The use of RC4 Encryption for Smart Meters

Lincoln Kamau, Philip Kibet, Christopher Maina

***Abstract*—**The electrical power grid is undergoing improvements and is being transformed to theSmart Grid. Smart Grid makes use of two way flow of power and information to better monitor, plan and control the electrical power grid. Advanced communication allow for better service delivery, faster problem detection and correction, and more efficient distribution. However, the same heavy reliance on data that makes smart grid possible is the same source of its vulnerability: cyber attacks and privacy leakages. By accessing information on monitoring such as a household's power usage, one candeduce when the owners of a home are present and even what electrical equipment they have. Such privacy leakages could be used in planning a break-in. To overcome this, we examine the use of encryption on smart meter data. RC4 stream cipher is used. We show that due to its low computational resources, RC4 is a suitable candidate for encryption.

***Keywords*—**Cyber security, Encryption, Privacy, Smart meter.

I. Introduction

THE traditional electrical grid is in the process of being upgraded to a better system known as the Smart Grid. The integration of modern telecommunication systems makes operations run more effectively. Through utility companies and consumers exchanging more data, power delivery is better planned, monitoring improves and faults can be corrected faster. As a result, there are less transmission losses, power outages, and CO_2 emissions.

Various players are involved in Smart Grid, as shown in Fig. 1. Communication between the various parties involved is crucial to enable all the parties to operate effectively.

Smart Grid makes it possible to have Demand Side Management (DSM). DSM is where the demand for power is altered, so as to better match the supply. Loads are shifted from peak to off-peak periods, thus increasing the utilization of power generation plants. Significant cost savings result, since DSM would reduce the dependence on peaker plants. Peaker plants are non-renewable power generation sources switched on to meet a brief shortfall in supply [1]. They are costly because they are only used for a small percentage of time, i.e. during peak demand.

DSM implementation requires various sensors and advanced measurement and control devices, and much more sophisticated energy metering and trading functions [3]. Smart Grid's enhanced meter readings allows for this.

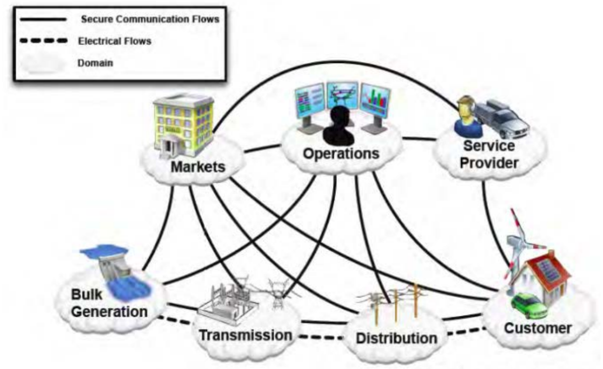

Fig. 1: Interaction of Actors in different Smart Grid domains through Secure Communication Flows[3]

However, the same source of its strength is also smart grid's source of vulnerability. With more data being sent, there is agreater threat in terms of cyber security and privacy invasion. When data consists of control and monitoring information of a system with many users, its protection becomes more crucial.

Cyber attackers can cause great damage to the grid by interfering with the data that is being sent between the consumer and utility. A hacker could corrupt data and cause the system to respond in unexpected ways (e.g. power outage). Crucial data could be delayed (e.g. fault response) leading to a system failure. Billing information could be altered, leading to massive energy theft.

Privacy leakage is a major problem for Smart Grid. A household can be monitored simply by analyzing how power consumed over time. Detailed consumption data would facilitate the creation of users' lifestyle profiles, with information such as when they arrive home, when they eat, etc [4]. The electrical devices within a household can also be identified, based on the pattern of how they consume power. Fig. 2 illustrates how this can be done from a typical household's electrical consumption data.

Such information can lead to great harm if it falls in the hands of robbers as it would be used to plan a break in. For the smart grid to be deployed successfully, cyber security and privacy concerns need to be addressed.

Adopting standard methods used in computer security may not be straight forward because Smart Grid devices use embedded systems, which have limited processing power and memory capacity. Furthermore, some applications have very small time allowances (i.e. latency). This paper seeks to examine RC4 encryption algorithm as a possible technique to enhance privacy.

Lincoln Kamau, Department of Telecommunication and Information Engineering, JKUAT (phone: +2540725515904; e-mail: kamaulincoln@jkuat.ac.ke).

Philip Kibet, Department of Telecommunication and Information Engineering, JKUAT (e-mail: kibetlp@jkuat.ac.ke).

Christopher Maina, Department of Electrical and Electronic Engineering, JKUAT (e-mail: cmaina77@yahoo.com).

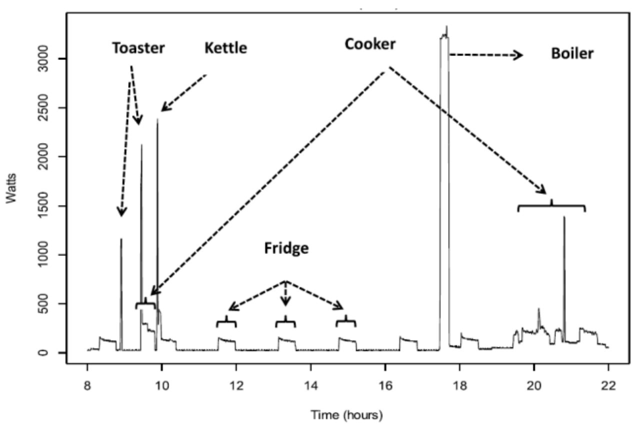

Fig. 2: Household electricity demand profile recorded on a 30-second time base from a one-bedroom apartment[1].

The rest of the paper is organized as follows: Section II looks at recommended security objectives for Smart Grid. Section III looks at cyber threats and privacy leakage. Section IV discusses encryption. The methodology is given in Section V, followed by a discussion of the results in Section VI and a Section VII concludes the paper.

II. Security Objectives

Three cyber security objectives are given for Smart grid by the National Institute of Science and Technology(NIST)[2]: Availability, integrity and confidentiality.

Availability – Timely and reliable access to information. Loss of availability means that information is not delivered and could lead to power disruption.

Integrity – Delivery of information without improper modification or alteration. Loss of integrity could cause incorrect decision making resulting from using wrong or incomplete data.

Confidentiality – Protection of personal privacy and proprietary information from unauthorized access. Loss of confidentiality could expose crucial information to malicious parties.

This paper focuses on the goal of confidentiality.

III. Cyber Threats and Privacy leakage

Cyber attacks can have severe consequences on the smart grid. An attacker could change monitoring or control signals, leading to massive blackouts and damage of equipment. Other attacks could simply involve slowing down the communication in the system leading to system inefficiency. Additionally, utility companies could experience losses from energy theft, which can be done by altering the billing or pricing information.

Attacks can be classified based on what they target, giving us three categories [5]:

Attacks targeting availability, also called denial-of-service (DoS) attacks, attempt to delay, block or corrupt the communication in the Smart Grid.

Attacks targeting integrity aim at deliberately and illegally modifying or disrupting data exchange in the Smart Grid.

Attacks targeting confidentiality intend to acquire unauthorized information from network resources in the Smart Grid.Wire tappers and traffic analyzers fall in this category.

Encryption, which has potential to mitigate attacks on confidentiality, is examined in the next section.

IV. Encryption

Encryption is an elementary cryptographic method used to achieve secure communication and information protection for any information system.

It involves taking a value known as the *plaintext* and using a *key* to convert it to *ciphertext.* The recipient of the message then uses the key to convert the ciphertext back to plaintext. The harder it is for another party to obtain the plaintext from the ciphertext, the better the encryption technique.

Encryption techniques can be divided into two major categories, depending on how the key is used.*Asymmetric key* cryptography uses a different key, public and private key, for encryption and decryption, respectively. In*symmetric key* cryptography, the same key is used.

Asymmetric key cryptography generally requires more computation resources than symmetric key cryptography for long key size (strong security). Thus, the use of asymmetric key encryption may be limited in embedded computing systems.

Symmetric key cryptography requires approximately constant computational resources regardless of the key size; however, it requires secure exchange and update of secret keys among network nodes, thereby complicating the process of key management [5].

Based on these differences, symmetric encryption is a preferred option for smart grid, since it relies on embedded systems and has time critical operations.

Symmetric encryption can further be divided into two groups: block and stream cipher. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.A stream cipher encrypts plaintext one bit or byte at a time.

Stream ciphers are typically faster and use far less code than block ciphers[6].This is advantageous in the smart metering application being examined in this paper.

The RC4 stream cipher algorithm was chosen. Plaintext is encrypted by taking its bitwiseexclusive-OR (XOR) with a stream of bytes. If the plaintext stream is 01010101 and the key is 11011101, then the ciphertext is

plaintext	01010101	
keystream	11011101	XOR
ciphertext	10001000	

Decryption uses the same algorithm:

ciphertext	10001000	
keystream	11011101	XOR
plaintext	01010101	

Fig. 3 shows how stream ciphers operate. The details for the RC4 algorithm, especially the key stream generator, are given in the appendix.

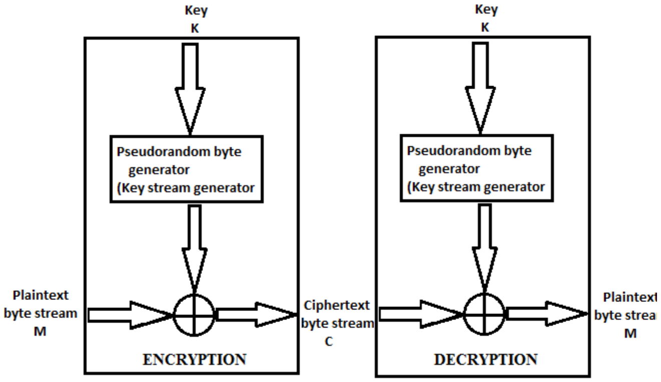
Key
K
Pseudorandom byte generator (Key stream generator
Plaintext byte stream M
Ciphertext byte stream C
ENCRYPTION
Key
K
Pseudorandom byte generator (Key stream generator
Plaintext byte strea M
DECRYPTION

Fig. 3:Block diagram for a stream cipher

V. METHODOLOGY

To illustrate the application of encryption, data on power consumption was encrypted and then plotted on a graph. The goal is to demonstrate that original consumption cannot be determined from resulting graph, without using the key. In addition, timing requirements are examined.

We used an average of daily power consumption data known as day load curves. This was obtained from Kenya's Least Cost Power Development Plan (LCDPD) [7], a document used to guide stakeholders on how to meet energy demands between the years 2011-2031. The graph in Fig. 4was generated by estimating the average demand for January 2010.

This data is an aggregate; it cannot be used to get the details on individual consumption of a user (creating the privacy leakage depicted in Fig. 2). However, it is sufficient to demonstrate the effect of encryption in guarding against privacy invasion.

The pattern for the consumption at different times needs to be hidden from an eavesdropper who may have malicious intentions.

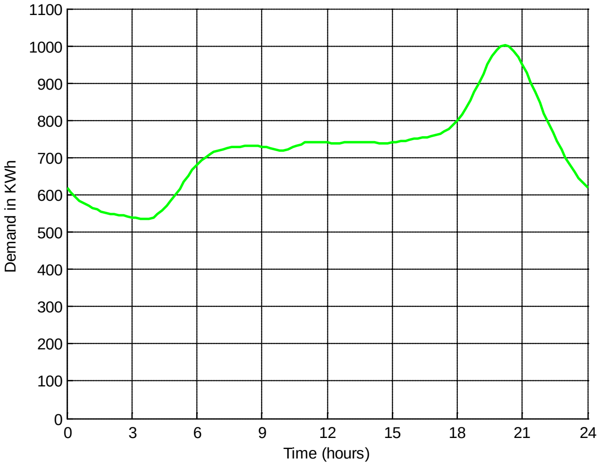

Fig. 4: Plot of Day load curves from LCPDP

RC4 encryption was applied to the data. Different keys were used. Decryption was performed on one to see if the original result would be found. A wrong key was also tried to see if the original data can be retrieved without the right key. Finally, the time for encryption was determined.

The steps followed were:

1. A sampling time of 1 sample per minute was assumed. This sampling time was used to generate Fig. 4.
2. Each value of demand was rounded off to the nearest integer and converted to binary. 10 bits were sufficient for all the values involved.
3. A stream of random bits (key stream) was generated using RC4 algorithm. An arbitrary key of *[3,4,5,12,34]* was used for the encryption.
4. XOR operation was applied to each 10 bit representation of energy demanded using 10 successive bits from the key stream.
5. The encrypted value was converted from binary to decimal representation and the resulting graph was plotted. The result is as shown in Fig. 5.
6. Decryption was performed to confirm that the results would be the same as the original. This is shown in Fig. 6.
7. Different keys were used on the same data of Fig. 4 to give Fig. 7, 8 and 9. The keys used were*[4,99,13,85,210,3]*,*[2,21,200,63,0,0,7]* and *[52,53,54,55,56,57,58,59]*.These keys will be henceforth referred to as Key1, Key2 and Key3 respectively.
8. To demonstrate the effect of using a wrong key, Key1 was used to decrypt the data shown on Fig. 5.
9. Time taken to perform the encryption was determined using Matlab's tool for examining computation, known as Profiler. Five (5) runs were performed to get average computation time.

VI. RESULTS

From the graphs of the encrypted data, privacy is created. Without the key, a person snooping would not be able to obtain power usage data.Once encryption is done, power usage patterns are concealed as shown in Fig. 5.

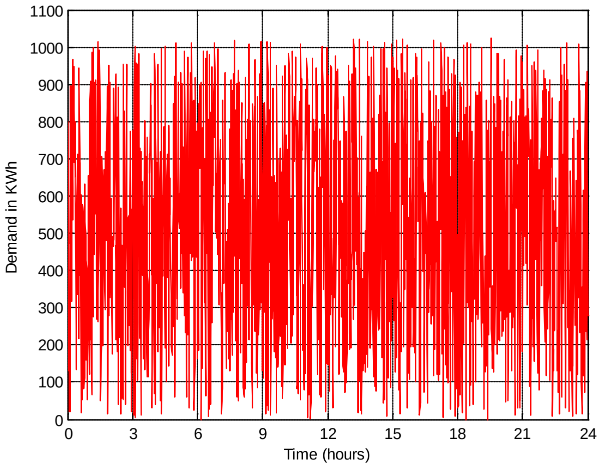

Fig. 5: Encrypted power demand.

Decryption of the above result gave the same results as the original curve. The resulting graph is shown in Fig. 6 and it matches Fig. 4.

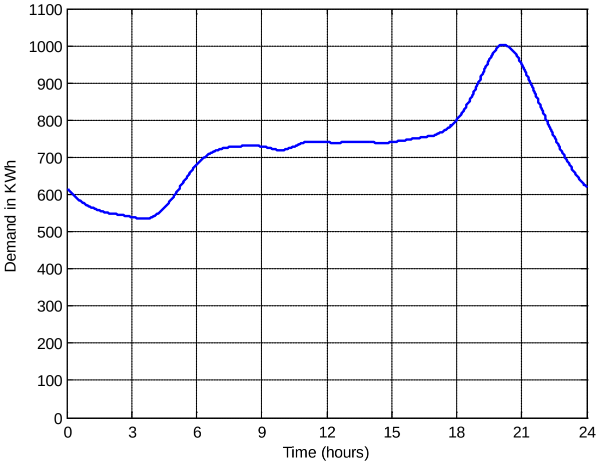

Fig. 6: Results after decryption

Different keys gave different results. For Key1 (i.e. [4, 99, 13, 85, 210, 3]), the graph of Fig. 7 was obtained.

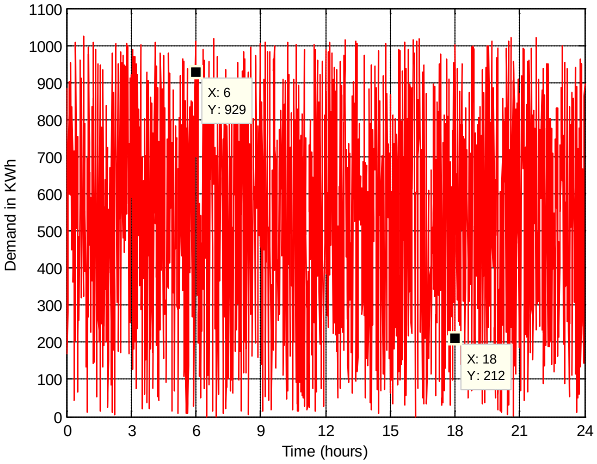

Fig. 7: Encryption using a Key1

To show the differences between the various graphs, a data cursor was placed at x = 6 and x = 18. These times correspond to 6 am and 6 pm respectively. As can be seen from Figures 7, 8 and 9, the value was different for each key. Table 1 gives a summary of these values.

TABLE I
Sample values distinguishing the different keys

Key	Value at x = 6	Value at x = 18
Key1	929	212
Key2	582	56
Key3	612	1023

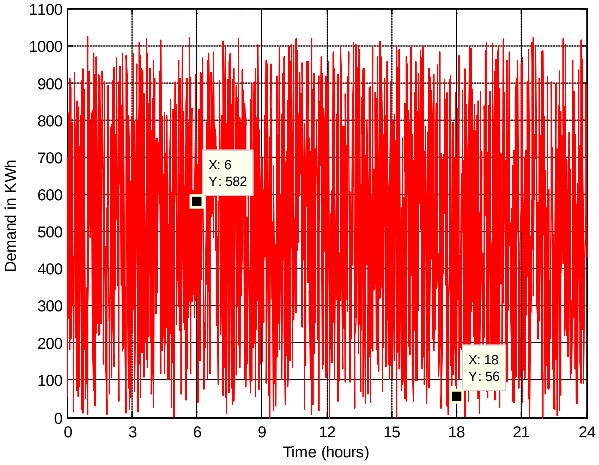

Fig. 8: Encryption using a Key2

Fig. 8 shows the result after using Key2 for encryption, while fig. 9 shows the effect of using Key3. The goal of hiding the information on user data is met.

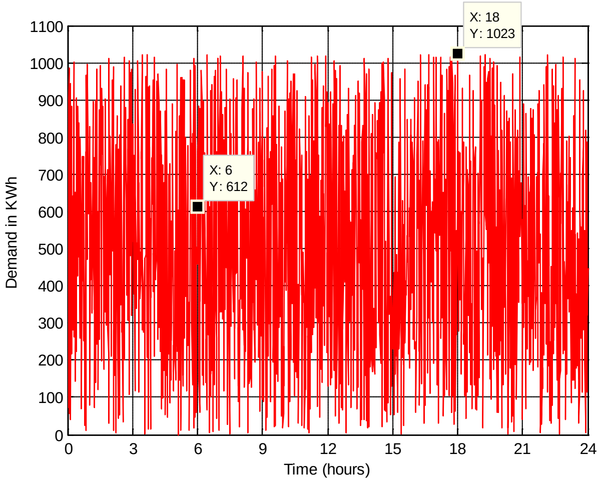

Fig. 9: Encryption using a Key3

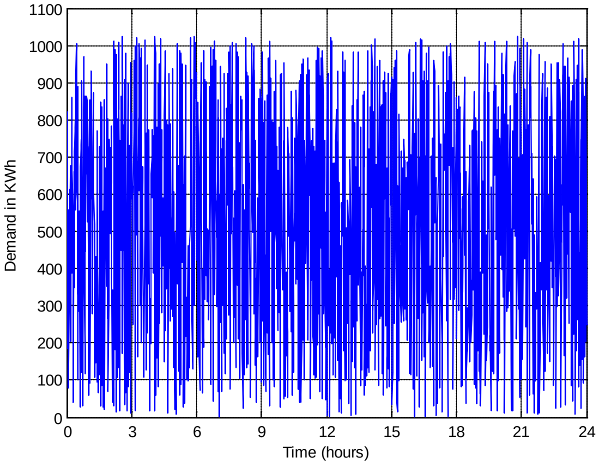

Fig. 10: Decryption using the wrong key.

If the wrong key is used, the results will be unintelligible. To demonstrate this, decryption of fig. 7 was attempted using the key for fig. 6 (i.e. [3,4,5,12,34]). The result was as shown in fig. 10.

A key concern in smart grid communication is the time taken to complete encryption. Delays in some applications can be costly. Most devices also have low capacity.

The encryption operations in this paper were done on Matlab 7.10. A laptop with 2.6 GHz processor and 4.0GB RAM. The time taken was 0.761 seconds (taking an average of 5 runs). Using Matlab’s Profiler, a tool used to determine how much time is spent executing sections of code, over 80% of this time was used in plotting and binary and decimal conversions. In an embedded system, these two operations would be unnecessary. Thus, about 0.15 seconds (20% of total run time) went into encryption of all the data. The data being used simulates a 24 hour period, taking samples each minute – a total of 1440 samples. Thus each sample would take 0.104 ms. Such a delay would be negligible in a metering operation and would not affect system operation.

VII. Conclusion

The importance of privacy cannot be ignored in the deployment of Smart Grid. Too much would be at stake considering the modern age’s dependence on electricity. In a time when cyber crimes are on the rise, ignoring these threats would hinder Smart Grid adoption. Improving privacy would go a long way in building customer confidence in Smart Grid.

The use of RC4 encryption was found to be an effective way of providing privacy involving electrical power usage. Due to the simplicity of the algorithm, the time required to perform encryption would not affect system performance.

Further work would involve implementing this algorithm on a microchip that can be installed in a smart meter. The chip would have fewer overheads than simulation, but also slower processing. An examination of its performance would provide the final verdict on its effectiveness.

Appendix

The RC4, key generation algorithm is as follows [6]:

A variable length key is used to initialize a state vector S, which contains a permutation of the numbers between 0 and 255 in its elements S[0], S[1],…S[255]. For encryption and decryption, a byte k is selected from S in a systematic fashion. The values in S are permuted each time k is chosen. Encryption is then done by finding the XOR of k and the byte to be encrypted (known as the plain text). The pseudo code below gives more details:

Entries of S are initialized with values from 0 to 255. The key is expanded to form a temporary vector T, by repeating the values if necessary. Vector T also has 256 entries, each containing 1 byte.

```
/* Initialization */
for i = 0 to 255 do
    S[i] = i;
    T[i] = K[i mod keylen];
```

T is then used to form an initial permutation of S. This is done by going through all elements of S swapping each using a scheme dictated by T[i].

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i], S[j]);
```

The key is then ignored and subsequent permutations of S are done using the current configuration of S. After reaching S[255], the process starts again from S[0]:

```
/* Stream Generation */
i, j = 0;
while (true)
    i = (i + 1) mod 256;
    j = (j + S[i]) mod 256;
    Swap (S[i], S[j]);
    t = (S[i] + S[j]) mod 256;
    k = S[t];
```

This key, k, is then used to generate the ciphertext, c, by using bitwise XOR with the plaintext, p, i.e. c = k XOR p.

Acknowledgement

The authors would like to acknowledge Jomo Kenyatta University of Agriculture and Technology for facilitating the study.

References

[1] Z. Fan et al., "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities," *Communications Surveys & Tutorials, IEEE*, vol. PP, no. 99, pp. 1-18, 2011.

[2] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for smart grid cyber security," National Institute of Science and Technology, 2010.

[3] G. Strbac, "Demand side management: Benefits and challenges. , 36(12)," *Energy Policy*, vol. 36, no. 12, pp. 4419-4426, 2008.

[4] Alfredo Rial and George Danezis, "Privacy-Preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, Chicago, USA, 2011, pp. 49-60.

[5] Wenye Wang and Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, April 2013.

[6] William Stallings, *Cryptography and Network Security: Principles and Practive*, 5th ed. USA: Prentice Hall, 2011.

[7] Ministy of Energy, Republic of Kenya, "Least Cost Power Development Plan," Nairobi, 2011.