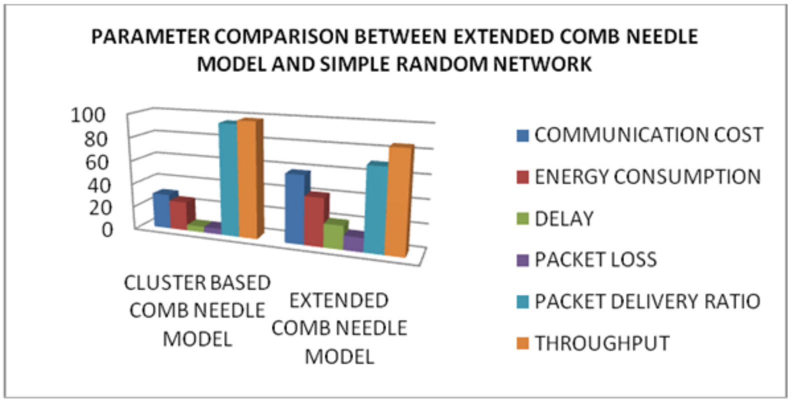


Figure 21. Parameter comparison between Cluster based CNM and Extended CNM in Simple Random Network

- Packet Delivery Ratio is 95% in Cluster based Comb Needle Model and 87% in Extended Comb Needle Model for Random Network. 8% is improved in our proposed model.
- Throughput is 98% in Cluster based Comb Needle Model and 90% in Extended Comb Needle Model for Random Network. 8% is improved in our proposed model.

6 Conclusion

At present, Wireless Sensor Networks have attracted much attention. An increasing list of military and civilian applications can employ WSN for increased effectiveness; especially in remote areas. For example Border protection, combat field surveillance and disaster management etc. These applications require good architecture and energy efficient data gathering and aggregation mechanism. We designed the Cluster based Comb Needle Model for Random WSN, by using two things clustering algorithm and comb needle model. All together it is Cluster based Comb Needle Model for Random sensor network. We analyzed the performance by using different parameters. They are Packet Delivery Ratio, Delay, throughput, Packet loss, Communication Cost, and Energy Consumption. Then we compared the proposed model with the Extended Comb Needle Model for random network. We observed that the Cluster based Comb Needle Model in Random networks is providing better results when we compare with a Extended Comb Needle Model in Simple Random Networks. It is well suited for military applications. Further our proposed model can be enhanced by applying compression techniques.

REFERENCES

[1] M. Cardei, J. Wu, M. Lu, M. Pervaiz. (2005). Maximum network lifetime in wireless sensor networks with adjustable sensing ranges, IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005 (WiMob'2005), vol. 3, IEEE, pp. 438–445.

[2] R. Subramanian, F. Fekri. (2006). Sleep scheduling and lifetime maximization in sensor networks: fundamental limits and optimal solutions, in: Proceedings of the 5th International Conference on Information Processing in Sensor Networks, ACM, pp. 218–225.

[3] M. Safar, H. Al-Hamadi, D. Ebrahimi, Peca. (2011): power efficient clustering algorithm for wireless sensor networks, Int. J. Inform. Technol. Web Eng. (IJITWE) 6 (1) 49–58.

[4] Ameer Ahmed Abbasi, Mohamed Younis (2007) '' A survey on clustering algorithms for wireless sensor networks'', Computer Communications 30 (2007) 2826-2841.

[5] A. Camillò, M. Nati, C. Petrioli, M. Rossi, M. Zorzi. (2013). IRIS: integrated data gathering and interest dissemination system for wireless sensor networks, Ad Hoc Netw. 11 (2) (2013) 654–671.

[6] E. Candes, M. Wakin. (2008). An introduction to compressive sampling, IEEE Signal Process. Mag. 25 (2) 21–30.

[7] V. Kawadia, P.R. Kumar, (2003). Power control and clustering in Ad Hoc networks, in: Proceedings of IEEE INFOCOM, San Francisco, CA.

[8] M. Chatterjee, S.K. Das, D. Turgut, (2002). WCA: a Weighted Clustering Algorithm for mobile Ad Hoc networks, Cluster Computing 5 (2) 193–204.

[9] A.D. Amis, R. Prakash, T.H.P. Vuong, D.T. Huynh, Max-Min D (2000). cluster formation in wireless Ad Hoc networks, in: Proceedings of IEEE INFOCOM.

[10] A.B. McDonald, T. Znati, (1999). A mobility based framework for adaptive clustering in wireless ad-hoc networks, IEEE Journal on Selected Areas in Communications 17 (8) 1466–1487.

[11] S. Basagni, (1999).Distributed clustering algorithm for ad-hoc networks, in: Proceedings of the International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN), Fremantle, Australia.

[12] G. Gupta, M. Younis, (2003). Load-balanced clustering in wireless sensor networks, in: Proceedings of the International Conference on Communication (ICC 2003), Anchorage, Alaska,.

[13] S. Bandyopadhyay, E. Coyle, (2003). An energy efficient hierarchical clustering algorithm for wireless sensor networks, in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, California, April

[14] S. Ghiasi, A. Srivastava, X. Yang, M. Sarrafzadeh, (2004). Optimal energy aware clustering in sensor networks, Sensors Magazine MDPI 1 (1) 258–269.

[15] O. Younis, S. Fahmy, (2004). HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks, IEEE Transactions on Mobile Computing 3 (4) 366–379.

[16] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, (2002). Application specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Networking.

[17] M. Shanmuki, O.B.V. Ramanaiah. (2016). "Extended Comb Needle Model For Energy Efficient Data Aggregation In Random Wireless Sensor Networks" Indian Journal of Science and Technology, Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/89953, June 2016

[18] S. Lee, S.H. Lee. (2010). Analysis of network lifetime in cluster-based sensor networks, IEEE Commun. Lett. 14 (10) 900–902.

[19] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, J. Crowcroft. (2008). in the air: practical wireless network coding, IEEE Trans. Network. 16 497–510.

[20] J. Haupt, W. Bajwa, M. Rabbat, R. Nowak. (2008). Compressed sensing for networked data, IEEE Signal Process. Mag. 25 (2) 92–101.

[21] O.M. Al-Kofahi, A.E. Kamal. (2009). Network coding-based protection of many-to-one wireless flows, IEEE J. Sel. Areas Commun. 27 (5) 797–813.

[22] W. Heinzelman, A. Chandrakasan, H. Balakrishnan. (2002). An application specific protocol architecture for wireless microsensor networks, IEEE Trans. Wirel. Commun. 1 (4) 660–670.

[23] C. Luo, J. Sun, F. Wu, C.W. Chen. (2009). Compressive data gathering for large-scale wireless sensor networks, in: Proc. ACM Mobicomn++09, pp. 145–156.

[24] J. Luo, L. Xiang, C. Rosenberg. (2010). Does compressed sensing improve the throughput of wireless sensor networks? in: ICC'10, 2010, pp. 1–6.

[25] W. Wang, M. Garofalakis, K. Ramchandran. (2014). Distributed sparse random projections for refinable approximation, in: 6th International Symposium on Information Processing in Sensor Networks, pp. 331–339.

[26] G. Cao, F. Yu, B. Zhang. (2014). Improving network lifetime for wireless sensor network using compressive sensing, in: 2014 IEEE 15th International Conference on High Performance Computing and Communications (HPCC), IEEE, pp. 448–454.

[27] L. Xiang, J. Luo, A. Vasilakos. (2014). Compressed data aggregation for energy efficient wireless sensor networks, in: 2014 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), IEEE, pp. 46–54.

[28] O.M. Al-Kofahi, A.E. Kamal. (2009). Network coding-based protection of many-to-one wireless flows, IEEE J. Sel. Areas Commun. 27 (5) 797–813.

[29] McQueen, J., "Some Methods for Classification and Analysis of Multivariate Observations", Proc. of 5th Berkeley Symp. on Mathematical Statistics and Probability, pp. 281-297, 1967.

[30] Ball, G.H., Hall, D.J., “ISODATA: A Novel Method of Data Analysis and Classification”, Technical Report, Stanford University, Stanford, CA, 1965.

[31] O.B.V. Ramanaiah, Hrushikesha Mohanty, “Adapting a Distributed Data Clustering Algorithm for Mobile Environment”, Proc. of Int’l Conf. on Information Technology (CIT ’01), pp. 72-80, December 2001.

[32] X. Liu, Q. Huang, and Y. Zhang,(2004). Combs, Needles, Haystacks:Balancing Push and Pull for Discovery in Large- Scale Sensor Networks, Proc. ACM Conf. Embedded Networked Sensor Systems (SenSys ’04), Nov. 2004.

[33] M. Shanmuki, O.B.V. Ramanaiah. (2015). Cluster-based Comb-Needle Model for Energy-efficient Data Aggregation in Wireless Sensor Networks, Applications and Innovations in Mobile Computing (AIMoC). 978-1-4799-1848-5/15/ ©2015 IEEE.

[34] M. Shanmuki, O.B.V. Ramanaiah. (2016). A Survey On Energy Efficient Data Aggregation Protocols For Wireless Sensor Networks’’ International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 10 (2016) pp 6990-7002.

[35] Website http://www.isi.edu/nsnam/ns/doc/node215.html

Society for Science and Education
United Kingdom

TNC Transactions on
Networks and Communications

Volume 4, Issue 5
ISSN: 2054 -7420

Performance Evaluation of Low Density Parity Check (LDPC) Codes over Gigabit Ethernet Protocol

Vinaya R. Gad, Udaysingh V. Rane, Rajendra S. Gad and Gourish M. Naik
Altera System on Chip Laboratory; Department of Electronics, Goa University Goa, India 403206;
rsgad@unigoa.ac.in

ABSTRACT

Error Correcting Low density Parity Check codes enable the communication systems to have a low-power, reliable transmission over noisy channels and can achieve data rates very close to Shannon limit when iteratively decoded. They are used in many digital communication systems such as digital video broadcasting (DVB-S2), MIMO-WLAN (802.11n), WMAN (802.16e), mobile broadband wireless access (MBW A) (802.20) and have a very good error correcting performance over a variety of channels. In this paper we present a performance platform for simulation studies of of LDPC decoding algorithms. We present the results of the simulation studies of Bit Error Rate (BER) performance for various block length like 64 and 256 bytes frame over Additive White Gaussian Noise (AWGN) channel. The comparative studies are made for Log Domain and Log Doman Simple decoding algorithms.

Keywords: LDPC, BER, PER, FPGA, Gigabit Ethernet.

1 Introduction

There is a growing literature on the practical design of LDPC codes [1]. To give few examples of ¼ code rate like irregular LDPC code over GF(8), blocklength 48 000 bits (Davey, 1999); turbo code (JPL, 1996) blocklength 65 536; Regular LDPC over GF(16), blocklength 24 448 bits (Davey and MacKay, 1998); irregular binary LDPC code, blocklength 16 000 bits (Davey, 1999); Luby et al. (1998) irregular binary LDPC code, blocklength 64 000 bits; Turbo code for Galileo; Regular binary LDPC code: blocklength 40 000 bits (MacKay, 1999b); they are now being adopted for applications from hard drives to satellite communications and quantum error-correction (MacKay, 2004). Although the primary goal of any error correcting code is to achieve a performance that is close to the Shannon limit, one has to realized themselves to practical implementations for limited resources on the computing machine, latency of the operating systems, Complex Instructions Set Computing (CISC) instructions types on computing cores and processing time; all by limiting the iterations involved in complex algorithms so they can be integrated into real systems. Error correction algorithms are often implemented in hardware for fast processing to meet the real-time needs of communication systems.

DOI: 10.14738/tnc.45.2035
Publication Date: 02nd October 2016
URL: http://dx.doi.org/10.14738/tnc.45.2035

2 LDPC decoding algorithms: Sum-Product Algorithm – Probability Domain and Log Domain

The direct implementation of the decoding algorithm for binary codes in the probability domain (i.e., the SPA) has several drawbacks as compared to an implementation. SPA used in decoding of LDPC codes requires a large number of multiplications of probabilities which makes the algorithm numerically unstable, especially for very long codes. It may be noted that the best performance is obtained for very long codes. This long block length, combines with the need for iterative decoding, introduces latency which is unacceptable in many applications. Thus, a log-domain version of the algorithm is preferred, denoted here by log-SPA, based on log-likelihood ratios (LLR): the direct implementation is more sensitive to quantization effects and requires more quantization levels than when using LLRs [2,3].

We define the following log likelihood ratios as part of the decoding algorithmWe define the following log likelihood ratios as part of the decoding algorithm: $Lc_i = \log\left(\left(P_r(x_i = +1 \mid y_i)\right)/\left(P_r(x_i = -1 \mid y_i)\right)\right)$; $Lr_{ji} = \log(r_{ji}(0)/r_{ji}(1))$; $Lq_{ji} = \log(q_{ji}(0)/q_{ji}(1))$; $LQ_i = \log(Q_i(0)/Q_i(1))$. This algorithm iterates over columns and rows of parity check matrix and operates on nonzero entries by performing the following steps:

Step 0: Initialize Lq_{ji} by: $Lq_{ji} = Lc_i = 2y_i/\sigma^2$;Which initialized the values of coefficients $Q(x)_{ij}$ over logarithmic scale for the received symbols 'y_i' obtained after hard-decision decoder of the received decoded vector having 'σ' as standard deviation of the noise over the channel.

Step1: Evaluate Lr_{ji} by:

$$Lr_{ji} = \left(\prod_{i'\varepsilon R_{j\backslash i}} \alpha_{ji'}\right).\phi\left(\sum_{i'\varepsilon R_{j\backslash i}} \phi(\beta_{ji'})\right) \quad ; \qquad (1)$$

where, $\alpha_{ji} = sign(Lq_{ji})$, $\beta_{ji} = \left\|Lq_{ji}\right\|$, $\phi(x) = -\log(\tanh(x/2)) = \log\left(e^x + 1/e^x - 1\right)$.

Step2:

$$Lq_{ji} = Lc_i + \sum_{j'\varepsilon C_i\backslash j} Lr_{j'i} \quad .$$

Step 3:

$$LQ_i = Lc_i + \sum_{j\varepsilon C_i} Lr_{ji} \quad . \qquad (2)$$

Step 4: For every row index i:

$$\hat{c}_i = \begin{cases} 1 & if\ LQ_i < 0 \\ 0 & else \end{cases} . \qquad (3)$$

If $\hat{c}H^T=0$, or if maximum number of iteration is reached then stop, else continue iterations from Step 1. The SPA requires message multiplications, whereas the log-SPA implementation uses message additions. The latter is more efficient in fixed point implementations, as fixed point multiplications can take up many clock cycles compared to additions.

2.1 Min-Sum Algorithm

Consider the update equation 1 for '***Lr***' in the log domain algorithm:

$$Lr_{ji} = \left(\prod_{i'\varepsilon R_{j\backslash i}} \alpha_{ji'}\right).\phi\left(\sum_{i'\varepsilon R_{j\backslash i}} \phi(\beta_{ji'})\right) \qquad (4)$$

The 'ϕ(x)' is a function which is decreasing for the values of x > 0. It is intuitive that the term corresponding to the smallest β_{ji} in the above summation dominates, so that the second term in above equation: $\phi\left(\sum_{i'\varepsilon R_{j\setminus i}} \phi(\beta_{ji'})\right) = \phi(\phi(\min_{i'} \beta_{ji'})) = \min_{i'} \beta_{ji'}$. The second equality follows from $\phi(\phi(x)) = x$. Thus the Min-Sum algorithm is the same as SPA in which Step(1) is replaced by this equation: Step 1': $Lr_{ji} = (\prod_{i'\varepsilon R_{j\setminus i}} \alpha_{ji'}).(\min_{i'\varepsilon R_{j\setminus i}} \beta_{ji'})$. Because of the approximation in this equation, there is degradation in the performance of Min-Sum compared to SPA.

3 Simulation platform relevance in Optimizing ECC's

The Simulation platform comprises of the platform design for Gigabit Ethernet protocol, which is interfaced with the Matlab(Version 7.0) simulation model for BER performance analysis.

3.1 Platform Design

The platform for Gigabit Ethernet protocol is implemented using Altera's Triple Speed Ethernet (TSE) softcore IP Megacore function [4]. The design has been implemented on Altera's Stratix II GX PCI Express development board and the device used is 'EP2SGX90FF1508C3'. The said device is a Field Programmable Gate Array (FPGA) with '90960' Configurable Logic Blocks (CLBS), 717 MHz of maximum clock frequency, PBGA1508 package with Combinatorial Delay of a CLB-Max of 4.45 ns. The Fig. 1 shows the simplified block diagram of the Gigabit Ethernet protocol platform.

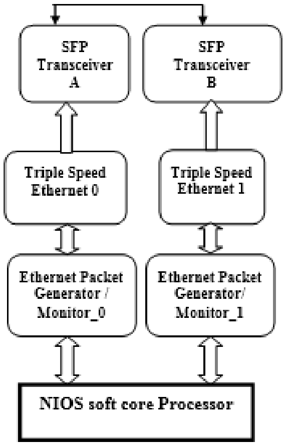


Figure. 1: Block Diagram of the Gigabit Ethernet protocol platform

The design includes two Altera TSE MegaCore functions, which implement the MAC, Physical Coding Sublayer (PCS) and Physical Media Attachment (PMA) sublayer in Full Duplex mode. There are two SFP (Small Form-factor pluggable) modules cages built onto the FPGA board, which provide the physical media interface. The Nios II processor is used to generate and monitor the Ethernet packets. The TSE MegaCore function handles the transmission and reception of the packets, which can be looped back using SFP modules with an Ethernet copper cable, fibre optic cable, or a switch using proper physical medias SFP. The design is built using Altera's Quartus II software and System On Programmable Chip (SOPC) builder. The design uses, on-chip memory of 256 Kbytes and the SOPC builder system uses a clock source of 83.33MHz. Altera's TSE design has been implemented and used as a platform for studying the performance of Gigabit Ethernet protocol Standards 1000Base-LX, 1000Base-SX and 1000Base-T.

There are three main components of the experimental setup as shown in Fig. 2(a). I. Stratix II GX PCI Express development board having device 'EP2SGX90FF1508C3': This is the platform for the Gigabit Ethernet protocol design wherein the algorithms are synthesized. II. SFP transceivers cages on the Stratix II GX FPGA: For interfacing different types of physical media of Ethernet like Cat5e, Cat6, Single mode fibre and Multi-mode fibre using SFP Transceivers. III. Fibre mounting and positioning three axis linear stages stand: Platform for mounting the fibre and introducing calculated optical attenuation in channel by lateral, longitudinal displacements of fibre joints. Now errors are introduced in the fibre channel by longitudinal displacement using the adjustment screw along the x-axis of the fibre mounting and positioning stand. The graph in Fig. 2(b) illustrates the packet loss introduced in the fibre with longitudinal displacement, which is equivalent to AWGN channel in the experimental setup. This confirms the Ethernet frame generator system development on configurable devices ready to be used for ECC platforms explain in next section. Figure 3 shows a MATLAB model developed to study the BER performance of Gigabit Ethernet protocol using LDPC codes. This model can be used for error correction performance analysis of Gigabit Ethernet protocol.

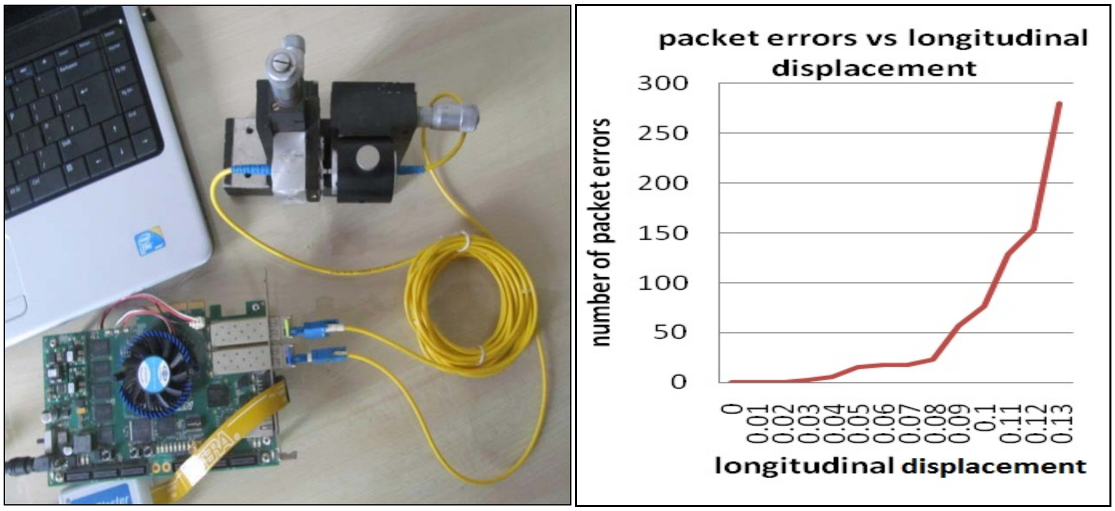


Figure 2: (a) Experimental Setup; (b): Packet errors vs longitudinal displacement.

The Ethernet frame is generated using ALTERA TSE IP core generator as shown in Fig. 1 and these frames are captured using WireShark and given to the Matlab simulation model of error correction shown in Fig. 3. The frames are encoded using the generator matrix. The BPSK modulator scheme maps the input binary signals, to an analog signal for transmission. The AWGN channel is the medium through which information is transmitted from the transmitter to the receiver for introducing errors in transmitted frames. The AWGN channel is representing the noisy physical media like a copper, fibre optic or wireless channel. The LDPC decoder is implemented at the receiver. Here, two decoding algorithms used i.e. Sum Product Algorithm (SPA)-logdomain and SPA-Min-Sum Algorithm, which loops through passing messages back and forth along the tanner graph until maximum number of passes have occurred. The estimated message is compared to the transmitted message at the receiver end in order to detect whether there was an error in transmission.

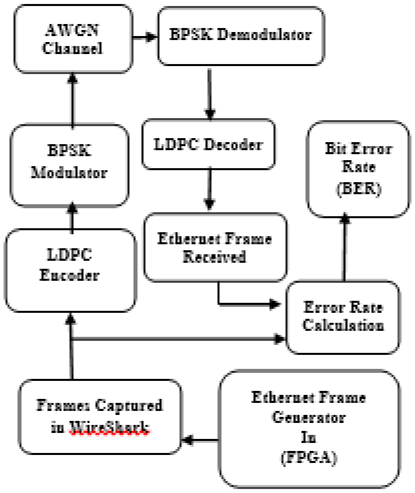
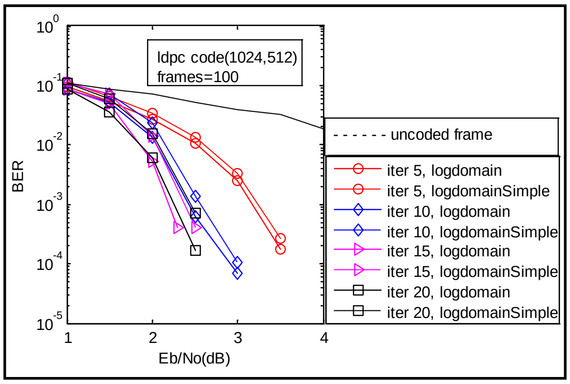


Figure 3: Simulation model for Error Correction interfaced with Triple Speed Ethernet design.

4 Results and Discussions

The LDPC decoding algorithms which are efficient for hardware implementation i.e. Sum Product Algorithm (SPA)-logdomain and SPA-Min Sum Algorithm (logdomainSimple) are chosen for simulation studies. The IBM X3200 server having one Intel quad-core (Xeon 3400 series) with 32 KB instruction cache, 32 KB data cache, and up to 8 MB L3 cache shared among the cores and support for Intel Extended Memory 64 Technology (EM64T) with 1333 MHz 32GB SDRAM DIMM has been set as a computing machine for model computation. The performance studies (Figures 4 and 5) of LDPC codes were computed for 100 numbers of Ethernet Frames having block length of 512 and 1024 bits corresponding to 64 and 256 bytes for number of iterations from 5 to 50 frame lengths respectively. The simulations were limited to lower value of frame lengths over higher iteration due to linear computation time. It may be noted that computation time for the block length of 512 (i.e. Figure 5.1. (a)) over 5-20 iterations was approximately 40 hours.

Results, as illustrated in Figure 4 to 5 indicate that the BER performance improves with increase in block length which can be optimized for error correction by setting the number of decoding iterations between 5 to 50 for a SNR close to 2dB. Since, more errors are introduced for larger frame lengths and hence the number of iterations needs to be increased for better Error Correction performance. It may be noted that for higher number of iterations 20 to 300 for block length of 512 bits corresponding to 64 bytes frame lengths there is no improvement in the error corrections, while obtaining performance of close to 10^{-3} BER at 2 SNR.



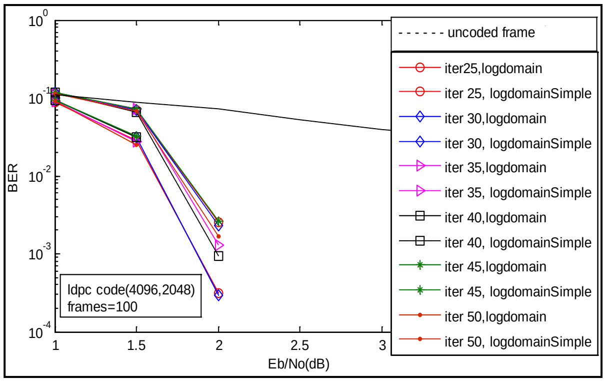


Figure. 4: BER vs SNR for 64 bytes frame over 5 – 20 iterations

Figure. 5: BER vs SNR for 256 bytes frame over 25 – 50 iterations

There are growing literatures on the practical design of LDPC codes; they are now being adopted for applications from hard drive to satellite communication. Khaled Shuaib et al, focuses on developing MatLab/Simulink models for the Zigbee protocol and the performance evaluation of these models. Several simulations were carried and the results were analyzed for the different scenarios. The results show how the relationship between the signal Bit Error Rate (BER) and Signal to Noise Ratio (SNR) was affected when varying the data rate and power [5]. David J. C. MacKay gives experimental results for binary-symmetric channels and Gaussian channels demonstrating the practical performance of LDPC codes is substantially better than that of standard convolutional and concatenated codes and is almost as close to the Shannon limit as that of turbo codes[6]. Murad Hossain et al presents a study of the errors observed when an optical Gigabit Ethernet link is subject to attenuation. They have introduced modified log-domain algorithm and min-sum algorithm of sum-product algorithm (SPA) for LDPC codes over GF (q) and compared the BER performance and computational complexity of the log domain algorithm, modified log-domain algorithm and modified min-sum algorithm. The BER performance of modified log domain decoding and modified min-sum decoding is better than log domain decoding algorithms [7]. Ganepola V. S. et al establish working in a higher order Galois field, significantly improve the performance of the LDPC code with moderate code lengths[8]. Hua Xiao et al proposed method for estimating the performance of low-density parity-check (LDPC) codes decoded by hard-decision iterative decoding algorithms on binary symmetric channels (BSCs) is proposed [8]. Chris Howland et al designed a 1024 bit rate 1/2 LDPC code decoder and implemented which matches the coding gains of equivalent turbo codes. This parallel decoder architecture supports throughputs upto 1 Gbps[9].

REFERENCES

[1] Yongyi Mao, Amir H. Banihashemi, Decoding Low-Density Parity-Check Codes With Probabilistic Scheduling, IEEE Communications Letters, 5(10)(2001).

[2] Bernhard, M. J. Leiner, LDPC Codes – a brief Tutorial , 2005.

[3] L. Ping , W. K. Leung, ‘Decoding low density parity check codes with finite quantization bits’; IEEE Comm. Letters, 4(2)(2000)62–64.

[4] S. Khatri, R. Brayton, A. Sangiovanni-Vincentelli, Cross-talk Immune VLSI Design Using a Network of PLAs Embedded in a Regular Layout Fabric', IEEE/ACM International Conference on Computer-aided Design, (2000) 412–418.

[5] K. Shuaib, M. Alnuaimi, M. Boulmalf, I. Jawhar, F. Sallabi, A. Lakas, Performance evaluation of IEEE 802. 15. 4: experimental and simulation results, Journal of Communications, 2(4)(2007) 29–37.

[6] D. MacKay, Good error correcting codes based on very sparse matrices, IEEE Trans. Information Theory,(1999)399-431.

[7] Md. Murad Hossain, Md. Rakibul Islam, Md.Jahidul Islam, Asif Ahmed, Md. Shakir Khan, S. M. Ferdous, Modified Log Domain Decoding Algorithm for LDPC Codes over GF(q), Journal of Selected Areas in Telecommunications (JSAT), (2011).

[8] Hua Xiao, Amir H. Banihashemi, Estimation of Bit and Frame Error Rates of Finite-Length Low-Density Parity-Check Codes on Binary Symmetric Channels, IEEE Transactions On Communications, 55(12)(2007).

[9] Chris Howland, Andrew Blanksby, A 220 mW 1Gb/s 1024-Bit Rate-1/2 Low Density Parity Check Code Decoder, IEEE 2001 Custom Integrated Circuit Conference;(2001), 0.7803-6591-7/01.

Society for Science and Education
United Kingdom

TNC Transactions on Networks and Communications

Volume 4, Issue 5
ISSN: 2054 -7420

Smart Metering for Intelligent Buildings

Natasa Zivic, Obaid Ur-Rehman and Christoph Ruland
Chair for Data Communications Systems, University of Siegen, Germany
natasa.zivic@uni-siegen.de, obaid.ur-rehman@uni-siegen.de, christoph.ruland@uni-siegen.de

ABSTRACT

Intelligent buildings are based on the use of smart metering devices. Smart metering provides instantaneous and accumulative metering information to the service providers on electricity, gas, water etc. This information is also given to the customers for the purpose of reduction of costs, energy consumption and emission of CO_2. The customers' saving of energy can be adapted dynamically using smart metering devices: this helps that the power generation and consumption are equally distributed in the smart grid. Liberalization of the metering market requires few strong security and privacy requirements for the metering data. Governmental organizations are responsible for the permanent correct delivery of metering data and are able to control and maintain the metering devices. The status of current smart metering progress in different countries is given in the paper with examples of successfully managed smart metering projects.

Keywords: Smart Metering, Smart Grids, Liberalization of Energy and Metering Market, Smart Meter Communications and Protocols, Security and Privacy, Smart Metering Projects.

1 Smart Metering Systems

1.1 Smart meter

A smart meter is a device installed at the consumer's premises (house or a facility) for measuring the consumption of commodities such as gas, water and electricity. The consumption of commodities can be measured in terms of volume or energy, e.g., gallons of water, cubic feet of gas or kilowatt hours of electricity. Smart meters are an advanced form of the traditional electromechanical devices with the ability to measure consumption of commodities in real-time and with the ability to communicate over one or more wired or wireless networks. They are equipped with digital displays for displaying the consumption of commodities and communication units for communication over a network. Nowadays, an energy importer / consumer can be an exporter / producer at the same time. The smart meters should therefore be capable to measure the amount of energy exported as well as imported.

1.2 Smart metering

The term smart metering is different from smart meters. Smart meter is a device that measures and possibly stores the consumption of a commodity. Smart metering, on the other hand, is referred to the whole infrastructure including smart meters, communication networks/infrastructure between the smart

DOI: 10.14738/tnc.45.2234
Publication Date: 10th October 2016
URL: http://dx.doi.org/10.14738/tnc.45.2234

meters and other concerned entities such as the energy consumer, the meter operator, the supplier of energy or the utility and the meter data management systems.

If smart metering is integrated in building management systems (BMS), automatic functions can be enabled or operators may be warned when peak use approaches critical price thresholds or system constraints. Data from smart meters (both real-time and near real-time) can be used to highlight anomalies, identify energy wasting equipment and may be used to offer improvements. They will not only be helpful for the end consumer to identify and remedy the sources of high energy consumption but also help the utility to identify the times of high energy demands and sources of energy wastage.

Smart metering should support:

- Acquisition, processing and communication of commodity consumption.
- Storage of consumption status and demand requirement over time.
- In house display for displaying the real-time consumption status. Such a display is normally in-room (not in the basement), and helps the consumer to monitor and control the energy consumption.
- Communication of the consumption measurements in real-time (or almost real-time) to the utility. This data is later used for billing and accounting.
- Bi-directional communication capability with the remote end such as the meter operator. This allows the meter operator to control the meter without physical visits to the consumer’s premises. This may also allow the download / update of software or firmware so that new services and protocols can be supported.
- Remote connection or disconnection of energy.
- Load limitation in case of high energy demand in peak hours.
- Scalability and interoperability, so that multiple vendors can be supported.
- Reduction of energy wastage and load control.
- Building load profiles and load schedules.
- Security and privacy of consumer data, e.g., using access control, confidentiality and authentication.

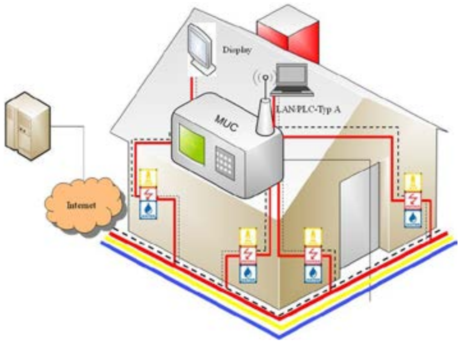


Figure 1. Multi Utility Communication (MUC) for measurements relay

1.3 Need for smart metering - load profiles and remote readout

A load profile is a plot of the variation in the energy demand versus time. The load profile is useful for power generation companies where it is required to know, in advance, how much energy will be required at a certain time period or over certain duration of time. Such information is extremely important to ensure the availability and reliability of power transmissions to meet the energy demands. The load profiles were traditionally maintained manually by measuring the energy consumption of customers on monthly basis, e.g., based on manual monthly meter readings. The energy suppliers' obligations are however settled on hourly or sub-hourly basis, whereas the demand may vary on hourly basis and the load profiles must be built with high probability of demand predictability in mind. Recently, with the introduction of modern electrical devices and due to the ever growing demands of energy, the load profiles need to be refined to a smaller interval in order for better delivery and availability of power supply. Load profiles can be split into categories on the basis of seasons, e.g., one profile for summer and another one for winter. Load profiles can also be refined up to the days of months, or for weekdays and weekends, holidays etc. One can even refine them to load profiles for hours in a day to predict the peak energy demand times.

Smart metering is a helpful tool, suitable in this situation. With their ability to remotely transmit the consumption in real-time, smart meters can help in building load profiles to fine grained intervals. Thus the need for manual monthly recordings of energy consumption is reduced to automated real-time demand gathering.

Smart metering also helps in reducing time and costs involved in visits to each and every customer's premises and to record the energy consumption status. This is now done via the ability of remote readout (either automatic or activated transmission of the consumption of the measurements).

1.4 Billing and accounting

Smart metering helps in improved and fine grained billing and is in fact the first application of smart metering. Traditionally, customer billing has been done on a monthly or yearly basis, based on one or two fixed tariff(s). With the availability of real-time (or almost real-time) consumption information, the billing can be improved and done on the basis of actual commodity consumption. Smart metering also makes the task of accounting more convenient by being able to store the commodity consumption over a period of time and with the ability to charge the customer as per actual consumption and on the basis of more flexible tariffs as compared to fixed monthly tariffs. This helps in the reduction of the billing conflicts between the consumer and the provider.

1.5 Customer awareness

With the increasing growth of the demand for energy, efforts on customer awareness need to be increased on the issues such as:

- The insufficient energy production capabilities
- Link of energy consumption to pollution and
- Threats to health in case of natural disasters from certain sources of energy

This is now possible due to smart metering and using the concept of smart billing. The consumer is empowered to actively participate in the demand response process. With the help of feedback and suggestions, the consumer is made aware of the actual consumption and by involving him in the process, the need for energy can be reduced. Governments have taken steps in this regard and the need for energy has been reduced by certain percentages around the world.

A thorough analysis of the impact of feedback and smart billing on the reduction of energy consumption is given in [5], where the authors used the following key performance indicators in their analysis:

- Improvement in the awareness of energy consumption
- Reduction of energy consumption
- Reduction in energy bills
- Aggregated impact on national energy consumption
- Cost effectiveness
- Impact on customer relationship

The case studies in [5] were conducted in the following countries or states,

- USA-California
- Republic of Ireland
- Sweden
- Australia-Victoria
- UAE-Abu Dhabi
- Chile
- South Africa
- PRC-Hong Kong

In conclusion to the case studies reviewed in the report [5], smart bills were declared as responsible for the reduction of household electricity consumption between 1.1% and 2.7%. The corresponding reduction of gas consumption was between 2.2% and 2.8%.

1.6 For whom is smart metering beneficial?

Smart metering is mutually beneficial for many stake holders. Some of the potential users of the smart metering data are listed in Table 1 along with the potential uses of the data gathered by smart metering systems.

Table 1. Need for smart metering data

Who is interested in smart metering data?	How could the data be used?
Utilities	• To monitor electricity usage and load • To be able to do accurate billing • Generation of load profiles
Electricity usage advisory companies	• To promote energy conservation • Customer awareness
Insurance companies	• To determine health care premiums based on unusual behaviors that might indicate illness
Marketing companies	• To profile customers for targeted advertisements • To find out suitable advertisement times
Law enforcing agencies	• To identify suspicious or illegal activities
Civil litigators	• To identify the property boundaries • To identify activities on premises
Landlords	• To verify lease compliance • To identify any unwanted activity
Private investigators	• To monitor energy consumers for specific activities

The press	• To get information about celebrities and other famous people • To report illegal activities
Creditors	• To determine behavior that might indicate creditworthiness
Criminals	• To identify the best times for a burglary • To identify expensive equipment / appliances to steal

2 Services of Smart Metering

2.1 Transparent energy usage

Smart Meters are envisaged to provide many services to the consumer as well as the utilities. First of all they provide the customer with the ability to measure their energy consumption. A customer is able to see the energy consumption in real time using a screen (In Home Display - IHD) installed at his or her premises. This gives the customer fine grained control over the resources he consumes and gives him the ability to save energy and stay inside his budget. This also gives the customer the ability to decide when to use most of the energy, e.g., choosing between day and night tariffs. The customer also has the ability to transparently switch from one utility to the other.

Smart Metering also come with new functionalities for the utilities. A utility can measure almost real time energy consumption of a certain customer or the aggregated energy consumption over a certain area. This enables the utility to offer different tariff schedules, e.g., one for the day time and another for the night time. The utility can also monitor the energy theft, e.g., by controlling how much energy goes in and how much is paid for in a certain area being monitored.

The utility also gets the ability to control the energy consumption in certain premises. In peak demand hours, the utility will have the ability to kill the unnecessary energy consumption by certain devices, e.g., a heater, when it should not be running after a certain temperature has been reached or the outside temperature has fallen down. Such a heater should have the ability to communicate with the utility through a Smart Meter.

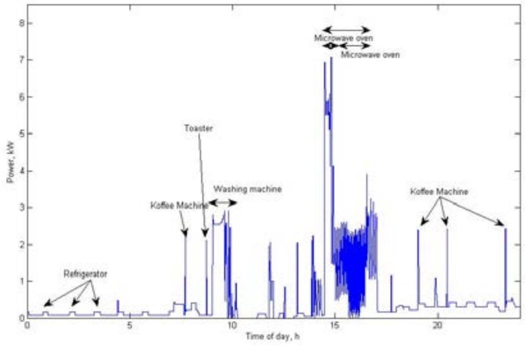


Figure 2. An example chart of energy consumption in a typical household, over a period of 24 hours

2.2 Advanced Smart Metering for Energy Saving

Energy efficiency has been a long-pursued goal spanning all fields of human activities. At first, these activities have not considered user involvement, focusing mainly on the technology efficiency (e.g., light bulbs). The interest in this topic has been produced by energy crisis and climate change. In this respect, the European Union has long been a driving force in international negotiations on climate. In 2007 EU leaders endorsed an integrated approach to climate and energy policy and committed to transforming Europe into a highly energy-efficient, low-carbon economy. Likewise, energy providers, having realized that they have to face a change in doing business, are now actively involved in energy-saving initiatives and the provision of value-added services for customers. However, users (the last link in the chain who have higher potential for an impact), in spite of all their efforts, are still not aware of the need to change and have not enough incentives for initiating the change.

All these changes have caused the manifestation of more ambitious energy-saving objectives, which can only be achieved by involving users and targeting changes regarding energy consumption and energy provision. Until recently, however, the tools for involving users in the rational use of energy have been limited to general messages and public awareness campaigns, which (even if successful) cannot match the needed level of change in the users' conduct. That is the reason for new forms of relations between users and their consumption of energy, for higher levels of efficiency and awareness.

The promotion of pro-environmental behavior through different intervention strategies has a long tradition in social and environmental psychology. Intervention programs have been developed since the 1970s, to promote household energy saving, recycling, the use of public transport etc. But the potential of these traditional strategies is limited because of the financial and human resources needed to carry them out on a large scale. Some studies point out that the reasons for new environmental behavior vary very much, ranging from economic, to social, political or health motivations apart from purely environmental reasons, but these other interests are often ignored. However, recent studies have shown that the key factor making people adopt pro-environmental behavior is collective exposure and awareness.

Besides, the type of representation used for feedback is also influential. If it is too obvious and explicit, for an example, it may be taken as too personal and direct, or 'in your face', resulting in objections. An alternative approach is providing simple anonymous but striking representations to lure people's attention. Thus, people can think of various available choices and even public debates on the issues can be promoted. On the other hand, if the representation is too abstract and implicit, it may be attributed other meanings (e.g., as an art performance), resulting in people ignore it. The solution is possibly in-between but the ways of making these displays effective and embedded in the environment are still open questions.

Some of the reasons for the failure or overall slow market adoption of the previous systems for energy management and smart metering are the threats to security and privacy (explicitly identified as controversial in the case of Power Meter, Green OS or some Smart Meters). They are considered to be the most important barrier to the acceptance of those systems. The fact is that security and privacy are really basic factors in any practical system affecting users' activities in everyday life. Failure to protect the users' privacy and security would immediately disqualify otherwise good solutions for practical applications.

These general requirements are especially significant for the smart home control systems, as they are installed in the most important privacy refuge, our homes.

3 Communication Protocols and Standards

Due to the separate evolution process used in many regions and countries, different communication protocols and standards have been developed for the communication between the elements of a smart metering system. For a smart metering gateway and other smart metering devices to be able to communicate over the WAN, HAN and the LMN networks, many open protocols are used and they should be supported. Though the data in an LMN and HAN can be exchanged over proprietary protocols, the data exchange over the WAN should be done using the open standards for future compatibility as it passes through open and non proprietary systems. In Table 2, different communication protocols in use are discussed. For a thorough analysis and list of the communication protocols and standards refer to [12].

Table 2. Communications standards and protocols for smart meters

Communication Protocol	Short Description
IEC 61850 and UCA 2.0	IEC 61850 is an application layer standard which is a superset of UCA 2.0 and is primarily designed with intra-substation communication in mind [13]. It can also be used between substations or control centers (IEC 62445-1 and -2) and for metering applications. All services and models are designed in an abstract form called the ACSI (Abstract Communication Service Interface) and therefore independent of the underlying medium. ACSI can be mapped to TCP/IP over Ethernet. Part 7-420 added to IEC 61850 in 2009 covers distributed energy sources and storage and could even be used for V2G (Vehicle to grid) activities.
IEC 61334 PLC	Part 5 of the 61334 suite of standards defines several narrowband PLC (Power Line Communication) systems. Part 5-1 S-FSK is the most widely used. Because the allowed frequency range (3 kHz to 148.5 kHz in Europe), transmission power and the bandwidth is small [14], its suitability for (e.g.,) TCP/IP communication is limited. A typical PLC system consists of a backbone-coupled concentrator close to a MV/LV transformer. All traffic on the line is initiated by the concentrator, which acts as a "local relay" for a management center.
IEC 62056-21 / IEC 61107	The IEC 62056-21 standard is sometimes referred to as "Flag" or by its old name IEC 1107 [15]. Part 21 "direct local data exchange" describes software protocols and hardware suitable for data exchange with utility meters [16]. As one of the first meter data exchange standards, IEC 62056-21 is widely used today. However it does not use a data model or uniform memory mapping. Therefore meter communication requires manufacturer specific information, limiting interchangeability.
SITRED / Telegestore	In the beginning of the 90s [17], ENEL (which is Italy's largest distribution company), developed a transmission system called SITRED to read and manage meters remotely. A large test proved that remote management via the LV network was technically viable but the use of Ferraris meters was not cost effective enough. At the end of 90s, technology had advanced enough and ENEL concluded that changing all the low voltage meters for electronic ones would soon be profitable. In October 1999, the Telegestore project was started [18]. At the consumer side fully electronic meters communicate with a concentrator close to a transformer via PLC. The concentrator communicates with the acquisition center through an access server using GSM, PSTN or satellite. Two communication protocols (using PLC) are used: an enhanced version of LonTalk and more recently ENEL reintroduced its proprietary SITRED protocol that was used in the original project. SITRED uses a simple narrowband FSK-based solution that is relatively reliable throughout their whole diverse grid, reducing the cost of transceivers and coupling devices but limiting the attainable speed to about 2400 baud.

	LonTalk and SITRED differ in the PHY and MAC layers but the same proprietary application layer is used on top of both, ensuring transparency for the acquisition center.
SML (Sym^2 project)	The Smart Message Language [19] is a communication protocol for data acquisition and parameterization developed by the German utility companies RWE, EON and EnBW. The main idea is a simple structure usable in low-power embedded devices. The application layer defines a file and document structure to transmit data between the measuring point and a collection center. Both push and pull operations are supported. For the presentation layer, SML provides two options: readable XML encoding or more efficient SML binary coding. In typical metering applications SML messages will then be transported using TCP/UDP over IP networks. But for serial links such as GSM/PSTN or direct readout the SML transport protocol is available. SML is tailored specifically towards electricity metering and has to be viewed alongside the SyM2 project.
EN 13757 / M-Bus and Wireless M-Bus	EN 13757 (Meter bus) is a European standard [20] for the remote interaction with the utility meters and various sensors and actuators. It was developed at the University of Paderborn in Germany. M-Bus uses a reduced OSI layer stack. Its part 2 describes the physical and link layers; part 3 describes the application layer [21] and part 4 defines the Wireless M-Bus standard. Primary focus of the standard is on simple, low-cost, battery powered devices. Noteworthy is the support for Device Language Message Specification (DLMS) and its Companion Specification for Energy Metering (COSEM) in the lower layers. The DSMR (Dutch Smart Meter Requirements) [22] specifies wired and wireless M-Bus as the means of communication between a metering installation and other (gas, water, ...) meters, though with improved security (AES instead of DES).
DLMS/COSEM or IEC 62056	DLMS (integrated in IEC 62056 [23]) stands for Device Language Message Specification and is an application layer protocol, specifying general concepts for the modeling of object-related services, communication entities and protocols. Companion Specification for Energy Metering (COSEM) comprises metering specific objects based on Object Identification System (OBIS) codes for use with (x) DLMS. xDLMS is an extension to DLMS and describes how to access attributes and methods of COSEM objects. DLMS/COSEM is based on a client/server structure in which the data collection system acts as a client requesting data from the servers (pull operation), in this case the meters.
IEC 62056-31 ”Euridis”	Euridis [24] is a standard for remote and local meter reading introduced at the beginning of the 90s. In 1999, it was integrated into IEC 62056 as part 31. Euridis uses a twisted pair cabling system which acts as a local bus onto which all meters in a building can be linked. A magnetic coupler then allows connecting a handheld unit for readout or programming. The bus can be up to 500m or 100 devices and allows a data rate of 1200 baud half-duplex. The scope of Euridis is the local meter reading.
KNX	KNX is the result of the joint effort of Batibus, EIB and EHS. These three European consortia work on home and building control. KNX was made into standard ISO/IEC 14543-3-x in November 2006. KNX provides application models for distributed automation, configuration and management schemes, device profiles and a communication system (media and protocol stack). Possible communication media are twisted pair cabling, RF, IP/Ethernet and/or PLC. Each bus device has some sort of certified BCU (Bus coupler unit) that is typically flush mounted for switches, displays and sensors. To manage network resources, KNX uses both point-to-point and multicast communication. KNX aims to provide a complete solution for home and building automation and is backed by a lot of manufacturers worldwide. It must be noted that most KNX success stories about reduced energy consumption involve a complex interaction of KNX enabled boilers, lighting, etc. making the installation costs very high, especially for retrofitting.

ZigBee (Smart Energy Profile)	ZigBee is a low-power wireless communications technology designed for monitoring and control of devices, and is maintained and published by the ZigBee Alliance [6]. Home automation is one of the key market areas. Zigbee works on top of the IEEE 802.15.4 standard, in the unlicensed 2.4 GHz 5 or 915/868 MHz bands. An important feature of ZigBee is the possibility to handle mesh-networking, thereby extending the range and making a Zigbee network self-healing. The Zigbee Smart Energy Profile (numbered 0x0109) was defined in cooperation with the Homeplug Alliance in order to further enhance earlier HAN (Home Area Network) specifications. The profile defines device descriptions for simple meter reading, demand response, FEV charging, meter prepayment, etc.
Homeplug (Command & Control)	The Homeplug 1.0 standard was developed by the Homeplug Powerline Alliance in 2001 and allows communication over power lines at 14 Mbps half-duplex. In 2005, it was succeeded by the Homeplug AV, allowing over 100 Mbps and meant for HD multimedia applications. In 2007, version 1.0 of Homeplug Command & Control was announced, providing a PHY and MAC specification for low-speed (up to 5Kbps), low-cost PLC usable in house-control applications (lighting, HVAC, security and metering) [25].
6LoWPAN	The 6LoWPAN is a standard under development [26-27] from the IETF designed from the ground up to be used in small sensor networks. It will be used on top of the low power wireless (mesh) networks, specifically IEEE 802.15.4 (thus directly competing with ZigBee). Highlights include low memory implementations, support for the Zero-Conf and Neighbor Discovery capabilities of IPv6 and stateless header compression allowing the packets to be as small as 4 bytes. 6LoWPAN could realize the main concept of the "Internet of Things" by making it feasible to assign an IP address to the smallest of devices, sensors and actuators.
DSfG (SELMA Project)	DSfG [36] (Digitale Schnittstelle für Gasmessgeräte) is a protocol developed for communication between gas metering devices in gas measuring and regulating stations. It was developed in the context of SELMA project [37]. SELMA stands for Secure Electronic Measurement Data Exchange. It is a concept for the secure transmission and storage of energy data in an open system environment. It provides cryptographic protection and authentication, using digital signatures based on public key cryptography, for transmission of gas measurements over public networks. The key distribution is done using standard certificates. The concept is based on XML and therefore is protocol independent.

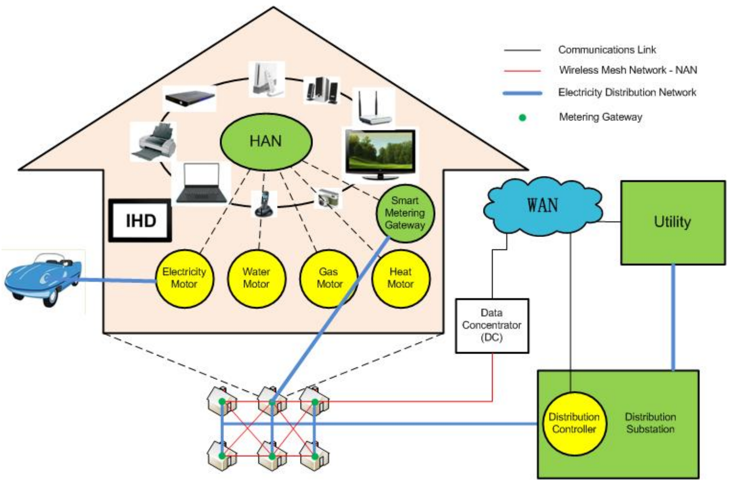


Figure 3. Elements of smart metering and the placement of a smart metering gateway and data concentrator

4 Privacy Concerns

4.1 Security vs. Privacy

Security and privacy are not the same, although sometimes due to misconception the terms are interchanged by novice in the field of information security. Privacy of information is extremely important in the context of smart metering. As the information is exchanged over public networks, it is susceptible to being seen or changed in transit by unintended people and this could have disastrous consequences for the individuals to whom the information belonged. Privacy is viewed differently in different cultures. Information security on the other hand addresses issues like confidentiality, integrity, authenticity, non-repudiation and availability. Confidentiality can address the privacy by protecting the data / information such that only the intended recipients can actually interpret the data and the non intended recipients are not able to interpret the data, although they might be able to see it.

4.2 Privacy risks with user friendly services

There are certain problems, which can affect and reduce the benefits of smart metering systems or the smart grid. The fine grain information on consumption / production gathered by smart meters is sufficient to infer very precise information on an individual life. The rapid progress of data mining technology and the integration of energy networks with other value-added services, even anonymous data can be used for deriving private information and thus creating huge legal loopholes. Besides, in future private data could be monitored in real-time or almost real-time, effectively transforming smart grids into a huge global surveillance system, which is even a greater problem not only for the individuals whose data is monitored but also for the entities responsible for maintaining the data.

These threats to security and privacy (identified as controversial in the case of Power Meter, Green OS or some smart meters) are thought to be the greatest barrier to the acceptance of the systems. These threats are the reason why the previous systems of energy management have failed or suffered a poor market adoption. Security and privacy are crucial aspects in any practical system affecting users' every-day activities. Any failure in this respect would disqualify for practical application solutions with potentially huge benefits both for individuals and industry participants. This is the reason why it is necessary to balance broad data information on consumption with the need for users' privacy protection.

As the security issues are also important to energy providers and distribution network providers, Smart Grid will become an integrated network although with communication still using existing public network and network nodes with unified protocols and communication stacks. A Smart Grid will be an attractive target for various attackers and cyber criminals, terrorists and even hostile nations. The most common cyber attacks are breaches of personal data within the network, payment fraud, 'denial of service' attack on the energy delivery across a smart grid. Besides, dangerous direct attacks to providers are also possible.

For all these reasons, some countries have considered these aspects within their legal framework. In Germany, for example, as energy consumption data is subject to privacy regulation, encryption methods are required for data transfer and processing. In addition to this, the German Ministry for economy and technology has asked the BSI (the federal agency for IT security) to develop a security concept and a protection profile for the smart meter gateway. The BSI picked a hardware security controller, called the Security Module, as an essential component for this protection profile. Moreover, the communication of data is further protected using a Communication Module, e.g., with a Transport Layer Security (TLS) channel. In order to address the potential man-in-the-middle attacks, dual encryption is proposed, i.e., the data is encrypted by the application and then again for transmission over the network.

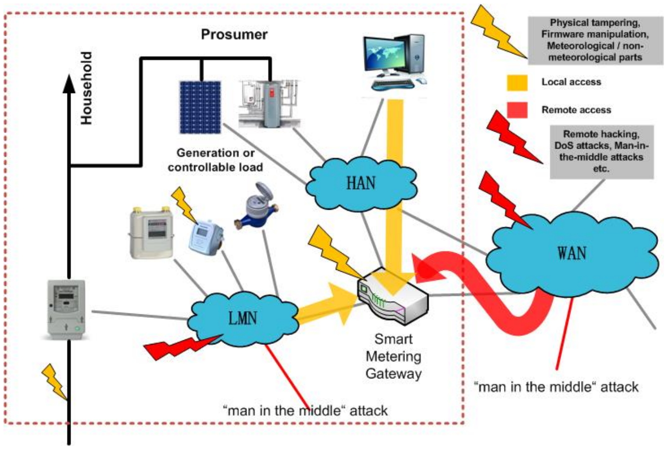

Prosumer
Household
Generation or controllable load
HAN
LMN
WAN
Smart Metering Gateway
"man in the middle" attack
"man in the middle" attack
Physical tampering, Firmware manipulation, Meteorological / non-meteorological parts
Local access
Remote access
Remote hacking, DoS attacks, Man-in-the-middle attacks etc.

Figure 4. Attack possibilities in a smart metering system.

4.3 Anonymity protocols for smart metering

Regulatory activities which are in use now focus only on some relevant elements of the smart grid, but they do not take into account the different processes supported by these components within the larger smart grid infrastructure, which consists of a number of different communication devices. The measures for privacy protection should be integrated into the design and deployment of the smart grid infrastructure (which is a challenging task) taking into account:

1. Privacy variable nature (data available within the smart grid together with the user's perception will change over time)
2. Technology evolution (the introduction of new additional devices and processes and loopholes, together with newly discovered privacy enhancing technologies (PETs)), while the smart grid infrastructure stays the same.

The European initiative for ITC architecture comprises technical, organizational and legal issues. If smart grids have to be adequately supported, an overview is needed (as large and detailed as possible) of the energy production, consumption, import and export status. It should be available for energy providers in a national or even international / European (critical) infrastructure / energy control center.

Smart meters are used for delivering the input. They measure the consumption or export (output), production and import (input) of energy or the balance of generated and consumed energy by customers, cars or any energy source or sink. In Smart Grids, meters have the function of sensors whose information is collected, accumulated and processed for local, regional, national or international management (generation, distribution, consumption, import, export). The results of the management centers activities will be commands and the metering devices will act as starters to the locally connected infrastructure.

The main goal of this activity is the support of a single or multiple points with a local, regional, national or European map of actual energy production and consumption; import and export, e.g., each input data should not be older than 15 minutes, where the metering data collection must not affect the clients' privacy.

This use case is independent of the smart meter accounting and billing applications. It only takes into account the energy situation monitoring used for various applications (management, distribution, leakage control, consumption control, forecasting, etc.).

Although the participating providers of the energy monitoring system are not interested in the private or personal information of the smart meters' clients, some measures have to be applied to avoid the misuse of the metering data delivered by smart grid meters. These measures provide privacy of the data needed for the energy map, even when collected frequently. The best proposed way to support the users' privacy is privacy by design. It means that it is not necessary to erase private or any other leaking information as they are supported by encryption during requirements that must exhibit a high level of trust with respect to accuracy of measures. Namely, we must avoid energy theft, and with respect to resources availability malevolent attacks must be avoided.

Apart from data compression and coding techniques, cryptographic mechanisms for providing privacy, correctness and trust have to be used together with different communication network technology and protocols.

The input data from the lower hierarchy level are stored into the intermediate aggregators between street level and the monitor center(s). The two-way communication is offered by the protocols. As a result, it is possible to get a zooming focus on regional, urban or suburban energy maps by the (national) monitoring center. Similarly, an interactive national or European energy map should be provided, allowing zooming on different levels of geographic areas down to the street level, but not to individual customers.

Some of the protocols and standards to address the issue of anonymity have been discussed in Section 5.

4.4 Scenarios based on user perception of privacy issues in smart grids

4.4.1 1st Scenario:

Imagine in January 2020, Claudia has just moved to her new smart home in Catania with an advanced energy control system connected to the smart grid through a smart meter. She is quite excited about her new home fully equipped with the newest generation of solar panels. She hopes she will be able to sell that energy, and not only save money in that way (as Catania, on the east coast of Sicily is the city with the most sunshine hours in Europe – an average of 2492 per year, or 6.8 hours per day), but to give her contribution to a better, greener planet as well.

Soon she finds out in a newspaper article that her situation is not only continuously monitored by the system (including every single electric appliance in the house which is necessary for the provision of the energy saving capabilities of the system), but also a lot of information is sent to the energy provider and the smart grid operator, in exchange for advanced services and reduced rates. As a matter of fact, the energy provider and the smart grid operator can control the load of the grid and energy production better in that way, allowing them to be more competitive and cost effective. As she considers it unacceptable to reveal her private information in this way, she decides to switch off the energy control system and to disable the communication capabilities of the smart meter. The same happens to many users.

As a result, the energy provider and the smart grid operator cannot accurately predict or react to the energy consumption peaks when they have no detailed information from the users, except approximately (which was done at the beginning of the century with electromechanical manual metering). The fact is that the smart grid operator has to work with huge infrastructure while the energy provider has to import energy coping with the unforeseen peaks, which all increases the average cost of the energy they sell and distribute. Analyzing the situation we can see that the energy control system was using an application not adapted to work with the specific smart meter and the smart grid equipment and for that reason the built-in privacy mechanisms were not effective.

This scenario reveals a few innovations which are not currently commercially available but have been identified as mid-term target by the industry:

1. Firstly, there is a new role (prosumer) which not only changes the relation to other roles, but introduces many technical challenges raising important concerns in relation to privacy and security.
2. Further, it is obvious that the scenario refers to the new generation smart meters capable of acting as a communication interface between the home appliances (including the advanced energy control system) and the smart grid. These smart meters are not yet available, but this fact (which might be a huge disadvantage for other smart grid projects) is an advantage for PSG to show the need for an engineering framework that can produce systems adaptable to the future evolution of the related systems and components (devices, services).
3. Lastly, the very existence of the advanced systems in the home and the grid with bi-directional communication capabilities is also new. It is evident that there is a service-based ecosystem in relations between the actors, in which prosumers, energy providers and grid operators are now acting both as service providers and service consumers.

Privacy and security expectations and requirements in this setting are both more numerous and more important as the failure to fulfill the expectations would result in a negative consumer response, slow market acceptance, or even commercial failure. In addition, this would imply significant damage to the actors' reputation. The crucial aspect for this scenario is to use an engineered approach which will ensure the system to operate in future, and integrating devices and other systems not fully known at design time, maintaining, at the same time, the original privacy and security requirements.

4.4.2 2nd scenario:

Nicole is authorized and granted to use the charge spot (through secure negotiation protocol with the Authorization Center- Trust & Security System) and the charge spot gives him a visual or acoustic signal feedback. Now he can activate and start the charging process, getting information on needed action steps to plug the car to the charge spot for the energy transfer.

The charging process is allowed by connecting the car to the charge spot. During the process, there is a data flow between the car and the charge spot which allows control and measuring the power and charging the level. This exchange is made by a secure communication link using wireless communication or the same cable used to transfer the energy.

This system (Vehicle to Grid) sends data and information on the "vehicle charging" process between the car and the charge spot and to other smart grid infrastructure elements and also to the Mobility Brokers. The data could be used for identification, localization, statistics accounting and billing, computing energy and power and charge level information used in the process for this vehicle by the identified user.

After the Fully Electric Vehicle (FEV) has been charged (High Battery Level), the charging stops. The user is informed by visual and acoustic feedback, while the vehicle and the charge spot can be released and disconnected and set up to an initial state to be ready for use by another user. During the charging process, physical security measures are taking account (through sensor or contact element) to avoid the possibility for the vehicle to be started or run causing an accident, or disconnected suddenly and abruptly when the battery charging is taking place and the car is plugged to the charge spot.

In this scenario, the grid and the Mobility Broker can gradually collect information on whereabouts of individual grid user (FEV users). But such information can be a privacy concern and that is why users may demand control of the information that grid operators and Mobility Brokers can infer on the user's grid use.

The system described above can be improved with privacy enablers to protect privacy, with the possibility to be introduced in the Mobility Brokers and at the charge spot.

The final enabler will be a privacy-enhanced mobility broker for FEV charging operations, using the specific mechanisms. Candidate solutions for consideration include making FEV anonymous or user identifiers in such a way that billing is still possible, but the tracking of FEV users is not, or encoding of the identifier's characteristics so that their access to some actors can be limited in a restricted way.

4.5 Miscellaneous privacy issues

There are many other privacy related concerns regarding the smart metering, as is the case with any upcoming technology. A passive adversary with access to the communication between a smart meter or a gateway and the utility can infer different observations from the usage data. The adversary can deduce when the customer wakes up, how many people are at home at a particular instance of time, when to they go to sleep, when do they have their breakfast, when do they watch TV and when they are or are not at home. It has been shown [8] that even the type of TV programs watched by consumers can be monitored and judged. In [9] an approach was proposed to identify the multimedia content through smart meter power usage profiles.

The data collected can potentially be used for many purposes, such as:

- Burglary
- Marketing / advertisement
- Piracy control
- Neighborhood check
- Consumer behavior
- Monitoring habits of neighbor
- Intrusion into privacy

Whatever the use of such data may be, there will always be an argument from the consumer side that his or her privacy is violated. One such argument was given by the Supreme Court in the U.S.A in this regard as follows,

The Supreme Court in U.S. affirmed the heightened Fourth Amendment privacy interest in the home and noted this interest is not outweighed by technology that allows government agents to "see" into the suspect's home without actually entering the premises. The Court stated, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search" and is "presumptively unreasonable without a warrant".

It is however, important to note that the privacy is not affected only by third party accessing customers' personal information without their knowledge. The privacy can also be violated by the customer themselves by allowing other people, firms or organizations to access their personal information or to be in-charge of this information.

4.6 Other issues that resists the usage of smart metering, e.g., health concerns

Customers have health concerns over the new technology of smart meters. The smart meters, as well as the gateway, are equipped to communicate over wireless links, e.g., between the smart meters, between meters and the gateway or from meter to the display units etc. The consumers and public health organizations have pointed out health risks, such as cancer, due to exposure to overexposure the wireless signals. The health concerns were one of the reasons which resulted in the UK government delaying the smart meter rollout by more than one year. There is however, no scientific evidence, so far, to support the claims that smart meters are bad for health or can cause cancer.

4.7 "Stop smart meters" protests

Recently, there have been a large number of protests against smart metering in the UK, USA and Canada. Specially people have been protesting against the smart meter rollout in California, USA [35] and British Columbia [36]. There are also a large number of websites [34-36] dedicated to register online protests against the smart meter rollout programmes. Most of these protests are based on the health issues, privacy concerns, safety violations and loss of sovereignty.

5 Security by Design

Because of the scale of the smart metering systems and the smart grid infrastructure, there is a need for security by design while developing the smart metering solutions. Though the support for remote software / firmware update to fix the security and other bugs is envisaged for smart meters and smart metering gateways, due to the criticality of the systems and its ultimate impact on a nation's security, it might be too late to react after an attack has been launched. Security by design is a group of concepts and means to induce security in a system by design rather than as add-ons when security loop holes are discovered. This means that the software and hardware systems for smart meters should be developed based on security analysis, security design, secure implementations and security testing in parallel to the analysis, design, implementation and testing of other system components.

In [10], a systematic method for modeling the functionalities of smart meters and a way to derive attacks that can be mounted on them was shown. The authors showed how attacks can be identified using the abstract model (behavior) of the software and then mapped to concrete model (actual implementation). An open source meter was used and two real attack scenarios were implemented, called as the communication interface attack and the physical memory attack. This approach shows that if the software of the smart metering systems is not designed with security considerations in mind, the attacks can always be done very systematically.

In the TERESA project [29], it was shown how security can be embedded into all the phases of the software development process, right from the analysis phase up until the implementation and testing phases. The results were applied and tested for the smart metering gateways according to the German BSI PP model (see Fig.5). A prototype was developed to show the applicability of the idea. If security is made a part of design, then many security issues can be solved through previous experiences gained from already discovered security loop holes. Pattern based engineering approach for secure software development was proposed in TERESA. A pattern is a general reusable solution to a commonly occurring problem in design [41]. Design patterns for software development were popularized in [39] where a large number of design level patterns were published aimed at object oriented programming. Secure design patterns, for aiding in secure software development were introduced in [39]. Secure design patterns for smart metering gateways, were proposed in [32] and used in the analysis, design, development and testing of software for the gateways of smart metering systems developed according to the BSI PP approach [30]. It was demonstrated that many flaws arising from loopholes in the analysis, design and especially in the development phase can be avoided if pattern based security engineering approach is used.

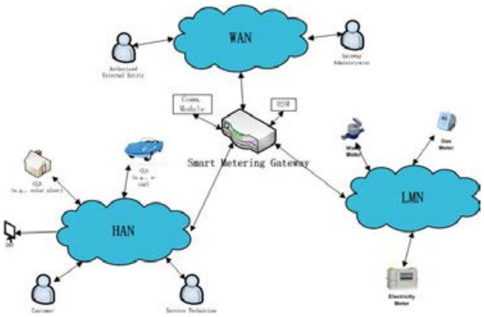


Figure 5. The smart metering gateway (TOE) architecture from the German BSI Protection Profile [29]

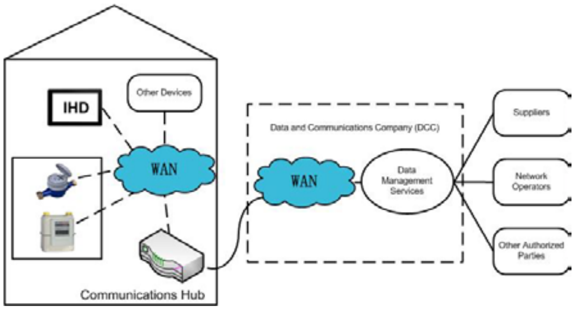


Figure 6. The smart metering architecture proposed by the department of energy and climate change, UK [32]

In addition to addressing the general security issues using security by design techniques, privacy protection should also be addressed. There are known means for privacy protection in other domains that could be imported and applied in the smart metering domain for "privacy by design". One such method was proposed in PriPAYD [42]. In Pay as you drive (PAYD) systems, for car insurance, the information for billing a user for his insurance, based on how much and when he drives, is normally collected by a black box in the car. This data is then transferred to the insurance company via a communications unit. In PriPAYD [42], only the minimum information necessary to bill the client is transferred to the insurance company. Privacy preserving methods are proposed in [42] to protect the privacy of clients. Such solutions should also be applied in the development of smart metering solutions so that the privacy of the customers is not compromised.

6 Smart Metering Projects

6.1 Research projects and their goals

Several research projects are funded globally to research the issues related to smart metering and smart grids. Many of the issues being researched in these projects involve scalability, availability, software development, hardware components, communication protocols, communication interfaces, security, privacy protection and actual physical installation of hardware devices.

A partial list of the smart metering and smart grid projects around the world and their goals are given below.

6.2 Building to Grid (B2G)-Smart Grids Modell region Salzburg

The B2G project was completed in 2013 in Salzburg Vienna. The goal of the project was to investigate through a series of experiments where the limits of intelligent buildings in a smart grid are. A number of generic load models for buildings were developed and embedded into an interoperable communication infrastructure. Methods for improvement of energy efficiency were researched in the project.

6.3 OPENmeter

OPENmeter project was funded by EU and it has been successfully completed. The main objective of the OPEN meter project was to specify a comprehensive set of open and public standards for AMI. It supported the electricity, gas, water and heat metering.

6.4 METER-ON

METER-ON, also an EU funded project and successfully completed now, was based on the coordination and support action to steer the implementation of smart metering solutions throughout Europe. The project aimed at speeding up and optimizing the adoption of smart metering technologies and infrastructures in Europe by effectively collecting the most successful experiences in the field and highlighting the conditions that enabled their development.

6.5 European Smart Metering Alliance (ESMA)

ESMA, funded by EU, has defined and spread best practices in smart metering across EU member states and sought to maximize the resulting energy savings. The project produced reports on key aspects of smart metering.

6.6 TERESA

Trusted Computing Engineering for Resource Constraint Embedded Systems Applications (TERESA), funded by the EU 7th FWP (Seventh Framework Programme), provided guidelines for the specification of sector specific RCES trusted computing engineering. Software process engineers in a given sector can then use the guidelines to define a trusted computing engineering process in the resource constraint embedded systems (RCES) sector.

The main application areas investigated in TERESA were:

- Automotive
- Home control
- Industry control
- Metrology (Smart metering gateways)

6.7 SMART METERING

The SMART METERING project, funded by the Latvia-Lithuania Cross border development programme and partly by European regional development program, envisaged the possibility to carry out the research, for implementation, testing, improvement and adjusting the automated meter reading systems, based on sensor networks, to local infrastructure and to clients. The aim of the project was to encourage the competitiveness of the region by creating a framework for technology development and accommodation for regional needs in the field of automated meter reading – smart metering.

6.8 FENIX

FENIX project was funded by the government of the United Kingdom. The objective of FENIX was to boost DER (Distributed Energy Resources) by maximizing their contribution to the electric power system, through aggregation into Large Scale Virtual Power Plants (LSVPP) and decentralized management.

6.9 Customer led network revolution

Customer led network revolution is an ongoing activity funded by the North East and Yorkshire, UK. Northern Power grid and its partners will be trialing smart grid solutions on the distribution network within the electricity grid as well as creating smart-enabled homes to give customers more flexibility over the way they use and generate electricity. The results will help the industry make sure the electricity networks can handle the mass introduction of solar PV panels, electric cars and other low-carbon technologies (find the best way to keep down the cost of connecting customers to the grid and minimizing the cost of meeting their electricity needs).

6.10 ESB Smart grid demonstration

The ESB Networks smart grid project, funded by Galway Ireland, explored the development of wind farm connections, assess the effectiveness of customer response and interest in demand and consumption management, investigate the readiness of secondary networks for high penetration levels of electric vehicles and maximize existing distribution electricity networks.

6.11 ADDRESS

The ADDRESS project, funded by The Houat and Hoedic islands, Brittany Region, France, aimed at delivering a comprehensive commercial and technical framework for the development of “Active Demand” in the smart grids of the future. ADDRESS investigated how to effectively activate participation of domestic and small commercial customers in power system markets and in the provision of services to the different power system participants.

6.12 REALISEGRID

The mission of REALISEGRID project, funded by the EU, was to develop a set of criteria, metrics, methods and tools to assess how the transmission infrastructure should be optimally developed to support the achievement of a reliable, competitive and sustainable electricity supply in the EU.

6.13 INOVGRID

INOVGRID project, funded by the EU in Portugal, aimed at replacing the current LV meters with electronic devices, called Energy Boxes (EB), using AMM (Automated Meter Management) standards. These EB are integrated in an automated third generation electrical grid (smart grid) in which network devices are placed (DTC) that will manage the EB through new TI/SI solutions by aggregating the gathered information and providing new services to consumers.

6.14 AMM Projects

The AMM projects were funded by the government of Helsinki, Finland. The target was the mass rollout of smart meters, which took just over one year. Now all the 200,000 meters have been installed and the customers are enjoying the benefits of smart metering. They will have access to new services, the most significant of which are changes to their electricity bills to actual and not estimated billing, and more precise reporting of their electricity usage as a whole. Consumers will see their consumption broken down into hourly reports online.

6.15 GRID4EU

Grid4EU, funded by EU, tests the potential of smart grids in areas such as renewable energy integration, electric vehicle development, grid automation, energy storage, energy efficiency and load reduction.

6.16 Smart House / Smart Grid

The SmartHouse/SmartGrid project, carried out in Germany and funded by the EU, was set out to validate and test how ICT-enabled collaborative technical-commercial aggregations of Smart Houses provide an essential step to achieve the needed radically higher levels of energy efficiency in Europe. Three main goals that SmartHouse/SmartGrid project is heading towards are to improve energy efficiency, increase the penetration of renewable energies, and diversify and decentralize Europe’s energy mix.

6.17 Hydro one smart meter rollout projects

The Hydro one smart meter rollout project installed 1.3 million meters in Ontario, Canada. The initiatives included employing numerous smart network and smart home technologies enabled by an integrated combination of standards-based mesh radio and state-of-the-art WiMAX wireless technology, including distribution station and security monitoring, mobile work dispatch and accomplishment reporting, automated vehicle locate safety monitoring etc.

The hydro one smart meter project was also implemented in British Colombia, Canada. BC Hydro upgraded homes & businesses across B.C. with smart meters. 1.8 million of BC Hydro customers were given smart meters with free installation.

6.18 Energy Smart Florida

This project involved deploying an advanced metering infrastructure (AMI) in Miami, Florida, USA. It included distribution automation, new electricity pricing programs, and advanced monitoring equipment for the transmission system.

6.19 AEP Texas GridSmart

American Electric Power (AEP) Texas in Corpus Christi, Texas, USA, installed smart meters to nearly 1,000,000 electric customers in October 2009. For its smart grid initiative, AEP has chosen Landi+Gyr’s Gridstream RF (Radio Frequency) smart grid network.

6.20 SCS Smart Grid

The Southern Company Services Smart Grid project, in Alabama USA, involved integrated upgrades of the distribution, transmission, and grid management systems throughout their large service territory. Major efforts included automation of major parts of the distribution system, automation of selected transmission lines, and new equipment for many substations.

6.21 Synergy Advanced Metering

The Thornlie and Canning Vale Advanced Metering Proof of Concept study, in Thornlie, Western Australia, involved an investigation into a behavioral trial of advanced metering solutions as a means of helping customers manage their electricity consumption habits. The study aims to revolutionize the way households consume energy and monitor their energy use. The study included multiple channels of communicating with customers including through an In Home Display, an interactive website, email and SMS to encourage behavioral change.

6.22 Adelaide Solar City

The program, being implemented in Adelaide, Salisbury, South Australia, combines solar power, smart metering, energy efficiency and cost reflective pricing to trial a range of innovative energy solutions. It's being delivered in the Cities of Salisbury, Tea Tree Gully, Playford and Adelaide City as part of the Australian Government's $94 million Solar Cities program.

6.23 Smart Grid Smart City

Smart Grid, Smart City is a $100 million Australian government funded project in Sydney. The project is testing a range of smart grid technologies; gathering information about the benefits and costs of implementing these technologies in an Australian setting. Up to 30,000 households will participate in the project which runs between 2010 and 2013.

6.24 Townsville Queensland Solar City

The Townsville Queensland Solar City project is part of the Australian Government’s leading-edge Solar Cities program in Queensland, Australia. The project trials a range of initiatives that aim to reduce wasteful energy usage, increase solar energy usage and cut greenhouse gas emissions by more than 50,000 tones. One of the trials comprises of the installation of 2,500 electricity smart meters for homes and businesses.

6.25 Mercury Energy Smart Meter Deployment

More than 300,000 Mercury Energy customers will receive a high-tech smart meter, through metering services provider in Aukland, New Zealand. The new meters record usage in 30 minute periods, meaning that information for bills will always be accurate and up to date and this information could also be used to help customers manage their power consumption.

7 Conclusion

Intelligent buildings are not imaginable anymore without smart devices for energy consumption and monitoring. The liberalization of the energy and metering services markets need new communication systems for smart metering and corresponding security architecture to enhance the trust level in the system. On one hand, a consumer won’t trust the system if he is not assured that his privacy will not be compromised. On the other hand, a utility won’t trust the system if the threat perception and security risks are high. This paper discusses the evolution of smart metering systems from manual readouts of the electromechanical metering devices to fully automated electronic smart metering systems with advanced metering infrastructure in the context of smart grids. However, this progress comes at the cost of security and privacy concerns. The paper looks in to the privacy and security issues that may arise due to the current solutions. The solutions for smart metering architectures and for security of the components therein, proposed or adopted by the smart metering architectures in different countries are discussed in the paper. The smart grid is a network of open systems and the data exchange takes place using different smart metering protocols and standards which are summarized in the paper. The need for a security by design approach is explored in this paper. Some solutions for security by design and privacy by design approach are discussed. A partial list of smart metering and smart grid projects, around the world, is given in the end.

REFERENCES

[1] C. Diakaki, E. Grigoroudis and D. Kolokotsa, “Towards a multi-objective optimization approach for improving energy efficiency in buildings”, Energy and Buildings, vol. 40, issue 9, 2008, pp. 1747-1754.

[2] J. Torriti, M. G. Hasan and M. Leach, “Demand response experience in Europe: Policies, programmes and implementation”, Energy, vol. 35, issue 4, 2009, pp. 1575-1583

[3] S. Marvin, H. Chappells and S. Guy, “Pathways of smart metering development: shaping environmental innovation, Computers, Environment and Urban Systems”, vol. 23, issue 2, 1999, pp. 109-126

[4] S. Hick and C. Ruland, “Security Aspects for Secure Download of Regulated Software”, Trustbus 2007, LNCS 4657, pp. 219 – 227, Springer Verlag, Berlin, Germany

[5] C. Dromacque, S. Xu and S. Baynes, "Case study on innovative smart billing for household consumers", VaasaETT Global Energy Think Tank, July 2013

[6] The ZigBee Alliance. [Online]. Available: www.zigbee.org

[7] Multi Utility Communication (MUC), Version 1.0, 8/2009, VDE, http://www.vde.de/de/fnn/arbeitsgebiete/messwesen/documents/FNN_LH-MUC_1-0_2009-08-05.pdf

[8] D. Carluccio and S. Brinkhaus, 28th Chaos Communication Congress (28C3), Dec 2011, Berlin, Germany.

[9] U. Greveler, P. Gloesekoetter, B. Justus and D. Loehr, “Multimedia Content Identification Through Smart Meter Power Usage Profiles”, Proceedings of the International Conference on Information and Knowledge Engineering IKE'12, Jul 16-18, 2012, Las Vegas, Nevada, USA.

[10] F. M. Tabrizi and K. Pattabiraman, "A model for security analysis of smart meters," IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 1-6, Jun 25-28, 2012.

[11] M. Moghavvemi, S.Y. Tan and S. K. Wong, 2005, “A reliable and economically feasible automatic meter reading system using power line distribution network”, International Journal Of Engineering Materials And Energy Research Center, Vol. 18, No. 3, pp. 301-318.

[12] K. D. Craemer and G. Deconinck, “Analysis of state-of-the-art smart metering communication standards,” IEEE Benelux Young Researchers Symposium 2010 in Electrical Power Engineering, Leuven, Belgium, March 29-30, 2010.

[13] C. Brunner, “IEC 61850 for power system communication,” in Transmission and Distribution Conference and Exposition, 2008. T&D. IEEE/PES, Apr. 2008, pp. 1–6.

[14] Z. Kapar, “Power-Line Communication - Regulation Introduction, PL Modem Implementation and Possible Application,” in In: Proc. 12th International scientific conference Radioelektronika 2002, Bratislava, SK, STUBA, 2002.

[15] The Flag Protocol. [Online]. Available: www.theflagprotocol.com

[16] L. Woolner and B. Loe, “FLAG/DLMS Communications,” in BEAMA Communications and Interoperability Seminar, 2007.

[17] E. Comellini, R. Gargiuli, C. Mirra, P. Mirandola, and M. Pioli, “ENEL standardised telecontrol system for MV distribution network automation,” in Electricity Distribution, 1989. CIRED 1989. 10th International Conference on, May 1989, pp. 341–345 vol.4.

[18] B. Botte, V. Cannatelli, and S. Rogai, “The Telegestore project in ENELs metering system,” in 18th International Conference on Electricity Distribution, Turin, Italy, Jun 6-9, 2005

[19] M. Wisy, “SML, Smart Message Language v1.03,” Nov. 2008.

[20] EN 13757 Communication systems for remote reading of meters, European Committee for Standardization (CEN) Std.

[21] Meter Bus, EN13757-2 and EN13757-3. [Online]. Available: www.m-bus.com/

[22] Kema Consulting, “Smart Meter Requirements - Dutch Smart Meter specification and tender dossier V2.31,” Jan. 2009.

[23] IEC 62056 Electricity metering - Data exchange for meter reading, tariff and load control, International Electrotechnical Commission Std.

[24] The essential of Euridis. [Online]. Available: www.euridis.org/solutiondetails.html

[25] IEC 14543-3 Information technology - Home electronic system (HES) architecture, International Electrotechnical Commission Std.

[26] Sabrina Bradbury and The Homeplug Command & Control Marketing Work Group, “HomePlug Command & Control (C&C) Overview White Paper,” Sep. 2008.

[27] N. Kushalnagar, G. Montenegro, J. Hui and D. Culler, “IETF RFC4919: Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” Sep. 2007. [Online]. Available: http://tools.ietf.org/html/rfc4919

[28] N. Kushalnagar, G. Montenegro, J. Hui and D. Culler, “IETF RFC4944: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals,” Aug. 2007. [Online]. Available: http://tools.ietf.org/html/rfc4944.

[29] Trusted Computing Engineering for Resource Constrained Embedded Systems Applications, [Online]. Available: http://www.teresa-project.eu.

[30] BSI: Protection Profile for the Gateway of a Smart Metering System (March 2013), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf, last accessed and verified Feb 01, 2014.

[31] BSI: Protection Profile for the Security Module of a Smart Metering System (March 2013), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP_Security_Module.pdf, last accessed and verified Feb 01, 2014.

[32] O. Ur-Rehman and Donatus Weber, "Security Patterns for the Gateway of a Smart Metering System", International Conference on Electrical Measurement and Instrumentation Engineering, Nov 22-23, 2012, Amsterdam, Netherlands.

[33] Smart Metering Implementation Programme: Prospectus, Department of Energy and Climate Change (DECC) and Gas and Electricity Markets Authority (GEMA), 27th July 2010, London, UK.

[34] Stop smart meters, UK, [Online], http://stopsmartmeters.org.uk/, last accessed and verified Feb 01, 2014.

[35] Stop smart meters USA, [Online], www.stopsmartmeters.org, last accessed and verified Feb 01, 2014.

[36] Stop smart meters, British Columbia, Canada, [Online], http://www.stopsmartmetersbc.ca/, last accessed and verified Feb 01, 2014.

[37] Digitale Schnittstelle für Gasmessgeräte (DSFG), [Online], http://www.selma-project.de/uebersicht/SELMA_Kurz_2007_09_V0.3.pdf, last accessed and verified Feb 01, 2014.

[38] Secure Electronic Measurement Data Exchange (SELMA) Project, [Online], http://www.selma.eu/

[39] E. Gamma, R. Helm, R. Johnson and J. M. Vlissides, “Design Patterns: Elements of Reusable Object-Oriented Software”, Addison-Wesley, 1995 (ISBN 0201633612).

[40] J. Yoder and J. Barcalow, “Architectural Patterns for Enabling Application Security.”, Proceedings of the 4th Pattern Languages of Programming conference September 3-5, 1997, Allerton Park, Monticello, Illinois, USA.

[41] C. Dougherty, K. Sayre, R. C. Seacord, D. Svoboda and K. Togashi, “Secure Design Patterns”, Oct 2009, CERT, Software Engineering Institute, Carnegie Mellon University.

[42] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel. “Pri-PAYD: Privacy Friendly Pay-As-You-Drive Insurance,” IEEE Transactions on Dependable and Secure Computing, vol. 8, issue 5, pp. 742-755, Oct 2011.