Elysium Journal
Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

A SECURE AND RELIABLE WIRELESS DATA COMMUNICATION FOR SMART GRID

Ms.S.Keerthana[1], Mr.P.Selvakumar[2], Mr. K. Kannan[3]

[1]*PG Student, Department of Electrical and Electronics, R.V.S. College of Engineering &Technology, Dindigul, Tamil Nadu*
E-mail: s.keerthanasankar@gmail.com

[2]*Assistant Professor, Department of Electrical and Electronics, R.V.S. College of Engineering &Technology, Dindigul, Tamil Nadu*
E-mail: selvame_85@yahoo.com

[3]*Assistant Professor, Department of Electrical and Electronics, R.V.S. College of Engineering &Technology, Dindigul, Tamil Nadu*
E-mail: kannankmeped@gmail.com

Abstract: Power system incorporating an information network, is the key to realizing the smart grid vision, but also introduced a number of security issues. Lower the high cost of wireless protocol to communicate the benefits of rapid deployment, shared communication medium, provides the movement; At the same time, it creates a number of security and privacy challenges. In this project, the concept of dynamic secret in order to ensure safety and reliability of data transmitted to a cryptographic system used to design smart grid wireless communication. Update the encryption key will be generated on both sides of the line of contact retransmission. Or to prevent the retransmission of missing keys to the display as an opponent to reach misjudging. Here's a smart grid platform for ZigBee wireless protocol for communication protocol, using the built. And a dynamic secret based encryption demo system is designed based on this platform. ZigBee communication protocol and the project results in the retransmission packet loss will be inevitable and unpredictable show that it is impossible to keep track of enemies, dynamic encryption key renewal. By this method we are able to verify the reliability of the transmitted data. In this scheme, a method of cyclic redundancy check data transmitted and received. The main objective of the project to protect the data from our enemies and make sure there is reliable data transmission.

1. INTRODUCTION

In this project we handle wireless data communication is a problem. Security is a major concern over the wireless network. The present work deals with key management for a secure wireless sensor network security. Ban on conventional public key system because computing power and memory space may be applicable. A lightweight protocol is used to solve this problem. The author has used the random-number key to set the E key management system to participate in the current job security is an important task. It is very difficult to break into rewarding jobs in today's new key that is generated for every pair. In the present work, the encryption and decryption, and changing the cipher key used techniques. By using the linear congruential generator will work in this project is important. The main advantage of this dynamic key encryption and decryption key is surviving after that. Our program provides a secure connection is ideal for small storage cost and in less time. In recent years, another technique known as data security management is key. Another approach is the use of the hash function for data security. Remove the encryption on the system microcontroller and the program in which the simulation was successful in getting the best performance of the system is checked.

2. PROJECT DESCRIPTION

Using the ZigBee protocol for wireless connection to a Smart Grid platform is built. And a dynamic secret based encryption demo system is designed based on this platform. ZigBee communication retransmission and packet loss in the test results show that the inevitable and unpredictable, dynamic encryption key renewal of enemies is impossible to monitor.

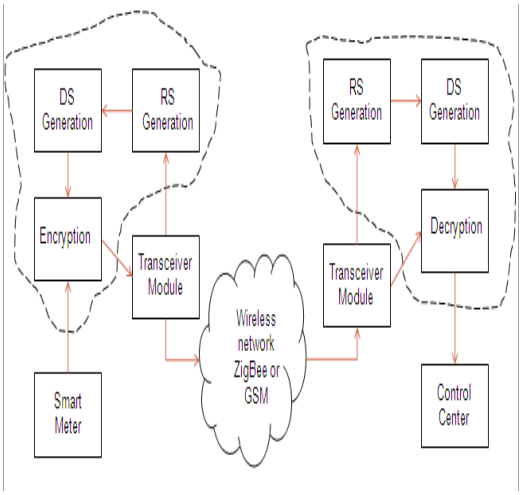
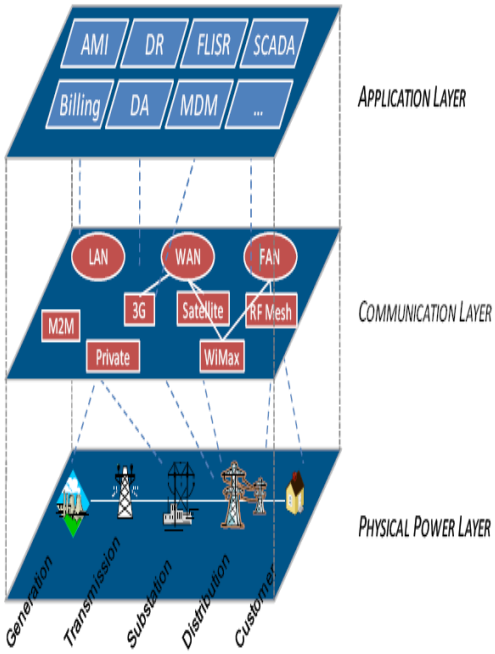


Fig.1 Framework of DSE scheme.

Many researchers focus Smart Grid systems and novel methods to soar! Special characteristics of the lot. Smart metering data privacy feature, but often enough to be sent to the control center in the compromise of a fictitious ID adopting various measures, not to be blamed, it is a solution focused on the data anonymizing high frequency measurement application and / or distribution network. Home area network (CAN), to protect the security of data sent to one of the proposed project. Household smart meters, smart home devices for reading chip orthogonal code to collect data and control messages to be distributed has been used to keep the confidentiality and anonymity. Performance and advanced metering infrastructure (AMI) to improve safety use a new wireless communication scheme. Improve the spectrum efficiency of power consumption measurements are transmitted only when there is a significant

P-ISSN: 2347-4408
E-ISSN: 2347-4734

change. Communication traffic analysis by monitoring user behavior and artificial spoofing packets are sent to prevent attackers from. Helmen achieve mutual authentication and smart meters are shared between the transmissions protocols used to establish a session key; Hash-based authentication is used to authenticate the message. SG Protect information collection, aggregation scheme to protect the privacy of an efficient and multi-dimensional data structure and Paillier homomorphic cryptosystem to encrypt a super-increasing series of structured data by using the technique, is proposed.



2.1 SMART GRID

Smart grid automation control, high-energy converters, modern communications infrastructure, sensing and measurement technologies, and improved performance and reliability with a modern energy infrastructure can be considered a modern electricity grid Hence the need, power and network availability, and optimization techniques in terms of management. Layer surrounding the power transmission and distribution; Data transport and control layer (or communication layer); and the application layer, grid applications and services do not really mean. Communication is the glue that holds the layer.

Image: Smart Grid architecture layer One power layer and applications, and smart grid operations as possible.

The Smart Grid, reliability, real-time information to end-users reliable delivery of electricity from generating units are the key factor. Equipment failures, capacity constraints, and power, riots and natural accidents and disasters, the impact tends to play a major system-level power monitoring, detection and can be avoided with care.

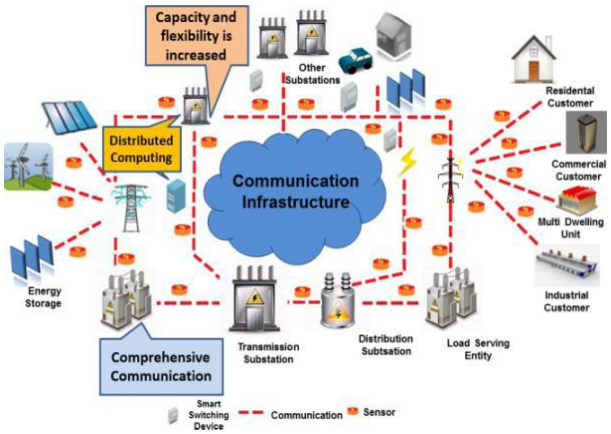


Fig.2 Communication infrastructure of smart grid

2.2 ZIGBEE

ZigBee is a wireless communications technology that is relatively low in power usage, data rate, complexity and cost of deployment. It is an ideal technology for smart lightning, energy monitoring, home automation, and automatic meter reading, etc. ZigBee and ZigBee Smart Energy Profile (SEP) have been realized as the most suitable communication standards for smart grid residential network domain by the U.S National Institute for Standards and Technology (NIST).

CYCLIC REDUNDANCY CHECK redundancy (CRC)
The cyclic redundancy check, or CRC, is a technique for detecting errors in digital data, but not for making corrections when errors are detected. It is used primarily in data transmission. In the CRC method, a certain number of check bits, often called a checksum, are appended to the message being transmitted.

2.3 SECURITY ISSUE

Security is protection against unwanted random events. Security deliberate, planned action to take place due to the result, the objective of which is protection against incidents. Based on the above analysis, both wired and wireless communication standard authentication, confidentiality, and integrity checks including the smart grid, can provide basic care. These measures can deal with network attacks. In order to provide a set of security services in the Smart Grid, Smart Grid Security and related standards proposed wire. Safe and reliable services than normal devices for security devices usually need to realize that. Therefore, more and more security measures will be added to the trusted information security standards. The extensions can be regarded as the standard of care of the safety standards. This protection is based on the quality and safety of data can be transmitted. Extension of wired communication standards for the quality of care, but only if the wireless communication standards, please note that there are no security, extensions.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

2.4 MD2 MESSAGE DIGEST ALGORITHM

RSA, Data Security Inc. R. Rivest, a number of "information collection" for Postal Code MD name of the hash functions, designed a series. Md1 is a protocol. MD2 Sun [175] In 1990, comment, and the BMAC, [193] is recommended instead. MD3 published, and its designer looks abandoned. MT 4 [279, 282] and MD5 [281, 283] will see in the next section. This can occur as part of a discussion of some of the attacks, MD2 Sun will give a brief description. In a first stage of the algorithm, a simple 16-byte Hashcode computed and integrated messaging. Then a second compression algorithm used for an extended message. T is divided into blocks of 16 bytes in the message package. T-1 and 0 _ J _ 15. _ individual bytes in two stages to be represented by a random 8-bit permutation sbox, 0 _ I use X [i] [j] is denoted by []. The first is easy to analyze the hash code. The hash code, it is easy to find a message in the last 15 bytes. Determined by a backward recursion and then the first one, you can choose other than bytes. Sun MD2 to attack this one, probably the last one to select the volume, and to calculate the previous set of 15 means that the same bytes. If the first byte of the yields, it is perfect for a probability of 1/256. The following observations should be the main hash code. State the facts of the last two 16-byte discarded last iteration seems that one can omit the last 32 operations. J after a kth stage internal status byte (0 _ J _ 17) Hj [K] should be marked.

2.5 C-FREE

C-Free is a professional C/C++ integrated development environment (IDE) that support multi-compilers. Use of this software, user can edit, build, run and debug programs freely. With C/C++ source parser included, although C-Free is a lightweight C/C++ development tool, it has powerful features to let you make use of it in your project.
Support Multi-compilers Now support other compilers besides MinGW as following:

- MinGW 2.95/3.x/4.x/5.0
- Borland C++ Compiler
- Cygwin
- Intel C++ Compiler
- Lcc-Win32
- Microsoft C++ Compiler
- Digital Mars C/C++
- Ch Interpreter
- Open Watcom C/C++

more compilers will be supported in the future version.

3. OUTPUT RESULTS

3.1 MICROCONTROLLER ENCRYPTION

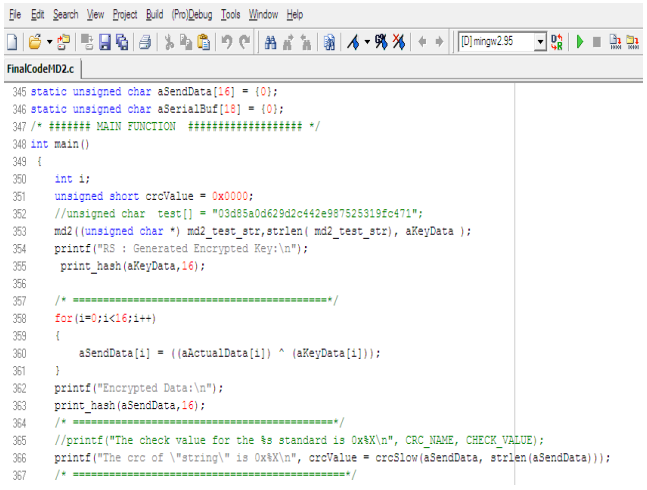


Fig.3 Encryption coding compilation in C-free

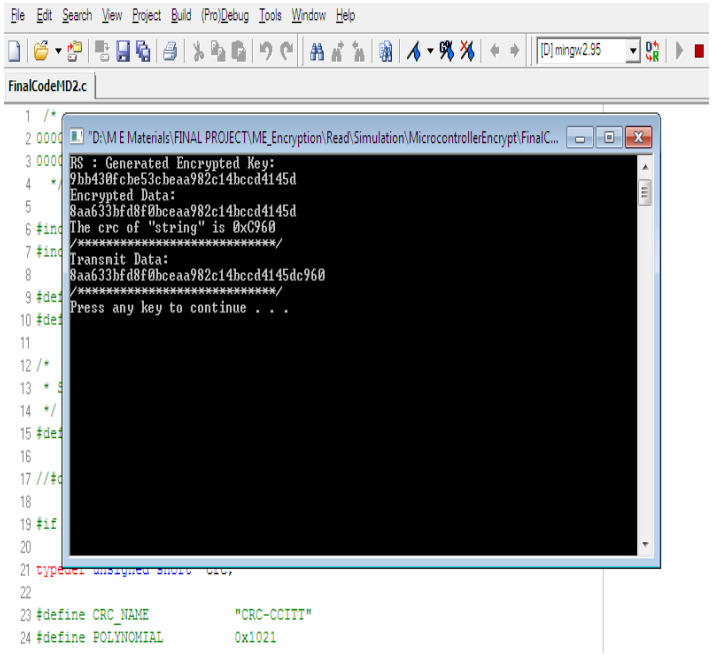


Fig.4 Output of microcontroller encryption

For the safety measures we are doing an encryption of the actual data and a CRC check is being done on the microcontroller side as shown in Figure.3. The Figure.4 shows the compiled sequence of the encrypted data. Initially a key is being generated dynamically by the setting of the system. Then accordingly the actual data will be encrypted with the help of a CRC string. Then after checking the CRC and encrypting the data a complete overloaded data is being transmitted.

3.2 PC DECRYPTION

This is the compilation of received data from the DOCK-LIGHT the serial port monitoring software. Figure.5 shows the data which will be checked for the CRC code initially.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

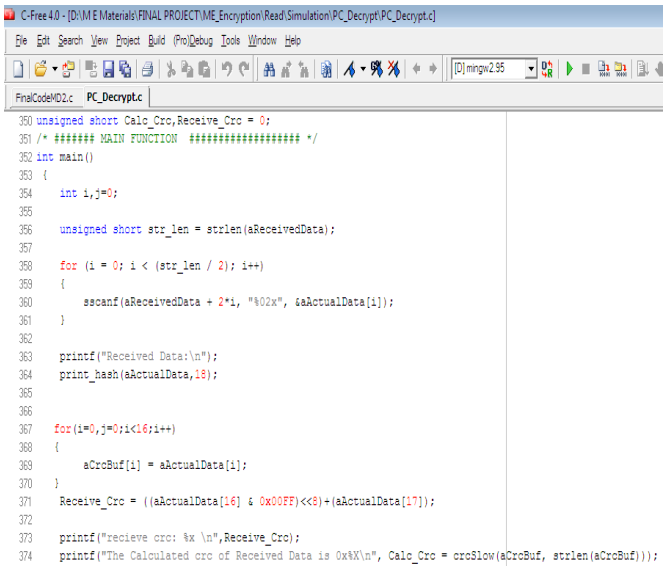


Fig.5 C-free compilation of the transmitted data

If the code is correct on both the sides, then the process will be continued with the decryption operation with the help of all the other operations that supports is retrieving the data from the encrypted data.

Here Figure.6 shows the decrypted data on the PC side. The overloaded data will be transmitted from the microcontroller kit and it will enter the PC via the serial port which will be recognized by "Dock light" the serial port monitoring software. Final smart meter readings will be displayed in the end of compilation.

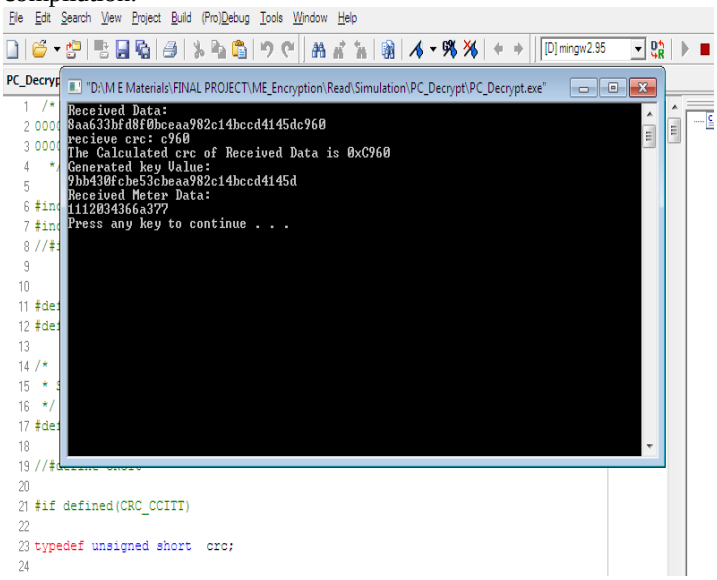


Fig.6 Output of PC decryption with the actually transmitted data

4. CONCLUSION

With the help of the cryptographic technique, the security and reliability of the data transmission is ensured. In the previous works data security is being taken care. But the validity of data is not considered. The data will not be lost. But it may be altered due to any of the external factors. So additionally we are performing CRC (Cyclic Redundancy check-CCRITT) to ensure whether the data received is same as that of data send. If there is any change in the transmitted data due to some external factors, this CRC check will completely help you in clarifying the reliability of the data. Once after the reliability is checked the data received can be forwarded for the other operations with no doubt. This can be achieved at low cost and simple process and used at RFID authentication scheme based on dynamic key generation, efficient user revocation for dynamic groups in the cloud and secure multi owner data sharing for dynamic group in cloud. The implementation of the hardware components for this sequence will be carried out by me in the future work of my project (Phase-II).

REFERENCES

[1] T. Liu, Y. Gu,D.Wang, Y. Gui, and X. Guan, "A novel method to detect bad data injection attack in smart grid," in Proc. IEEE INFOCOM Workshop Commun. Control Smart Energy Syst.

[2] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," Security Commun. Net 2012 [Online]. Available: http://http://onlinelibrary.wiley.com/doi/10.1002/sec.559/abst ract

[3] K. Ren, Z. Li, and R. C. Qiu, "Guest editorial cyber, physical, and system security for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 643–644, 2011.

[4] Office of the National Cordination for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards," 2010 [Online]. Available: http://www.nist.gov/smartgrid/

[5] Federal Energy Regulatory Commission, "Renewable & energy efficiency-Generation & efficiency standards" 2011 [Online]. Available: http://www.ferc.gov/market-oversight/othr-mkts/renew.asp

[6] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009.

[7] Cisco, "Security for the smart grid," 2009, White Paper [Online].Available: http://www.cisco.com/web/strategy/docs/energy/ white paper c11_539161.pdf

[8] W. Xudong and Y. Ping, "Security framework for wireless communications in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, pp. 809–818, 2011.

[9] R.Moghe, F. C. Lambert, and D. Divan, "Smart "Stick-on" sensors for the smart grid," IEEE Trans. Smart Grid, vol. 3, pp. 241–252, 2012.

[10] "The smart grid: An introduction," in DOE's Office of Electricity Delivery and Energy Reliability 2008.