International Journal of Applied Science and Engineering
2017. 14, 3: 147-169

Towards Secure & Green Advanced Metering Infrastructure (AMI)

Qutaiba I. Ali[*]

Computer Engineering Department, Mosul University, Iraq

Abstract: This paper deals with the design issues of a secure and green Advanced Metering Infrastructure (AMI). The first part of the paper suggests enhancing the reliability of AMI system using wireless ad hoc Network technology. The suggested Advanced Metering Infrastructure consists of various types of wireless nodes we called Green Wireless Router (GWR). Here, we propose that GWRs can harvest the energy needed for its work from the surrounding environment, especially solar energy. Such suggestion permits to install GWRs in any place without considering the power supply availability and hence, extensive area is covered by the AMI. The different network traffic patterns generated from running a customized AMI simulation model were used in an experimental network based mainly on UBICOM IP2022 network processor platform (as the implementation of the intended GWR)with the aim of measuring its power consumption under different realistic circumstances. In order to decrease the power consumption of the suggested GWR and to extend the life time of the batteries, two power management schemes we called Controlled Duty Cycling (CDC) and Event Driven Duty Cycling were suggested and implemented. The second part of the paper suggests a GWR security model to protect it against different internal and external threats. The suggested GWR security model must respond to many objectives, it should ensure that the administrative information exchanged is correct and undiscoverable (information authenticity and privacy), the source is who he claims to be (message integrity and source authentication) and the system is robust and available (using Cooperative Intrusion Detection System).

Keywords: Advanced Metering Infrastructure (AMI); Green Wireless Router (GWR); Solar Energy Harvesting; Network Security.

1. Introduction

Smart Grid is a contemporary electric power grid infrastructurefor enhanced effectiveness, consistency and safety, with soft combination of renewable and alternative energy sources throughout automated control and modern communication technologies. In the smart grid, reliable and real-time information becomes the key factor for consistent delivery of power from the generating units to the end-users [1-4].

The key component of smart grid which facilitates this intelligent integration and communication is Advanced Metering Infrastructure (AMI). An AMI comprises of advanced meters (i.e., Smart Meters; SM) that performs various tasks apart from recording power usage. The smart meters collect and analyze the information of energy consumption and demand data from home appliances, communicate and control for optimization of energy management, power quality

[*]Corresponding author; e-mail: qut1974@gmail.com

doi: 10.6703/IJASE.2017.14(3).147

Received 19 September 2015
Revised 15 February 2017
Accepted 25 February 2017

etc. AMI provides a two-way information flow between SMs and electric power control centre for reporting and analysis to offer direct load control. Thus, a communication network which transfers massive amount of real time information to the control centre requires a high degree of operational reliability.

In this paper, we suggest enhancing the reliability of AMI communication network using wireless ad hoc Network technology. The suggested AMI infrastructure consists of various types of wireless fixed nodes performing different actions according to the applications demands. An important class of these nodes are Green Wireless Router (GWR). GWRs, as a part of the AMI infrastructure, receive different packets from SMs, then forward them to the AMI server. These GWRs would create an *ad hoc* network in order to assist each other to deliver data packets to their destinations, that's why a suitable ad hoc routing protocol is needed, see Figure 1. As a member in the ad hoc network, GWR also behaves as a router in order to deliver other GWRs traffic to their destinations. The adoption of ad hoc networking to enhance AMI systems reliability is much superior over other wireless and wired methods. Ad hoc networks are developed to provide protocol functionality suitable for wireless routing application within both static and dynamic topologies. Also communication is established among the nodes without the use of centralized infrastructure or administration and each node acts as both an end-host and as a router. In addition, the cost of ownership, installation and maintenance is very low comparing to other networking methods.

Due to power supply requirements, it is required to localize GWRs near to wired electricity sources, however, such placement limits the area covered by the suggested infrastructureand hence, their services. In order to overcome this restriction, it is required to establish a self powered GWRs. Here, we suggest that GWRs can harvest the energy needed for its work from the surrounding environment, especially solar energy, see Figure 1. Such suggestion permits to install GWRs in any place without considering the power supply availability and hence, extensive area is covered by the proposed infrastructure. However, GWR may be subjected to different network traffic conditions which affect seriously on their power consumption and hence their running period. One of the goals of this paper is the planning procedure of a solar powered GWR using an efficient power management method.

On the other hand, it is clear that GWR plays a major rule in the suggested green AMI, and hence, securing this device is a priority. GWRs are subjected to different network traffic conditions and security attacks, which affect seriously on their performance, power consumption and hence their running period, so that the second goal of this paper is to define different security methods to protect GWR (in special) and AMI (in general) against these threats.

Since we are dealing with energy harvesting and security issues in AMI, it is important to investigate several previous works in these fields. There is some recent work addressing different security issues of AMI in smart grid. In [4], the authors proposed a new utility security management and authentication scheme for action/command requests in the host area electric power system (AEPS) and interconnected multiple neighboring AEPSs. Secure and intuitive device authentication techniques for smart-grid-enabled home area networks (HANs) are proposed in [5], where the authors assumed a distributed architecture for a HAN consisting of smart appliances, a smart meter, and a gateway. Focusing on authentication protocols, in [6], the authors discussed the key design principles and engineering practices that can help to ensure the correctness and effectiveness of the authentication standards in power grid protocols. A method for secure anonymization of frequent electrical metering data was described in [7]. It provided a third party escrow mechanism for authenticated anonymous meter readings that are difficult to associate with a particular smart meter or customer. The privacy issues implicated by the development of demand response systems were explored in [8], which demonstrated that the data collected by AMI reveals detailed information about the user behavior within home. The authors in [9] propose two-phase method to provide security of data using dedicated authentication server which inhibits malicious and unauthorized nodes to gain access to AMI communication network. On the other hand, in [10] the authors propose a new protocol, Integrated Authentication and Confidentiality (IAC), to provide trust services, data privacy, and integrity by mutual authentications whenever a new smart meter initiates and joins the smart grid AMI network. Finally, the authors in [11] suggested a security-communication trade-off Smart Grid AMI by proposing a secure lossless aggregation protocol facilitating both per-hops as well as end-to-end security, which is also energy efficient.

Regarding energy harvesting, some papers deal with diverse aspects in this field. In [12], the authors investigate the feasibility of powering wireless metering devices, namely heat cost allocators, by thermal energy harvested from radiators. While the authors in [13] showed that energy harvesting provides increased privacy by diversifying the energy source, while a storage device can be used to increase both the energy efficiency and the privacy of the user.

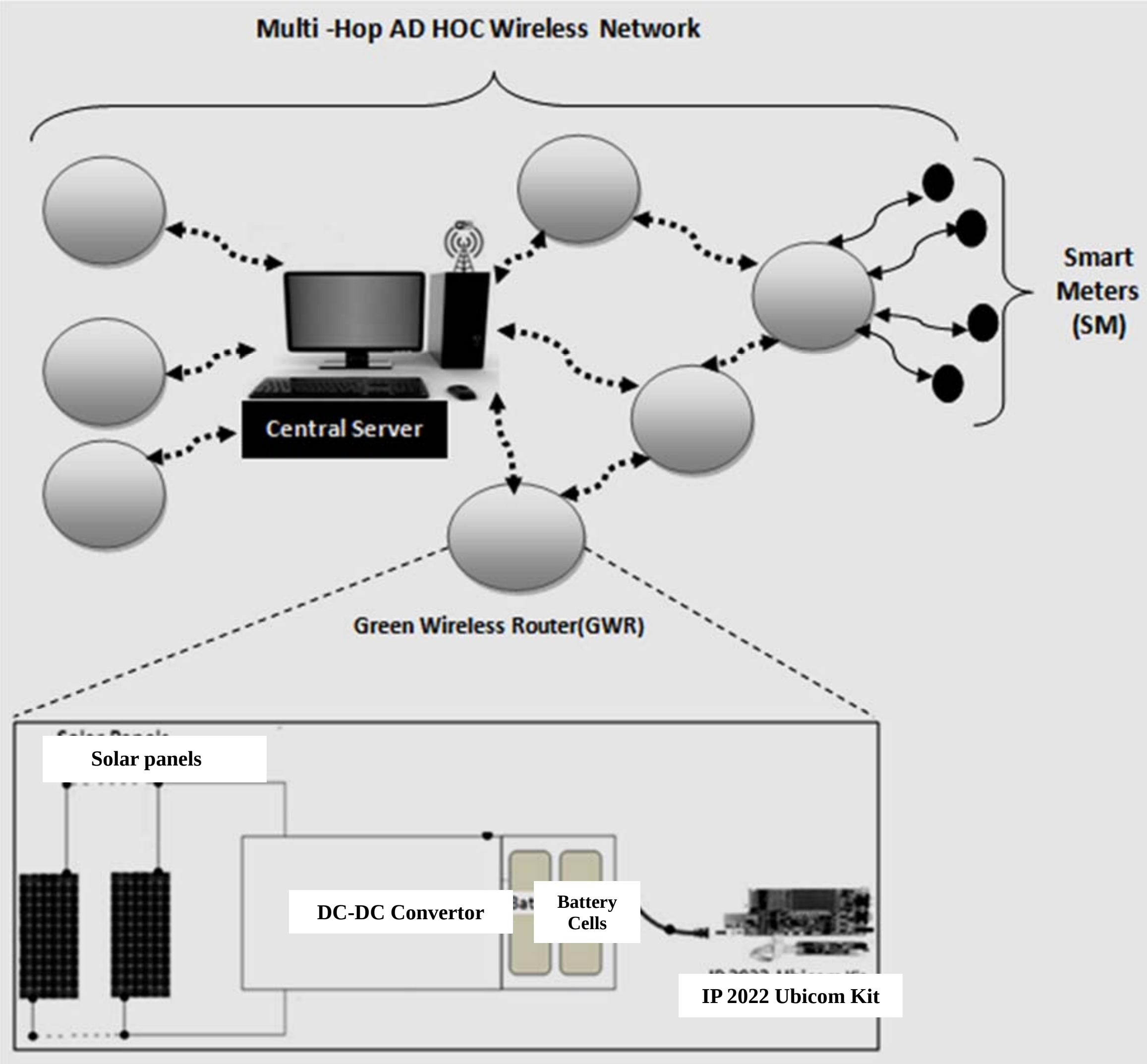


Figure 1. The suggested green AMI

2. Investigation of Power Requirements of UBICOM IP2022 Network Processor

This paper focus on using solar cell energy harvesting in providing an alternative power source to supply GWRs. A 4-4.0-100 solar panel (from Solar World Inc.) that measured 4.25” x 2.5”, was adopted in this work. In this paper, we make use of our earlier design of an energy harvesting module which can be used with diverse categories of embedded GWRs [14]. Even though, UBICOM IP2022 was chosen to be the proposed GWR, the recommended energy harvesting circuit can be slightly customized to suit other embedded devices. The central part of the harvesting module is Texas Instruments TPS63000 low power boost-buck DC-DC Converter [14], see Figure 1. The electrical energy produced by the solar panels are routed by the harvesting circuit and then stored in two parallel AA battery cells with voltage varies between 2.9V and 3.1V [14].

Due to its multipurpose features, embedded UBICOM IP2022 platform [15] was chosen in this paper to realize the proposed GWR. An experimental network setup must be used to perform several tests in order to determine the power requirements of UBICOM IP2022 platform, see Figure 2. The experimental network consists of an ordinary PCs supplied with Belkin Dual-Band Wireless PCMCIA Network Card F6D3010working at different data rates, IP2022 Ubicom platform was also supplied with the same WLAN NIC, the energy harvesting module and a real time storage oscilloscope. Traffic generator PC1 was programmed to send and receive a 1Mbps streamed UDP traffic to and from the IP2022 Ubicom platform. The real time oscilloscope (Tektronix224) was used to measure the drained current from the batteries (according to the different network traffic conditions) by measuring the voltage across a (0.1Ω) resistor, which is proportional to the drained current. The objective of this experiment is to record the current drained by the GWR according to its different modes of operation: Transmission, Reception, IDLE, CPU full load and SLEEP. Table 1 summarize the settings of this experiment while Table 2 lists the average values obtained for different data rates.

As expected, the maximum drained current was achieved when working in the transmission mode, while the reception mode requires less current. Ubicom board measurements were performed after disconnecting the WLAN NIC and the drained current was observed in three cases: IDLE mode (CPU utilization is 0%), when CPU is fully loaded (CPU utilization is 100%) and SLEEP mode (explained later).

3. Research Methodology

In order to evaluate the power consumption of the intended Ubicom GWR under realistic network traffic conditions, a simulation model was built using the Network Simulation package. The goal of building this model is to generate a traffic patterns as close as possible to the real situations. Our network represents a typical Advanced Metering Infrastructure of 50 GWRs covering (10 Km x 10 Km) area. The data traffic generated by the GWRs (as a result to their interaction with the SMs and other GWRs) are forwarded using a suitable routing protocol to a central server. It was assumed that SMs generate their 200 byte status packets each two seconds [3], while GWRs generate their 1000 byte measurement report 10 times per minute and forward them to the central server [3]. As a result of our earlier analysis in [16], Optimized Link State Routing (OLSR) gives the best performance compared to other ad hoc routing protocols when working in non-stationary ad hoc topology, so that it was adopted in our simulation model. OLSR is a *proactive link-State* routing protocol designed for *ad hoc* networks which show both low bandwidth utilization and low packet delay. OLSR is a type of classical link-state routing protocol, which relies in employing an efficient periodic flooding of control information using special nodes

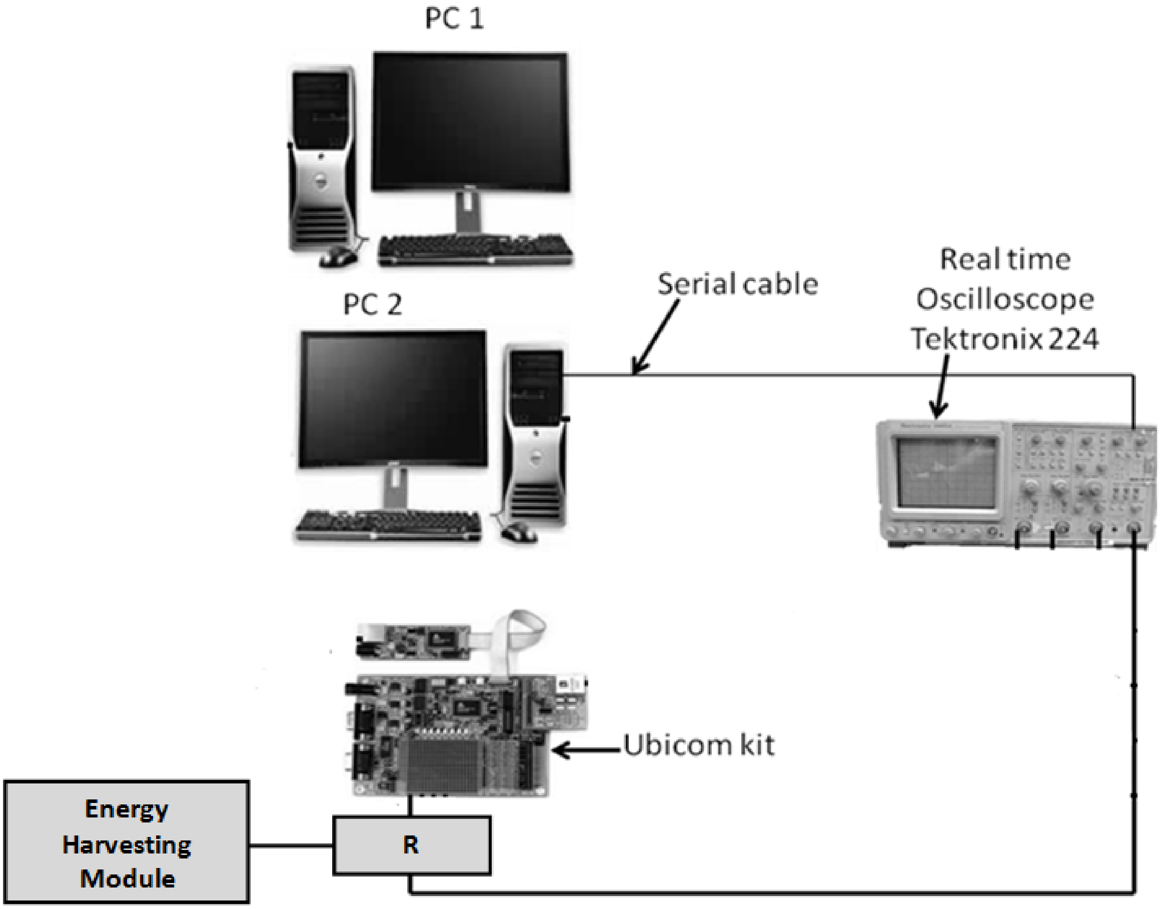


Figure 2. The Experimental Network Setup

Table 1. Network setup

Experiment duration in each Case (Minute)	5
WLAN NIC	Belkin (a/b/g) Dual-Band WLAN PCMCIA Card
Supply Voltage(v)	3
RF power (W)	1 dBm
WLAN Packet length (Byte)	1500
Packet/sec.	84

Table 2. Measured current values

Current drained in TX mode(mA)	150(for IEEE802.11a)
Current drained in RX mode(mA)	120 (for IEEE802.11a)
Current drained in IDLE mode(mA)(WLAN NIC disconnected)	100
Current drained in CPU full load mode (mA) (WLAN NIC disconnected)	150
Current drained in SLEEP mode(mA)(for the Ubicom board only)	1

that act as *multipoint relays* (MPRs). The use of MPRs reduces the number of required transmissions [17]. OLSR daemons periodically exchange different messages in order to maintain the topology information of the entire network. The core functionality is performed mainly by using three different types of messages: HELLO, TC (topology control), and MID (multiple interface declaration) messages. The OLSR mechanisms are regulated by a set of parameters predefined in the OLSR RFC 3626 [17] which was used in our simulation model, see Table 3. In order to simplify our simulation model, GWRs were assumed to be identical and subjected to the same network traffic conditions. Different scenarios were built to determine the effect of different network parameters on the network traffic and hence, GWR power consumption.

Table 3. Simulation model parameters

Simulation Time (Minute)	60
No. of GWR nodes	50
Network Span Area (Km^2)	100 (10 K m x 10 K m)
AMI Traffic Description	SMs to GWR packet length = 200 Byte SMs to GWR packets rate = 0.5 Packet/s GWR to Central Server packet length = 1000 Byte GWR to Central Server packets rate = 10 Packet/Minute
GWR Modeling Parameters	Packets Processing Rate (Packet/sec.) = 2000 Memory = 2 M Byte
WLAN settings	Data Rate (Mbps) : 6, 12, 18 for IEEE802.11a
OLSR settings	Hello Interval(sec.) = 2 TC Interval(sec.) = 5 Neighbor Hold Time(sec.) = 6 Topology Hold Time(sec.) = 15 Duplicate Message Hold Time(sec.) = 30

Scenario 1:

In this scenario, we will determine the most appropriate data rate which gives the best network performance. It was assumed that the maximum number of SMs served by each GWR were 200. Table 4 lists the results obtained from running the simulation model. From the measured statistics, it is clear the 18 Mbps gives the best network performance in terms of bandwidth-delay metrics (file transfer latency was less than 10 ms which is the recommended value for AMI and SM applications [4, 9]) and it will be our choice for the rest of this paper (higher data rates were also tested but give unstable performance in the nominated TX power, so that their results were discarded). The listed network traffic values were originated from different protocols in the TCP/IP stack. The major contributor was the application layer traffic in both directions (sent & receive) while other traffic sources such as layer2 packets and OLSR related traffic have much less effect. It is worthwhile to mention that GWR location in the ad hoc network affects seriously on its network traffic and the highest traffic (higher power consumption) was observed in the GWRs nearer to the central server. These GWRs were selected in our experimental model as they represent the worst possible case (from power consumption point of view).

Table 4. Network traffic as a function of data rate

Data Rate (Mbps)	Traffic Sent From GWR Node (kbps)	Traffic Received By GWR Node (kbps)	Total Traffic (kbps)	WLAN Delay (Sec.)	File Transfer Latency (Sec.)
6	55.5	335	390.5	0.00042	0.01
12	78.5	368	446.5	0.00018	0.008
18	78.7	401	479.7	0.00013	0.007

Scenario 2:

In this scenario, the effect of varying the number of served SMs (by each GWR) on the generated network traffic was studied. From Figure 3, it is noted that increasing the number of SMs add more traffic to the system (especially received traffic). Next, we will make use of these traffic patterns in our experimental work in order to estimate the real power consumption by GWR as a result of different network conditions.

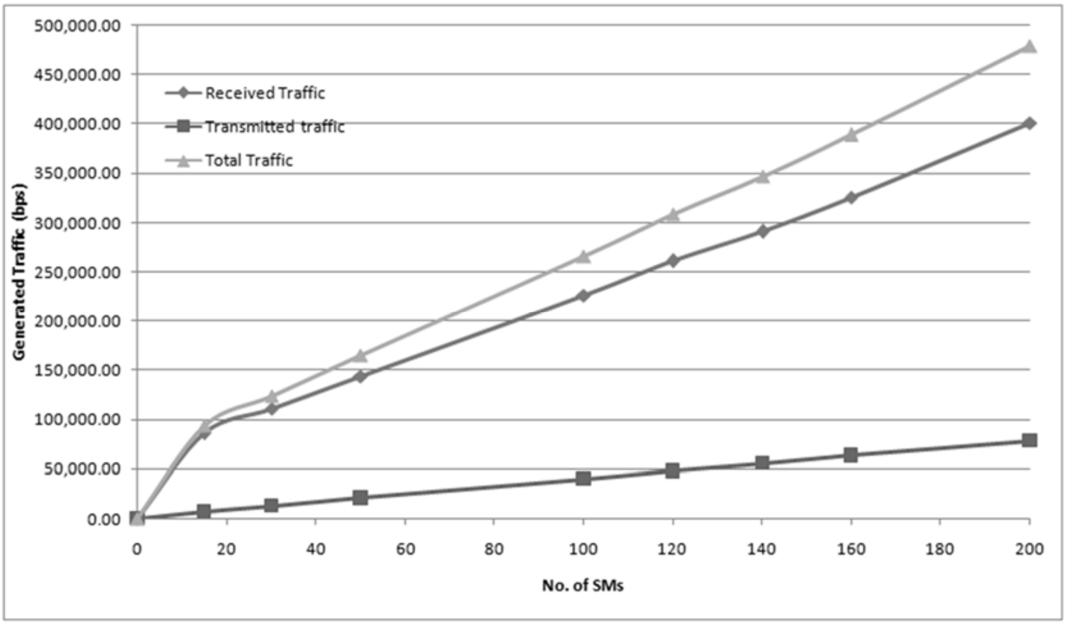


Figure 3. Green AMI traffic

4. Experimental Work

In this section, the different network traffic patterns generated from running the previous simulation model were used in our experimental network. As mentioned earlier, the goal is to generate a realistic network load (as close as possible to the actual circumstances) while measuring the drained current by the Ubicom (GWR) resulting from this network conditions. Our tests includes measuring two quantities:

1. Current drained in Normal Mode: In this mode the Ubicom board and its accessories are working without any power management.
2. Current drained in Sleep Mode: In this mode, the power consumed by the Ubicom platform was governed by a new power management scheme we called Event Driven Duty Cycling (EDDC).

Traditionally, power management protocols used for Wireless Sensor Networks (WSN) can be implemented either as independent sleep/wakeup protocols running on top of a MAC protocol (typically at the network or application layer), or strictly integrated with the MAC protocol itself [18]. Unlike the Wireless Sensor nodes, GWRs must always be ready to receive different packets and cannot be turned OFF entirely. It was noted from our earlier measurements that Ubicom board spends at least 60% of its time in IDLE mode, so that it will be useful to send it to SLEEP mode to save power. The suggested Event Driven Duty Cycling(EDDC) technique makes use of an important feature in Ubicom board "Clock Stop Mode"; in which the system clock may be disabled which disables the CPU core clock and hence, the Ubicom board. When the system clock is disabled, the interrupt logic continues to function, and a Sleep timer may be enabled to keep running. Recovery from clock stop mode (Sleep Mode) to normal execution is possible using Sleep timer interrupts or in response to an external interrupt form WLAN NIC, see Figure 4. This method do not reset the chip, so program execution continues from where it was stopped. This mode sends the Ubicom board only (WLAN NIC is still ON) to power saving mode in which its circuitry (except the External interrupts circuits and the program memory) goes OFF. Whenever an interrupt occurs (due to the reception of a packet by the WLAN NIC), the board wakes up within 3 clock cycles (25 nsec.) to perform the necessary actions, see Figure 4.

The experimental results shown in Figure 5 record the average current drained from the GWR as a function of changing the number of SMs related to each GWR. It is clear that the current drained when working in SLEEP mode is much lower than Normal mode because of excluding the current drained during IDLE state (when the board circuitry consumes power without performing any action).

In order to finalize our design procedure, we need to estimate the required number of paralleled solar panels, number of parallel AA battery pairs and their capacity. We begin our analysis using the following procedure which reflects a realistic power demanding conditions:

1. Figure 6 shows several solar panel tests which were performed in different times in the year in Mosul city/Iraq [14]. The main observations which could be extracted from these experiments indicate that the amount of the electrical current produced by the solar cell panels depends mainly on the number of parallel connected cells, the weather conditions and the day time (effective charging time) period. The maximum working time ***without*** battery cells being charged is 14 hours per day. Meanwhile, it can be shown that the least average charging current (rainy day and 10 hours effective charging time) is 14.4 mA. We will make use of these figures in our planning procedure.
2. In order to determine the battery capacity, we make use of the following relation:

$$\text{Battery Capacity (mAh)} = \text{Current Drained by GWR} \times \text{Maximum Operation Period} \tag{1}$$

3. To determine the necessary number of the paralleled 4-4.0-100 solar panels, we must determine their duties to produce the necessary amount of current for supplying the GWR for the least day period and to charge the batteries at the same time. It was calculated using equation (2) below:

$$\text{No. of Parallel Solar Panels} = \text{SPGWR} + \text{SPBC} \tag{2}$$

SPGWR is the number of solar panels to energize GWR and can be expressed as:

$$\text{SPGWR} = \text{Current Drained by GWR/Current Produced by a Single Solar Panel} \tag{3}$$

On the other hand, SPBC is the number of solar panels to energize the battery cells and can be expressed as:

SPBC = Battery Capacity/(Minimum Day Period × Current Produced by a Single Solar Panel) (4)

Table 5 declares that GWR, when working in SLEEP mode, needs far less number of paralleled solar panels and lower battery capacity to serve different number of SMs. This results prove the effectiveness of the suggested power management scheme to extend the life of the solar energy harvested-battery based GWR and their serviceability which will be reflected positively on building a reliable and available advanced metering infrastructure.

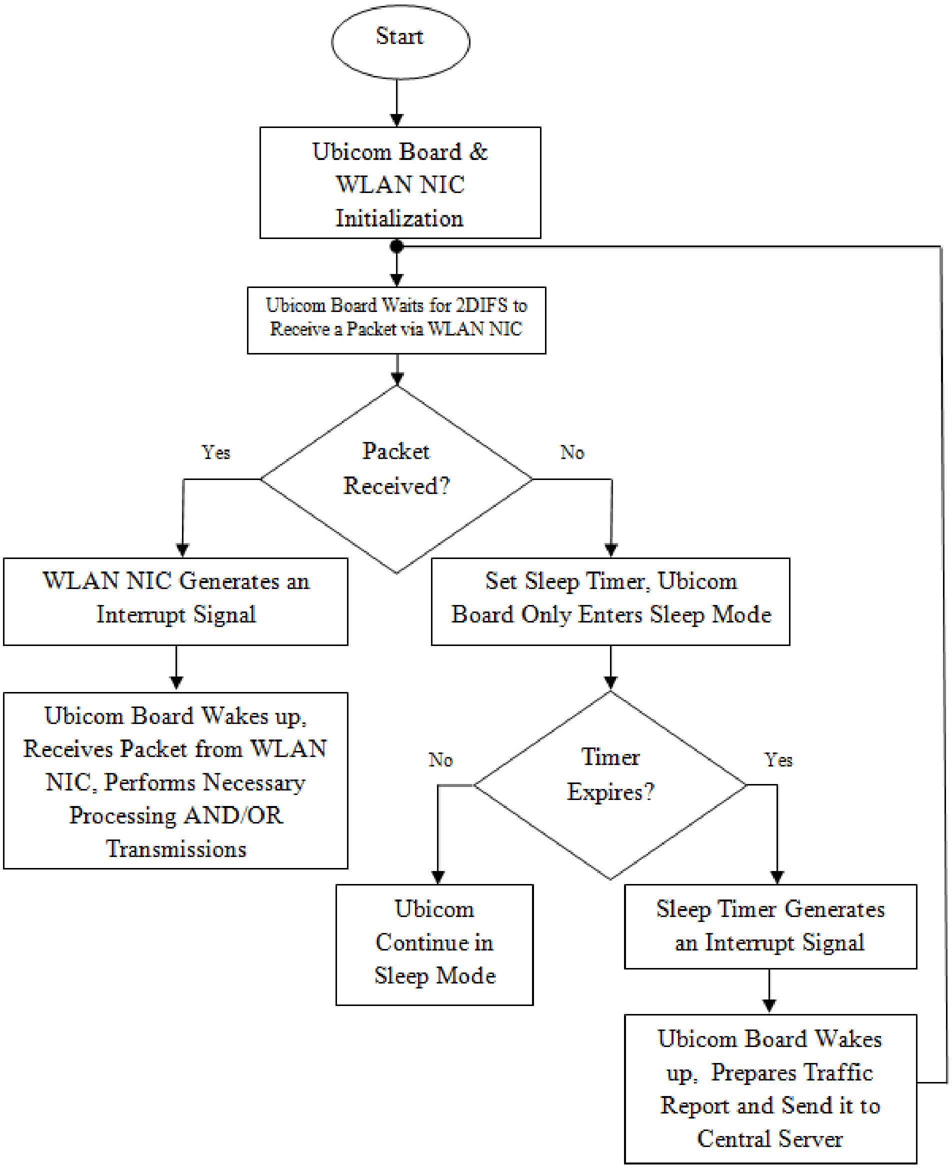

Start
Ubicom Board & WLAN NIC Initialization
Ubicom Board Waits for 2DIFS to Receive a Packet via WLAN NIC
Packet Received?
Yes
No
WLAN NIC Generates an Interrupt Signal
Set Sleep Timer, Ubicom Board Only Enters Sleep Mode
Ubicom Board Wakes up, Receives Packet from WLAN NIC, Performs Necessary Processing AND/OR Transmissions
Timer Expires?
No
Yes
Ubicom Continue in Sleep Mode
Sleep Timer Generates an Interrupt Signal
Ubicom Board Wakes up, Prepares Traffic Report and Send it to Central Server

Figure 4. Flowchart of SLEEP mode

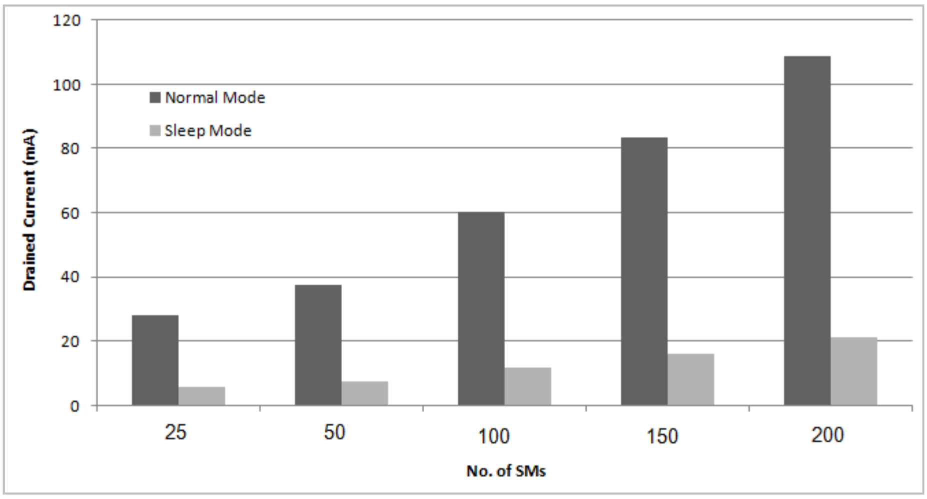
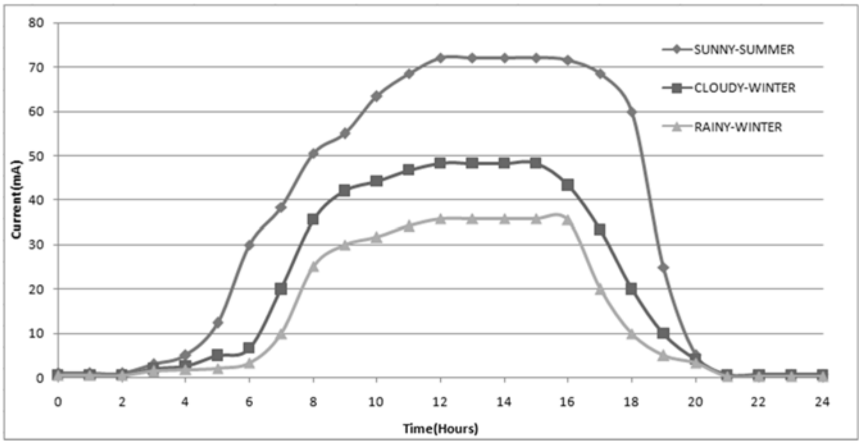
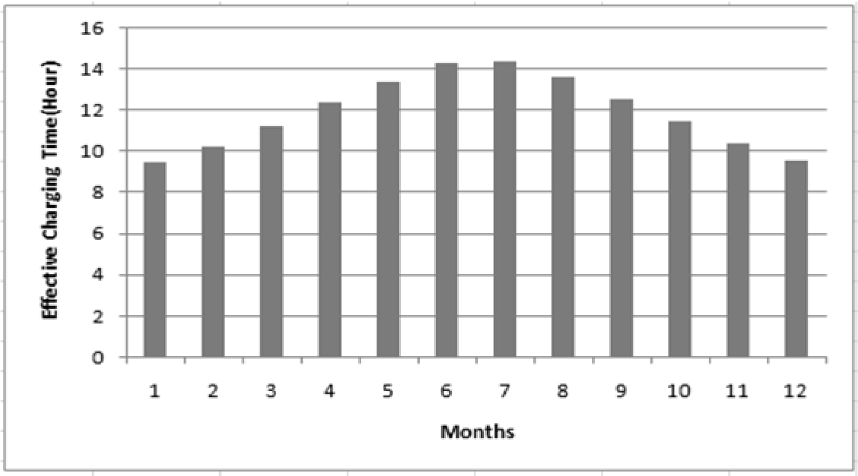


Figure 5. Average current drained for different modes



(a)



(b)

Figure 6. Measured characteristics of the panel: (a) Produced current variation a solar panel in different weather conditions (b) Effective charging time/month

Table 5. No. of solar panels & battery cells in various conditions

Number of SMs served by GWR	Normal Mode		Sleep Mode	
	No. of Parallel Solar Cells	Battery Capacity (mAh)	No. of Parallel Solar Cells	Battery Capacity(mAh)
25	5	392	1	76
50	6	524	1	101
100	10	845	2	162
150	14	1170	3	224
200	18	1526	4	294

5. Security Issues of Green AMI

In order to immunize the proposed green AMI, we will suggest a security model for GWR to protect it against different internal and external threats. The main goal is to protect GWR specific data (needed for its operation) as well as its functionality and accessibility. The suggested GWR security model must responds to many objectives, it should ensure that the administrative information exchanged is correct and undiscoverable (information authenticity and privacy), the source is who he claims to be (message integrity and source authentication) and the system is robust and available (using Intrusion Detection System (IDS)).

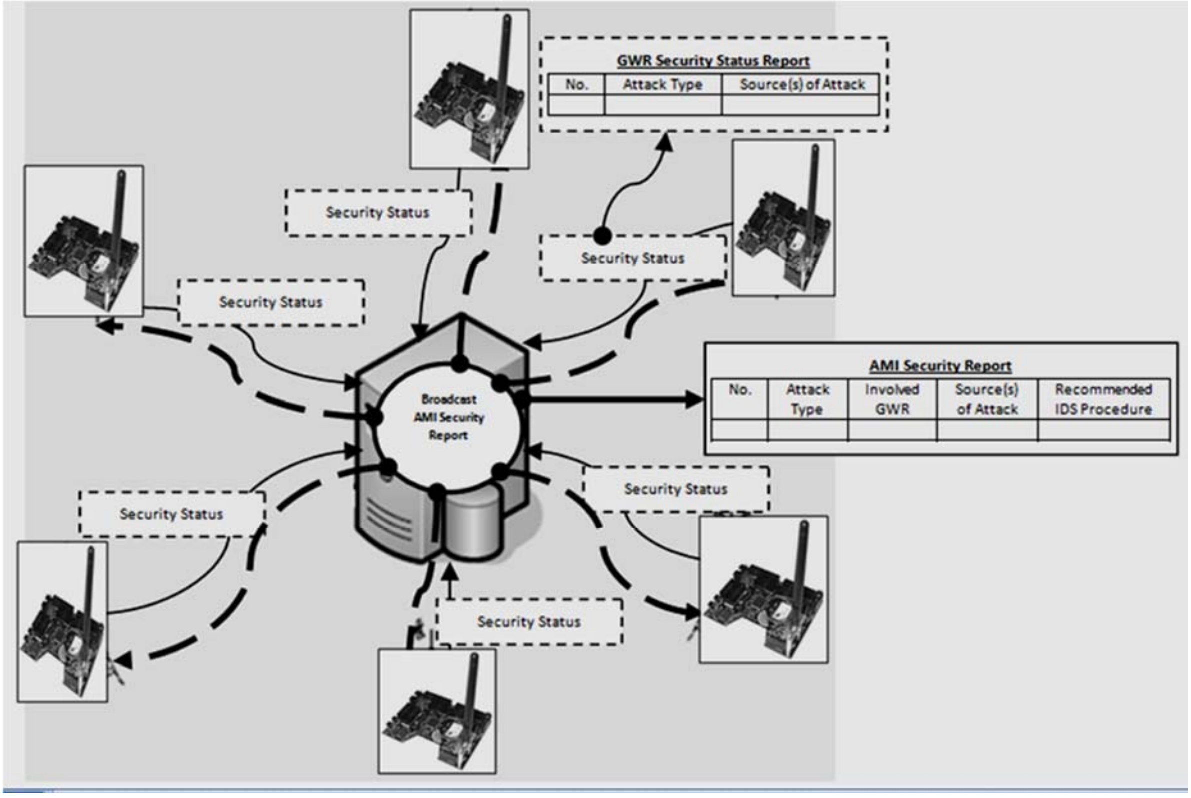
In this paper we are concentrating on attacks perpetrated against the GWR itself as an essential element in the AMI infrastructure. Security threats against GWR can take different forms and originate from different sources. When investigating the possible types of attacks, GWRs are susceptible to a variety of attacks differ in their nature, goals and catastrophic effects. We have made a survey on the possible attacks against GWRs (as a member in an ad hoc network) according to their type and the results of this survey are abstracted in Table 6.

Table 6. The possible attacks against GWR

Attack Type	Description
Denial of service (DOS) Attack	The attacker jams the main communication medium and the network is no more available to legitimate users
Distributed Denial of service (DDOS) Attack	The attackers launch a DOS attacks from different locations
Black hole attack	The attacker can selectively filters or drops the traffic from a particular part of the network
Worm hole attack	Two malicious nodes in a network transfer packets from a private tunnel which they have built by cooperation with each other and if the message passes through this tunnel then a security breach occurs.
Application Attack	The attacker changes the content of the RSU applications and uses it for his own benefits
Timing Attack	Attacks against the timing of a RSU periodic activities
Energy Exhaustive Attack	Sending a high traffic volume to the RSU to exhaustive its stored energy (in the case of a battery based RSUs)

5.1. Embedded Cooperative intrusion detection system

Service availability is an important security issue which means that authorized access of data and other AMI resources is made ready when requested or demanded. This feature can be obtained by protecting the system against the different types of attacks using an Intrusion Detection System (IDS). In order to offer a high level of defense against various attacks and to cope against the limited processing and energy resources in the GWR, we suggest a cooperative IDS approach. In this approach, GWRs do not depend only on their local view to make conclusions about the security status of their network, but also cooperate with their AMI server by exchanging security reports to create a more global and accurate idea about the security situation of the whole network, the possible attacks and their origins. The implementation of the suggested cooperative IDS is shown in Figure 7. In such systems, GWRs play the role of an IDS sensors, they generate "*periodically*" their security status reports then forward them to the AMI server. These reports contains the necessary data about the number, types and sources of attacks against this GWR at that time. On receiving these reports, AMI server accumulates them, then makes the necessary processing to obtain the final report about the security status of this part of the network. Also, AMI server suggests the necessary IDS reactions to accomplish against these attacks and declares them to the GWRs and to the AMI administrator.



GWR Security Status Report

No.	Attack Type	Source(s) of Attack

AMI Security Report

No.	Attack Type	Involved GWR	Source(s) of Attack	Recommended IDS Procedure

Figure 7. Cooperative IDS functionality

In this paper we will adopt a behavioral IDS strategy, which is based on divergence from usual behavior in order to identify attacks through manually defined conditions that explain what a proper operation is and observe any behavior with respect to these restrictions. This technique is easier to be applied in AMIs, since normal behavior cannot easily be districted by machine learning techniques and training. In order to clarify the principles of our cooperative IDS approach, we build a behavioral based IDS to detect two examples of AMI specific attacks: Black hole attack and Energy Exhaustive Attack.

Black hole attack occurs when a compromised node drops a packet that is bound for a particular destination. In this way, an attacker can selectively filter traffic from a particular part of the network. Other possible variations of selective forwarding can involve dropping all packets or randomly dropping packets. Although random dropping is less disruptive, it can also be much harder to reliably detect and trace [19-21].

Detecting black hole and selective forwarding attacks can be a rule on the number of packets being dropped by a GWR (each of the GWRs will apply that rule for itself to produce an intrusion alert). The adopted approach is to set a threshold of the rate at which packets are dropped (we called Recorded Dropping Rate (RDR)), and when this is reached an alarm can be generated (Packets dropped at a lower rate were returned to other reasons such as collisions or node collapse). Here we assume that GWRs are capable of simply observe the activities of their neighbored GWRs to see whether they forward correctly the packets they receive by listening *promiscuously* to their transmissions (promiscuously we mean that since GWRs are within range of each other, they can overhear other nodes traffic). Therefore we need each GWR to keep track of the packets not being forwarded within a predetermined amount of time we called analyzer time slot, during which it creates statistics on the overheard packets. At the end of each time slot an alert may be created according to the threshold condition, which is sent by that GWR to the server as a security report. when the next time slot is started, the same process is repeated periodically, for all GWRs, see Figure 8. The next design concern we need to resolve is who is going to make the final conclusion that a node is certainly an impostor and the procedures should be taken. In this paper, we makes use of a cooperative decision making approach, where the GWRs and their associated AMI server *cooperate* in order to decide whether a definite GWR is launching a selective forwarding attack and take the suitable actions. For instance, if the security reports received by the server states that more than 50% of the neighbored GWRs generate an alert against certain GWR, then the target GWR is regarded as compromised and should be removed from the routing tables of the other GWRs, see Figure 8.

In order to show the importance of removing *black holes* from the AMI infrastructure, we perform the next experiment which deals with the effect of Black Hole attack on GWRs' power consumption and hence its battery life. In this experiment, two variables were changed: the percentage of the GWRs' traffic dropped by its neighbors (due to the Black Hole attack) and the number of retransmission attempts made by the GWR to compensate this dropping. Figure 9 shows the destructive effect of such attack on the drained current and hence the battery life of the GWR as listed in Table 7. These measurements also confirm the importance of our earlier procedure to cope against this type of attack using the suggested cooperative IDS.

It is importance to mention that similar power consumption behavior was observed when the GWR was subjected to the Energy Exhaustive attack (will be illustrated later) because it is based on the same principle, i.e., extra traffic volume to/from a GWR to exhaustive its stored energy.

Algorithm for Black hole attack Detection

```
Parameters Definition
Analyzer Time Slot Counter (ATSC)
Dropped Packets Counter (DPC)
Recorded Dropping Rate (RDR)
Normal Dropping Rate (NDR)
Black hole Detection Threshold (BDT)

GWR Side
{
10      ATSC Initialization
20     ATSC =ATSC+1
GWR records the dropped packet
IF packet is dropped by a neighbored GWR THEN
DPC=DPC+1
ELSE IF ATSC >= Threshold THEN
RDR= DPC/ATSC
ELSE
GOTO 20
ENDIF

IF RDR >NDR THEN
GWR generates a "Black Hole Intrusion" alert and adds it to the security report

GWR updates the routing table to remove the Black hole GWR

ENDIF

GWR Sends its Security Status Report to the AMI Server
GOTO 10
   }

AMI SERVER Side
{
AMI Server receives and analyzes the security reports from the different
GWRs
10  IF "Black Hole Intrusion" alerts for a certain GWR > BDT THEN
    The Server considers this GWR as a Black hole

                The Server sends a security alarm to all GWRs to remove this
GWR from their routing tables
                ENDIF
The Server sends a security status report to all GWRs
GOTO 10
   }
```

Figure 8. The suggested IDS procedure against anti-black hole attack

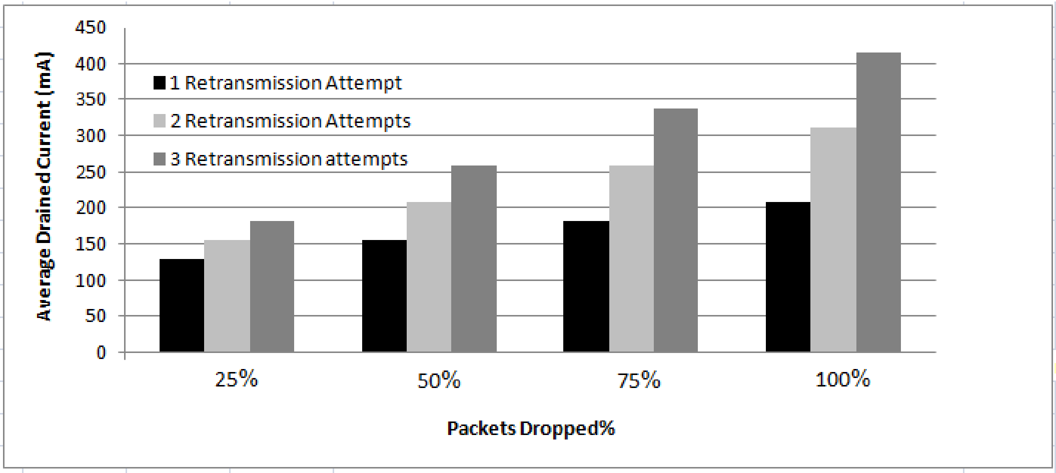


Figure 9. Effect of black hole attack on GWRs' drained current

Table 7. Effect of black hole attack on battery life (2800 mAh AA battery)

Packets Dropped%	Battery Life (Hour) One Retransmission Attempt	Battery Life (Hour) Two Retransmission Attempts	Battery Life (Hour) Three Retransmission Attempts
25%	21.5	17.9	15.4
50%	17.9	13.5	10.8
75%	15.4	10.8	8.3
100%	13.5	9.0	6.7

Energy Exhaustive Attack is a special type of Denial of Service (DoS) attack which is based on sending high traffic volume to the GWR to exhaustive its stored energy (in the case of battery based GWRs) rather than jamming the communication medium. Our approach to defend against this attack is to adopt a proper power management scheme.

In this paper, we need to modify our earlier EDDC technique so that GWR would perform according to its available energy, specifically, the service rate of the GWR is determined as a function of the GWRs' power budget. In this case we need to derive a relation among Duty Cycling periods (Sleep/Active), Average Service Rate (ASR) and the Available Energy (AE). We firstly start by defining the following terms:

- Average Service Rate (ASR) is the average of total traffic (in bps) transmitted from and received by the GWR.
- Duty Cycling Periods: In this paper, time is divided into (1s) slots. Hence, Duty Cycle is the ratio of the active periods to the total slot time.
- Available Energy (AE) is the summation of the residual energy in the batteries from the last day plus the expected energy in the next day.

Our approach involves the following steps (see Figure 10):

In the beginning of each *working day*, GWR calculates the Available Energy (AE) as follows:

$$AE = RE + EE \quad (5)$$

where RE is the Residual Energy from the last day, EE in the Expected harvested Energy in the current day, and RE of the batteries can be found as:

$$RE = (\text{Initial Energy} + I_{in} \times \text{Effective Charging Time}) - I_{out} \times 24 \quad (6)$$

It is obvious that in order to calculate RE, GWR needs to measure the current flowing to/from the batteries (I_{in} & I_{out} respectively) during the whole working day. We make use of the Ubicom's integrated 12 bit A/D convertor to achieve this task. Our measurement process involves taking a sample every one second, then calculating the average current values in each hour. Effective Charging Time represents the number of hours in which the current drained from the solar panels is greater than zero.

In order to estimate the value of EE, we suggest that the AMI server should broadcast (to all GWRs) the weather forecasts and the effective charging time for this particular day. This weather report includes the expected weather (Sunny, Cloudy or Rainy) and the number of useful charging hours. As a function of current measurement procedure mentioned earlier, GWR can determine the current value expected according to its historically recorded current values in a similar weather conditions, and hence, EE could be calculated as:

$$EE = \text{Average Expected Current} \times \text{Effective Charging Time} \tag{7}$$

The next step is to calculate the Average Service Rate (ASR) of the GWR in this particular day according to the value of AE. The relation between Service Rate (SR) and AE could be derived by determining the power consumed according to GWR activities as follows:

$$AE = E_{TX} + E_{RX} + E_{Proc.} + E_{Sleep} \tag{8}$$

E_{TX} is the energy consumed during data transmission and can be expressed as:

$$E_{TX} = I_{TX} \times \text{bit time during transmission} = SR(I_{TX}/n \times \text{Data Rate}) \tag{9}$$

where (SR) is the service rate, (I_{TX}) is the current drained by WLAN NIC when working in TX mode and (n) is the ratio between RX to TX periods.E_{RX}, is the energy consumed during data reception and can be expressed as:

$$E_{RX} = I_{RX} \times \text{bit time during reception} = SR(I_{RX}\times(n-1)/n \times \text{Data Rate}) \tag{10}$$

where (I_{RX}) is the current drained by WLAN NIC when working in RX mode. $E_{Proc.}$ is the energy consumed during data processing and can be expressed as:

$$E_{Proc.} = SR\ (\ I_{Proc.}/\text{Data Processing Speed of the GWR}) \tag{11}$$

where ($I_{Proc.}$) is the current drained by Ubicom Motherboard during processing. E_{Sleep} is the energy consumed during Sleep mode and can be expressed as:

$$E_{Sleep} = SR((I_{Sleep} \times \text{Data Processing Speed} - I_{Sleep})/\ \text{Data Processing Speed}) \tag{12}$$

where (I_{Sleep}) is the current drained by Ubicom Motherboard in Sleep mode.

The next step is to calculate the Average Service Rate (ASR) of the GWR in this particular day according to the value of AE as:

$$ASR = 0.5\ (AE - d)\ /\ (a + b + c - e) \tag{13}$$

where

$a = (I_{TX}/n \times \text{Data Rate})$
$b = (I_{RX}\times(n-1)/n \times \text{Data Rate})$
$c = (\ I_{Proc.}/\text{Data Processing Speed of the GWR})$
$d = I_{Sleep} \times 24$
$e = (I_{Sleep}/\ \text{Data Processing Speed})$

The last step is to calculate the Sleep period in each time slot (i.e., 1s) as:

$$\text{Average Sleep Period} = 1 - (\text{ASR}/\text{Data Rate}) \tag{14}$$

After performing the above calculations, GWR can begin its work safely. As each time slot is divided into Active and Sleep periods, Ubicom's enters the sleep period first. At the same time, different types of data packets are accumulated in the WLAN NIC buffers (which is still ON). When Active period starts, Ubicom board wakes up and begin to process the packets received from its WLAN NIC, see Figure 10.

CDC Power Management Algorithm

Parameters Definition

Available Energy (AE) Residual Energy (RE) Expected Energy (EE) Average Service Rate (ASR) Average Sleep Period (ASP) Sleep Tim (ST)	Energy consumed in TX mode (E_{TX}) Energy consumed in RX mode (E_{RX}) Energy consumed in processing mode ($E_{Proessing}$) Energy consumed in sleep mode (E_{Sleep}) (n) is the ratio between RX and TX Traffic Current drained during TX mode (I_{TX})	Current drained during RX mode (I_{RX}) Current drained during Processing mode ($I_{Proc.}$) Current drained during Sleep mode (I_{Sleep})

Sleep Period Calculation

```
{
GWR receives weather forecasts & effective charging time from the AMI Server
GWR calculates EE = Average Expected Current × Effective Charging Time
GWR calculates AE = RE + EE
GWR shares out AE to the different tasks as: $AE = E_{TX} + E_{RX} + E_{Proessing.} + E_{Sleep}$
GWR calculates    $a = (I_{TX}/n \times \text{Data Rate})$ ; (a) denotes the transmission process contribution in the Energy budget
GWR calculates    $b = (I_{RX} \times (n-1)/n \times \text{Data Rate})$ ; (b) denotes the reception process contribution in the Energy budget
GWR calculates    $c = (I_{Proc.}/\text{Data Processing Speed of the GWR})$ ; (c) denotes the processing process contribution in the Energy budget
GWR calculates    $d = I_{Sleep} \times 24$ ;
GWR calculates    $e = (I_{Sleep}/\text{Data Processing Speed of the GWR})$ ;
                  (e, d) denotes the sleep process contribution in the Energy budget
GWR calculates $ASR = 0.5\,(AE - d) / (a + b + c - e)$ ; calculation of Average Service Rate
GWR calculates $ASP = 1 - (ASR/\text{Data Rate})$ ; calculation of Average Sleep Period
GWR performs mapping to the service rate according to the applied load        }
```

Operation Mode

```
{
10          GWR sets sleep timer to ST
Ubicom board only enters sleep mode
20            ST=ST-1
WLAN NIC stores the incoming packets in its buffers
IF ST = 0 THEN
Sleep timer generates an interrupt signal
Ubicom board wakes up
Ubicom receives the stored packets from WLAN NIC
Ubicom performs the necessary processing and/or transmission tasks
GOTO 10
ELSE
Ubicom Continues in the Sleep Mode
GOTO 20
ENDIF
    }
```

Figure 10. The suggested anti-energy exhaustive attack IDS procedure

The suggested power management technique was tested to evaluate its ability to manage the energy consumed by GWR, and hence to defend against unmanaged network traffic conditions (such as those result from the Energy Exhaustive Attack)**.** The Purpose of these experiment is to examine the ability of the suggested method to adapt against different working conditions wherein different Available Energy (AE) levels were assumed. Table 8 lists the different values of ASR and ASP obtained from these scenarios, where Residual Energy (RE) stands for a sample case of 50% battery charging percentage and (N) is the number of paralleled solar panels. It is noted that the suggested power management technique was able to adapt its performance according to the available energy levels and hence continue to function in a pre-managed and planned manner which extends the battery life of the intended GWR.

Table 8. ASR & ASP values under different conditions

RE (mAh)	N	Weather Condition	AE (mAh)	ASR (Mbps)	ASP (s)
50%	1	Sunny	1910	2.98	0.83
50%	1	Cloudy	1666	2.6	0.85
50%	1	Rainy	1558	2.43	0.86
50%	3	Sunny	2930	4.57	0.74
50%	3	Cloudy	2199	3.43	0.81
50%	3	Rainy	1875	2.93	0.83
50%	6	Sunny	4460	6.96	0.61
50%	6	Cloudy	2999	4.68	0.73
50%	6	Rainy	2350	3.67	0.79

5.2. Securing GWR Functionality

The different transactions among the AMI server and its associated GWRs are susceptible to many type of attacks and care must be paid to immunize the messages and their origins against them. We suggest the following methods in order to obtain:

- Bidirectional entity authentication between the AMI server and a GWR.
- All the packets (related to the transactions among AMI nodes) are encrypted and sent together with their HMAC in order to obtain message confidentiality, authentication and integrity.
- A new method was suggested to discover malicious or misbehaved GWRs.

Public key encryption methods consumes more resources and needs high processing capabilities to perform their calculations, so that we decided to use it only in the procedures which require short packets. We suggest Advanced Encryption Standard (AES) for other encryption purposes, however, different sets (or pairs) of AES keys are needed to encrypt the packets in the various sessions. Table 9 summarizes the required encryption keys, their purpose and source-destination pairs. We assume that GWR has a tamper-proof device for storing the values of these keys and they were pre-injected into each GWR prior to installing them in the field

5.2.1. Bidirectional Entity Authentication

Prior to accepting the packets sent by different GWRs, AMI server must check the identity of the sender. This can be done by adopting a particular challenge response procedure suggested in this paper, see Figure 11. The challenge is a time-varying value which is a random number and a timestamp which is sent by a GWR. We called this procedure a "bidirectional" because it confirms AMI administrator identity to the GWR and vice versa. This method assumes that the clocks of

Table 9. The required key groups

Key Name	Purpose	Source	Destination
Keys group1 (Multiple AES keys, one for each GWR)	To encrypt GWRs' security status reports	Each GWR has a different AES key	AMI server
AES Key2 (one key)	To encrypt AMI server security reports	AMI Server	All GWRs
Keys group3 (each node has a puplic/private keys pair)	Bidirectional entity authentication	AMI server	Certain GWR
		Certain GWR	AMI server

both sides are synchronized and they also have synchronized and equivalent pseudo random number generators (having the same code functionality, their seeds are equal and generate their outputs at the same time intervals). The challenge/response begin when a GWR sends an encrypted packet contains a generated random number (RND1) and a timestamp (T1). This arrangement proves the identity of the GWR in several aspects:

1. The value of RND1 is already known by the server because its pseudorandom number generator is synchronized with that of the GWR. Only this particular GWR can generate this value at that time. The server checks the value of RND1 which is the first prove of the GWR identity.
2. The value of T1 is a time stamp (represents the time value in the GWR side) which is synchronized with the server clock. This arrangement prevents reply attack and can be considered as the second prove of the GWR identity.
3. This short packet is encrypted firstly using the private key of the GWR itself, then with the public key of the server. This procedure guarantees that the packet can be decrypted only by the server (because it was encrypted using its public key) and at the same time proves of the GWR identity (as it was encrypted using the private key of the GWR).
4. If the request passed the identity checking procedure, then the server accepts the connection and sends a similar packet containing the next random number, so that its identity is also proved to the GWR.

5.2.2. Bidirectional Message Confidentiality, Integrity & Authentication

In order to obtain Confidentiality, Integrity & Authentication for the data packets and the security reports transacted between the AMI server and each GWR, the packets transferred between them are encrypted (using a secret 128 bit AES key) and sent together with their Hashed Message Authentication Code (HMAC), see Figure 12. HMAC creates a nested MAC by applying a keyless hash function (Secure Hash Algorithm 2 (SHA2) in our case) to the concatenation of the message and a symmetric key. A copy of the symmetric key is prepended to the message. The combination is hashed and the result of this process is an intermediate HMAC which is again prepended with the same key, and the result is again hashed using the same algorithm. The final result is a HMAC. The receiver receives this final HMAC with the encrypted message and creates its own HMAC from the received message and compares the two HMACs to validate the integrity of the message and authenticate the data origin. Although Figure 12 shows the data transaction from the server to a GWR, this procedure was implemented in both directions to protect the whole session.

In order to measure the additional delay added to the packet creation procedure as a result of applying these security methods, several tests were performed to determine the Ubicom's performance for AES encryption/decryption and HMAC (SHA2) for different packet lengths as shown in Figure 13.

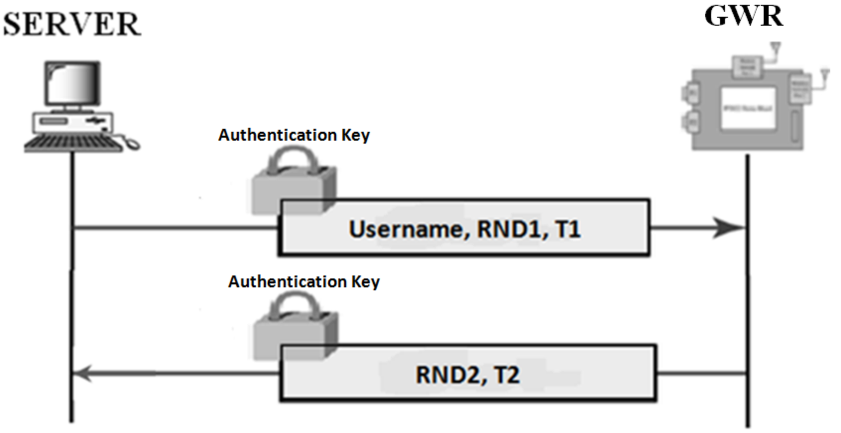


Figure 11. The suggested bidirectional entity authentication

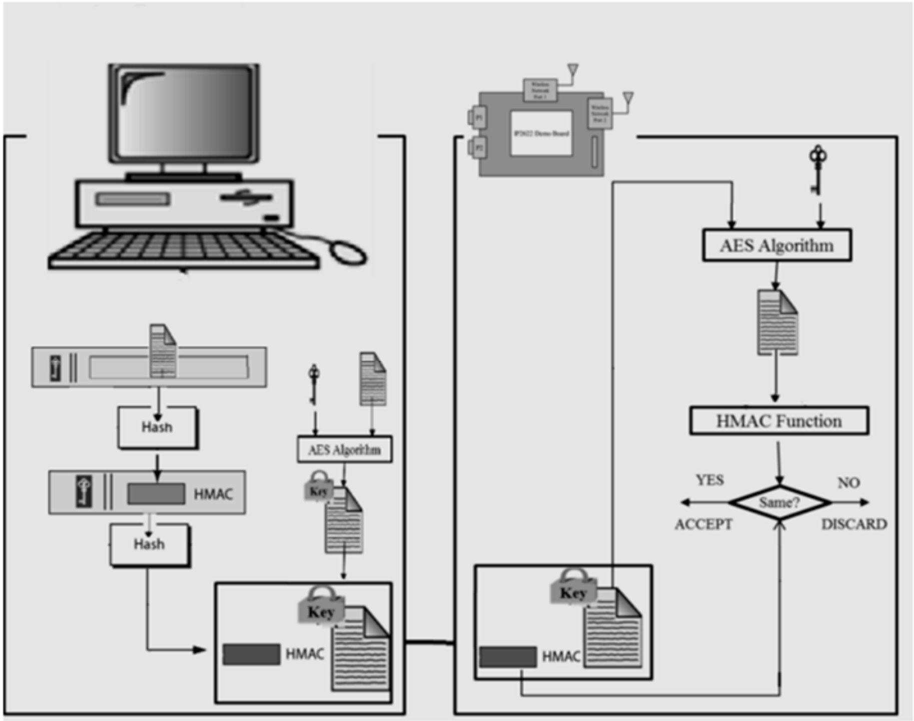


Figure 12. The suggested bidirectional message confidentiality, integrity & authentication procedure

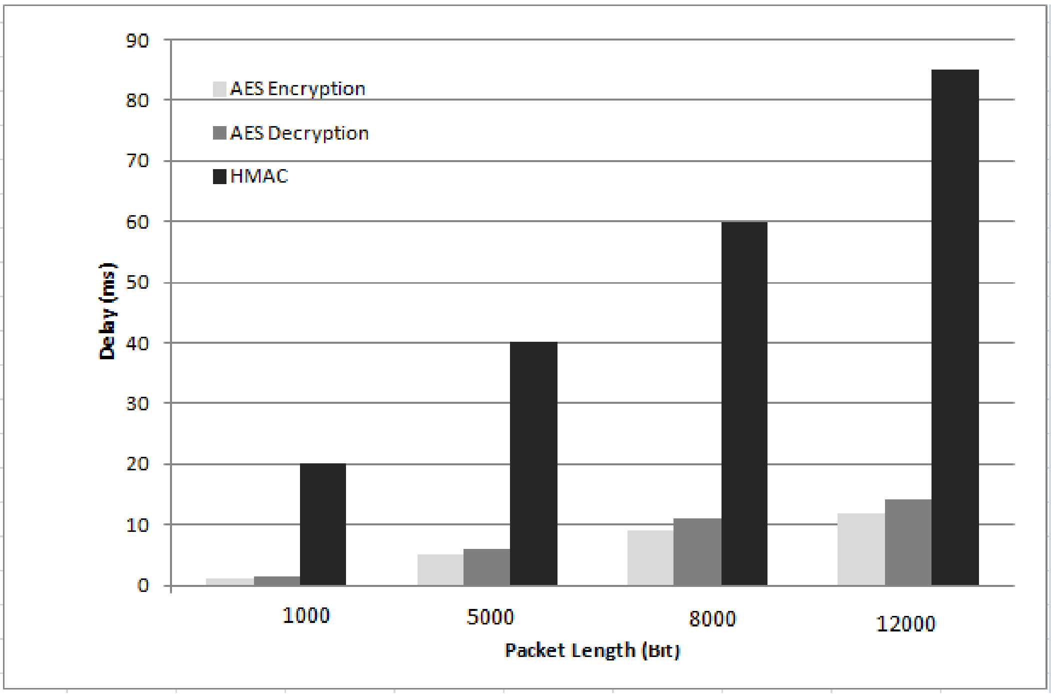


Figure 13. Ubicom's performance for AES encryption/decryption and HMAC (SHA2) for different packet lengths

5.2.3. Malicious or Misbehaved GWRs Detection

In real world, GWRs can be susceptible to physical attacks by malicious entities, or they might simply misbehavior. In order to discover such a GWRs, we suggest the following procedure:

1. In each GWR, there is a long period pseudo random number generator (PRNG) routine. Another identical copy of this PRNG exists in the AMI server.
2. Each pair of these PRNGs are firstly synchronized off-line prior to installing the GWR in the field. Synchronization procedure includes feeding the two routines with the same seed values, then beginning the random numbers generation procedure until they produce the same sequence. This initialization point is saved in the GWR and the server and added to the (Factory Default Settings) to be used later when resetting the GWR.
3. At this point, the two PRNGs are ready to generate synchronized random numbers which will be used for different purposes such as generating the random number used in the challenge response procedure mentioned earlier or to check the functionality of a certain GWR.
4. In order to check GWR functionality, AMI server and their associated GWRs perform periodic synchronization tests or in response to a security report about misbehaving or malicious GWR. These tests begin from the server side and involves sending an encrypted challenge packet (similar to that shown in Figure 11 to the GWR. This packet contains a sequence of random numbers generated by the PRNG routine in the server side and a time stamp. On receiving this packet, the GWR performs the identity check procedure mentioned earlier and generates the next sequence of numbers and send them (together with a time stamp) back to the AMI server.

If the receiver was a malicious or faulty GWR, it will neither be able to decrypt the challenge packet, nor be able to generate the next correct sequence of random numbers. In this case, the AMI server broadcasts an encrypted security report to all GWRs about the discovery of a malicious GWR with its details.

6. Conclusion

This paper presents a design methodology for solar cell energy harvesting Advanced Metering Infrastructure(AMI). The main player of such infrastructure are Green Wireless Routers (GWRs), which are important devices and play an important role in the AMI networking. The continuous operation of these devices guarantees the success of the AMI existence goals. On the other hand, the ability to harvest energy from the environment represents an important technology area that promises to eliminate wires and battery maintenance for AMI applications and permits deploying self powered GWRs. The integration between these technologies and the wise management of the power resources creates a solid foundation to establish a reliable Advanced Metering Infrastructure. In addition, it is essential to protect the GWRs against various types of internal and external threats. The proposed defense strategies took into account the embedded nature of a GWR and hence the recommended solutions make a compromise between highly secured and good performed system.

References

[1] Kolhe, M., 2012. Smart Grid: Charting a New Energy Future: Research, Development and Demonstration. *The Electricity Journal*, 25, 2: 88-93. doi: 10.1016/j.tej.2012.01.018.

[2] Wang, W., Xu, Y., Khanna, M. 2011. A Survey on the Communication Architectures in Smart Grid. *Computer Networks*, 55, 15: 3604–3629. doi: 10.1016/j.comnet.2011.07.010.

[3] Güngör, V. C., Sahin, D., Kocak, T., Ergüt S., Buccella C., Cecati C., and Hancke G. 2011. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Transactions on Industrial Informatics*. 7, 4: 529–539. doi: 10.1109/TII.2011.2166794.

[4] Hamlyn, A., Cheung, H., Mander, T., Wang, L., Yang, C. and Cheung, R. 2008. Computer Network Security Management and Authentication of Smart Grids Operations. In 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, USA, July 20-24, 2008. doi: 10.1109/PES.2008.4596900.

[5] Ayday, E. and Rajagopal, S. 2011. Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks. In *Proceeding of 2011 IEEE Consumer Communications and Networking Conference*, Las Vegas, USA, January, 9-12: 1161–65. doi: 10.1109/CCNC. 2011.5766359.

[6] Khurana, H., Bobba, R., Yardley, T., Agarwal, P. and Heine, E. 2010. Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols. In 43rd Hawaii International Conference on System Sciences, Koloa, Hawaii, USA, January 5-8, 2010: 1–10. doi: 10.1109/HICSS.2010.136.

[7] Efthymiou, C. and Kalogridis, G. 2010. Smart Grid Privacy via Anonymization of Smart Metering Data. In *Proceedings of 2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, October 4-6, 2010: 238–43. doi: 10.1109/ SMARTGRID.2010.5622050.

[8] Wicker, S. and Thomas, R. 2011. A Privacy-Aware Architecture for Demand Response Systems. In *Proceedings of the 44th Annual Hawaii International Conference on System Sciences*, Koloa, Kauai, Hawaii, USA, January 4-7: 1–9. doi: 10.1109/HICSS.2011.24.

[9] Mehra, T., Dehalwar, V., Kolhe M. 2013. Data Communication Security of Advanced Metering Infrastructure in Smart Grid. In *Proceedings of Fifth International Conference on Computational Intelligence and Communication Networks*, Mathura, India, September 27-29, 2013: 394-399. doi: 10.1109/CICN.2013.87.

[10] Yan, Y., Hu, R. Q., Das, S. K., Sharif, H., and Qian, Y. 2013. An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid. *IEEE Network*, 27, 4: 67-71. doi: 10.1109/MNET.2013.6574667.

[11] Bartoli, A., Hernandez-Serrano, J., Soriano M., Dohler, M., Kountouris, A., Barthel, D. 2010. Secure Lossless Aggregation for Smart Grid M2M Networks. In *Proceedings of 2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, October 4-6, 2010: 333-338. doi: 10.1109/SMARTGRID.2010.5622063.

[12] Madava, D. V., Fafoutis, X., Andersen, C. B., Dragoni, N. 2013. Medium Access Control for Thermal Energy Harvesting in Advanced Metering Infrastructures. In *Proceeding of EuroCon 2013*, Zagreb, Croatia, July 1-4, 2013: 291-299. doi: 10.1109/EUROCON. 2013.6624999.

[13] Tan, O., Gündüz D., and Poor, H. V. 2013. Increasing Smart Meter Privacy through Energy Harvesting and Storage Devices. *IEEE Journal on Selected Areas in Communications*, 31, 7: 1331-1341. doi: 10.1109/JSAC.2013.130715.

[14] Ali, Q. I. 2011. Design & Implementation of a Mobile Phone Charging System Based on Solar Energy Harvesting. *Iraqi Journal for Electrical And Electronic Engineering*, 7, 1: 69-72. Retrieved from http://www.ijeee.org/volums/volume7/IJEEE7PDF/Paper713.pdf.

[15] IP2022 Ubicom Data Sheet, WWW.Ubicom.com.

[16] Ali, Q. and Faher, F. 2013. Evaluation of Routing Protocols of Wireless ad hoc for AMI Systems Using OPNET Simulator. 2nd Scientific & Engineering Conference, College of engineering, Mosul University, Mosul, Iraq, November 16-19, 2013.

[17] Lin, T. 2004. "*Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications*". Internal report, Computer Engineering Department, Virginia Technical University.

[18] Anastasi, G., Conti, M., Francesco, M., and Passarella, A. 2009. Energy Conservation in Wireless Sensor Networks: A Survey. *Ad Hoc Networks*, 7, 3: 537–568. doi: 10.1016/ j.adhoc.2008.06.003.

[19] Ali, Q. I., Lazim, S., and Fathi, E. 2012. Securing Wireless Sensor Network (WSN) Using Embedded Intrusion Detection Systems. *Iraqi Journal for Electrical And Electronic Engineering*, 8, 1: 54-64.

[20] Ali, Q., and Lazim, S. 2012. Design and Implementation of an Embedded Intrusion Detection System for Wireless Applications. *IET Information Security*, 6, 3: 171-182. doi: 10.1049/iet-ifs.2010.0245.

[21] Erritali, M, El Ouahidi, B. 2013. A Survey on VANET Intrusion Detection Systems. In *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics*, Rhodes Island, Greece, July 16-19, 2013: 66-69.