International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Embedded Systems with Wireless Networks for Data Security in Industry Applications

J.S.Prasath, U. Ramachandraiah, G. Muthukumaran

Abstract: ***Embedded system technologies are widely used in a variety of industry applications. Embedded devices with wireless technology are vulnerable to a variety of attacks due to their large number of deployment, resource limitations, and increased complexity. Embedded systems with wireless technology often have to work in an untrusted and harsh environment, which allows attackers to analyze side channels and physical component attacks. The unauthorized parties can access and modify the sensitive process information that is transmitted across wireless networks. The integrity of information results not only damages the physical components but also failure of entire plant operations. The embedded systems without security mechanisms results in unsafe working environment. This proposed work is the implementation of a security mechanisms using embedded system with wireless networks in order to protect the sensitive plant information from unauthorized access. It reads the temperature and gas data through the embedded system and performs encryption which converts the process data into unreadable format. This unreadable cipher text is transmitted across wireless networks using zigbee technology. This encrypted data is converted back to plain text by the process of decryption at the receiver. This received process data is monitored using Graphical User Interface (GUI). The security threats increases due to the wide deployment of embedded systems. This proposed work provides cost-effective solutions in protecting the process equipments and safety to the operators. It can be applied to secure sensitive process data in any industry applications.***

Keywords**: Sensor, Embedded systems, Wireless networks, Security mechanism, Zigbee**

I. INTRODUCTION

Embedded system with wireless technology is a current trend and is widely used in various fields. Embedded devices with wireless networks often need to access the information, to store the data and communicate the sensitive information to the outside world. The drawback of embedded system is the severe resource constraints in terms of memory, computational capability and energy. The security threats are increases due to the usage of embedded devices with wireless technology in all fields. The security of embedded systems can be performed at various levels which include protocol, algorithm, architecture and circuit. Information and communication security of embedded system with wireless networks has gained significant attention. The flexible embedded system architecture is essential to support the security standards and functionalities. The various attacks on embedded based wireless networks are energy drainage, physical intrusion, network intrusion, information theft, damaging of sensors or peripherals and systems reprogramming. Hardware based attacks such as physical attacks, system-on-chip and networks-on-chip attacks cause serious problems and results in failure of embedded based wireless networks. The address and data buses can be monitored by the attacker to perform spoofing, splicing and replay attacks.

The hardware based attacks disturb the physical behavior of the wireless based embedded systems. Software based attacks such as code injection attacks and cryptographic attacks on embedded wireless networks disturb the normal functioning of plant operations. The packet switching protocols could also be targeted by software attacks and could result in a malicious behavior such as unknown destination, packet replay or deadlock. The buffer overflow attack results in serious damages to application-oriented embedded systems. The usage of embedded based wireless networks in industrial operations becomes more vulnerable to attacks on the integrity of data. This may results in failure of industrial process equipment. Embedded systems are designed to perform any specific pre-defined task that must meet any real time constraints. The information in a network passes through a number of untrusted connection. During the design phase of the product, security is not usually taken into account. The implementation of security in wireless networks becomes complex after the product is manufactured. The information security in embedded based wireless networks is necessary to protect the hardware equipment from the failure. It is essential to implement the protocols for secure data transmission in embedded based wireless networks.

II. SECURITY ATTACKS ON EMBEDDED BASED WIRELESS NETWORKS

The attacks on embedded based wireless networks include combination of hardware, software and wireless medium. The attack causes failure of physical components, equipment damage and unsafe working conditions to operators. The risk assessment is essential to identify the security threats and vulnerabilities in the embedded based wireless networks.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Mr. J.S.Prasath,* Department of EIE, KCG College of Technology, Chennai, India. Email: jsprasath@gmail.com
Dr. U. Ramachandraiah, Department of EEE, Hindustan Institute of Technology and Science, Chennai, India. Email: uppur@hindustanuniv.ac.in
Dr. G. Muthukumaran, Department of EEE, Hindustan Institute of Technology and Science, Chennai, India. Email: gmkumaran@hindustanuniv.ac.in

The embedded system security improvement during various product development phases are proposed [1]. The physical behavior of the embedded based wireless networks is monitored by the hardware based side-channel attacks.

A Dynamic Security Risk Management (DSRM) mechanism is proposed for networked industrial applications which manage the aperiodic real-time tasks [2].

This mechanism provides increased level of real-time embedded based wireless security.

The various classes of physical attacks on embedded systems are addressed [3]. The physical attacks are categorized into Invasive, Semi-invasive and Non-invasive attacks. The aim of these attack is to physically disturb the embedded chip operation, observing the behavior of embedded chip and to extract about the processed data such as power dissipation, computation time etc. The various causes of security threats and suggested solutions to protect the systems from the attackers are presented [4]. The security attacks takes place at design level, implementation level and testing level. The system of attack may also vary for users, content providers and manufacturers. The experimental analysis done for analyzing the characteristics of security algorithms in a real-life embedded platform [5]. The speed, power and energy cost of cryptographic algorithms are analyzed. The experimental result and analysis predicts that the energy requirement and time overheads of cryptographic algorithms are non-linear to the size of plain text. The Time Stamps Verification (TSV) is an energy efficient approach proposed which provides Memory Integrity verification in embedded systems [6]. The memory integrity attacks are splicing attack, spoofing attack and replay attack. In cryptography, the message integrity is achieved by using hash function. The message authentication codes are used to secure the integrity of message. The pseudo random number generator can be used to generate timestamps such as block ciphers.

The security requirements, attack methods and its countermeasures are surveyed for embedded systems [7]. The attacks are categorized as physical attacks, software attacks and side channel attacks. The probe is used to eavesdrop the inter-component communications in circuit board of embedded systems by physical attacks. It is necessary to ensure the confidentiality of information, integrity of data and code while designing countermeasures against software attacks. A hardware monitor is proposed which detects any attack that causes the embedded processor to deviate from its normal programmed behavior and operates parallel to an embedded processor [8]. The processing steps only verified by the hardware monitor that are matched with the original application. The attack on execution steps pattern is monitored. The confidentiality of information, integrity of data and code is ensured by the cost-effective and flexible architecture for mid-range to high-end embedded processors [9]. The configured secure processor operates securely which allows only execution of trusted programs. The cryptographically sound signatures embedded in the code and data ensures integrity using runtime verification. A scalable, application-specific methodology is proposed for securing the program execution on embedded processors [10]. The hardware-assisted architecture monitors the performance of program execution time. The detection and prevention of unintended program behavior is achieved by employing dedicated hardware monitoring. The consistency between static and dynamic aspects of a program should be ensured by suitable hardware design.

III. BLOCK DIAGRAM OF PROPOSED EMBEDDED BASED WIRELESS SECURITY SYSTEM

The security in embedded based wireless networks is essential due to communication of sensitive information takes place between process equipment. Figure 1 shows the block diagram of Embedded based Wireless Secure process monitoring.

In this proposed work, secure monitoring of process parameters such as temperature and presence of gas is implemented using embedded based wireless networks. The LM35 series chips are used for sensing the temperature from -55ºC to 150°C. The MQ-2 gas sensor is used to sense the harmful gases which include LPG, butane, propane, methane, alcohol, hydrogen and smoke. Zigbee is based on wireless mesh standard operates on low power and widely used for monitoring and control applications. A unique Personal Area Network (PAN) identifier is defined for each network which is common among all devices of the same network. A 64-bit and a 16-bit PAN IDs are supported by Zigbee which are used to identify a network and shared by the devices on the identical Zigbee networks. The unique PAN ID should be used if multiple Zigbee networks are operating within range of each other. The data transmission in wireless networks using Zigbee technology ensures integrity. If the third party's PAN ID is different from the Zigbee coordinator PAN ID, data cannot be accessed. The unauthorized users cannot read the sensor data and it is impossible to modify the data. This wireless transmission of process parameters ensures confidentiality and integrity.

IV. PROPOSED SECURITY ALGORITHM

In this proposed work, asymmetric algorithm is used for secure data transmission over wireless networks. An asymmetric algorithm involves three steps.

A. Key Generation

First step is to generate public key and kept open to everyone. A private key is then generated which is kept secret. The authorized receiver is only given rights to access the private key. It is necessary that private key should not be accessed by the third party.

B. Encryption

Public key is used to encrypt the original text into cipher text.

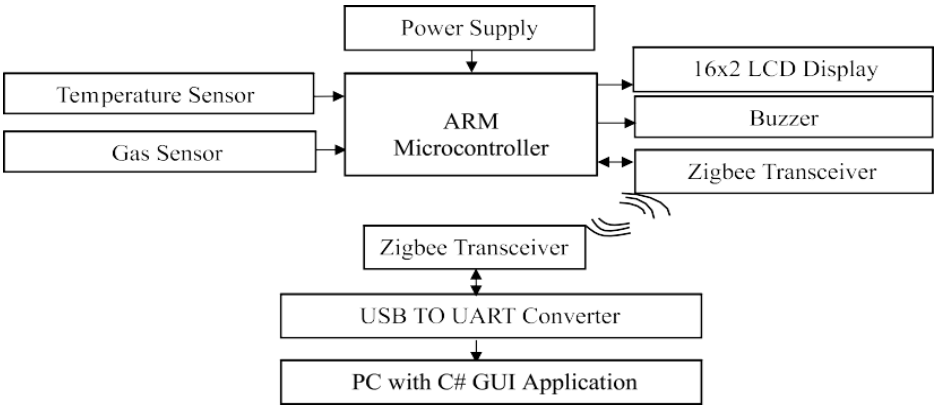

Fig. 1 Block diagram of Embedded based Wireless Security System for Process monitoring

C. Decryption

Private key is allowed only to user who is responsible for accessing the received data.

D. Algorithm for Key Generation:

The algorithm involves generation of public key and a private key. The public key is used to encrypt the data before transmission and private key is used to decrypt the data after reception.

The plain data is taken as input and converted to encoded form by the process of encryption. This encoded data is transmitted through wireless medium to the receiver. The decryption algorithm is used at the receiver to convert the encrypted data back to the original data. The various steps involved in the key generation are shown in the flowchart.

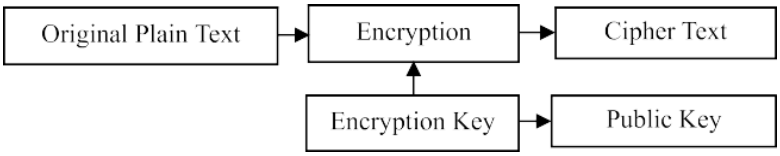

Fig. 2 Block diagram of Asymmetric Encryption

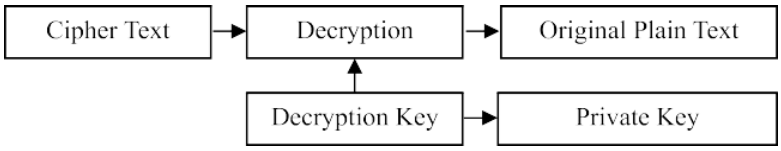

Fig. 3 Block diagram of Asymmetric Decryption

V.FLOWCHART

The flow chart given below represents various steps involved in data encryption. The mathematical calculations are used to obtain the cipher text (C) from the plain text (M) called encryption and to obtain the plain text (M) from the cipher text (C) called decryption. The proposed security algorithm is based on asymmetric and it uses two keys known as public key which is denoted by 'i' and private key which is denoted by 'j'.

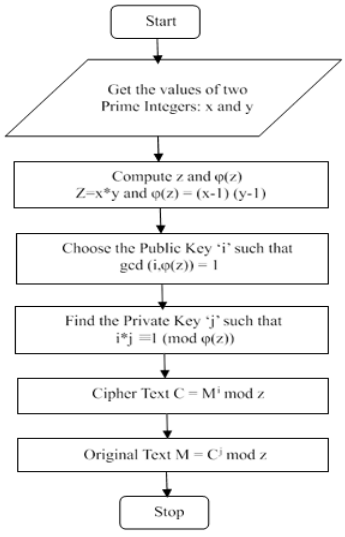

Fig. 4 Flowchart for the Proposed Security Algorithm

VI. IMPLEMENTATION OF EMBEDDED SYSTEM WITH WIRELESS NETWORKS FOR SECURE PROCESS MONITORING

This proposed security algorithm is programmed in keil C compiler and implemented using ARM LPC2148 microcontroller. Keil is employed as the Integrated Development Environment and embedded C is used for firmware development. The keil C code is used to initialize the UART serial port, ADC and LCD. The threshold value is set for temperature which is 40°C and for gas sensor which is 300. The buzzer gives the beep sound if the sensor value exceeds the threshold value. A 16x2 alphanumeric LCD is used to display the temperature and gas sensor data.

A. Transmitter Section

The transmitter section shown in Figure 5 which includes temperature and gas sensors, ARM LPC2148 microcontroller, buzzer, 16x2 LCD display and Zigbee coordinator. The keil C compiler is used for programming ARM microcontroller to read the temperature and gas sensor data.

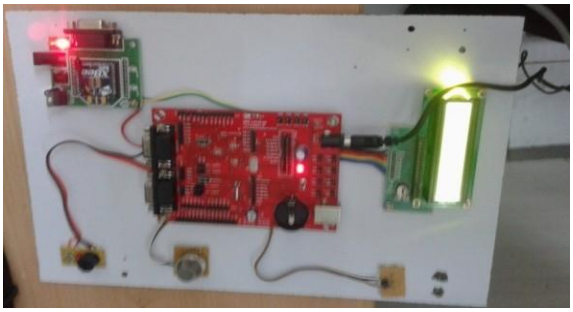

Fig. 5 Secure transmission of process data using Embedded System with Wireless network

The Zigbee is a wireless personal area networks which operates on IEEE 802.15.4 physical radio specification. The Zigbee protocol can support the mesh network in which the multiple pathways connect each node. The PAN ID should be configured between Zigbee Coordinator and Zigbee router devices. The unauthorized users cannot access the Zigbee network if the PAN ID is different from the configured PAN ID. The confidentiality and integrity of process data can be achieved.

B. Receiver Section

The receiver section shown in Figure 6 which includes Zigbee router, ATmega 8A microcontroller and adriver circuit. The Zigbee router acts as receiver which is used to receive the process data from the Zigbee Coordinator. The Atmel ATmega8A microcontroller is programmed to receive the sensor data.

VII. RESULTS AND DISCUSSION

This proposed work is the secure transmission and monitoring of temperature and gas sensor data using embedded system and the Personal Computer (PC) based data acquisition system. The sensor data is transmitted through zigbee network and monitored through the GUI. The sensor data at the receiver is acquired through the COM port and monitored through the PC.

The temperature and gas sensor data monitored through GUI which is shown in figure 7. The COM port number is to be given in the GUI and click the OPEN COM block. The data acquisition system will not indicate the process data if the COM port number is wrong. The wireless process monitoring and control is the current trend in the industrial operations. It reduces the cable cost and allows monitoring and controlling of process parameters long distance.

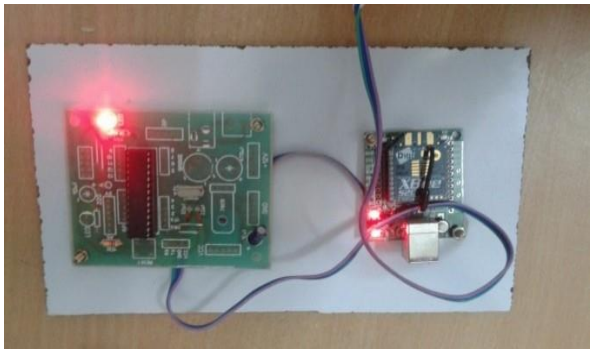

Fig. 6 Secure reception of process data using Embedded System with Wireless network

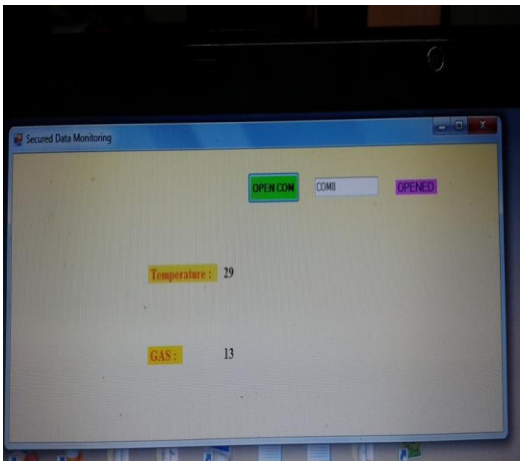

Fig. 7 Temperature and Gas Sensor Data monitoring through GUI

The drawback of wireless monitoring is unsecure and the sensitive process data can be altered by the attackers. This leads to damage of valuable process equipments and unsafe to operators. The security mechanism is essential for wireless networks in order to protect the sensitive process information and to ensure smooth plant operations. This proposed work allows continuous monitoring of process data in remote place. This concept can be used in any process industries to monitor the parameters wirelessly and securely.

VIII. CONCLUSION

The process data security is an essential concern for smooth plant operations. Although the embedded systems are vulnerable to variety of attacks, the data monitoring through the wireless medium provides additional security threats. This proposed work is the implementation of data security in monitoring of temperature and harmful gases which include LPG, propane, methane, hydrogen and smoke using embedded systems with wireless technology.

The sensitive gas and temperature data is read through the embedded system and perform data encryption. The symmetric algorithm is adopted which needs single key for both encryption and decryption. The transmitter section performs symmetric encryption of sensor data and the cipher text is transmitted across wireless networks. The wireless network used in this work Zigbee standard which is low cost and low powered widely used for monitoring and controlling applications. Zigbee includes Coordinator, router and end device which all together performs communication of process data over wireless networks. The receiver section reads the cipher text and performs symmetric decryption. The process data is monitored through GUI in numerical form. The benefit of this work is cost effective embedded system and wireless monitoring of process parameters which greatly reduces the cable cost. This proposed work can be applied for continuous secure monitoring of process parameters using embedded systems with wireless medium. The designers should give top priority to analyze possible security attacks and to ensure secure functioning of wireless based embedded systems.

REFERENCES

1. Haytham Elmiligi, FayezGebali, and M.Watheq El-Kharashi, “Multi-dimensional analysis of Embedded Systems Security,” Microprocessors and Microsystems, vol. 41, pp. 29–36, 2016.
2. Wei Jiang, Yue Ma, Nan Sang, ZiguoZhong, “Dynamic security management for real-time embedded applications in industrial networks,” Computers and Electrical Engineering, vol. 41, pp. 86-101, 2015.
3. Apostolos P. Fournaris, Nicolas Sklavos, “Secure Embedded System Hardware Design – A flexible security and trust enhanced approach,” Computers and Electrical Engineering, vol. 40, pp. 121-133, 2014.
4. AnikBarua, Mohammad Minhazul Hoque, Rubina Akter, “Embedded Systems: Security Threats and Solutions,” American Journal of Engineering Research, vol. 3, pp. 119-123, 2014.
5. Wei Jiang, Zhenlin Guo, Yue Ma, Nan Sang, “Measurement-based research on cryptographic algorithms for embedded real-time systems,” Journal of Systems Architecture, vol. 59, pp. 1394-1404, 2013.
6. Satyajeet Nimgaonkar, Mahadevan Gomathi sankaran, Saraju P. Mohanty, “TSV: A Novel Energy Efficient Memory Integrity Verification scheme for Embedded systems”, Journal of Systems Architecture, vol. 59, pp. 400-411, 2013.
7. Mirza Aamir Mehmood, Amir Shahzad Khokhar and Mazhar Ali, “Incorporating Security in Embedded System – A critical analysis”, International Journal of Computer Science Issues, vol. 8, pp. 156-160, 2011.
8. Shufu Mao, Tilman Wolf, “Hardware Support for Secure Processing in Embedded Systems”, IEEE Transactions on Computers, Vol. 59, pp. 847-854, 2010.
9. Austin Rogers, Aleksandar Milenkovic, “Security extensions for integrity and confidentiality in Embedded processors”, Microprocessors and Microsystems, Vol. 33, pp. 398-414, 2009.
10. Divya Arora, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha, “Hardware-Assisted Run-Time Monitoring for Secure Program Execution on Embedded Processors”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 14, pp. 1295-1308, 2006.

AUTHORS PROFILE

Mr. J S Prasath, received M.E degree in Process Control and Instrumentation Engineering from Annamalai University, Chidambaram and pursuing Ph.D. in Embedded Wireless Sensor Networks for Industrial Security at Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as Assistant Professor in the Department of Electronics and Instrumentation Engineering at KCG College of Technology, Chennai, India. He is an interdisciplinary and guiding many Research projects at under graduate and post graduate level. Earlier he served as Assistant Professor in SRM University. His research interests are Embedded Systems, Wireless Sensor Networks, Process Control and Industrial Automation.

Dr. Uppu Ramachandraiah, received M.Tech. degree in Electronics and Instrumentation Engineering from National Institute of Technology, Warangal and Ph.D. degree in Signal Processing from Indian Institute of Technology Madras, India. Currently he is working as Professor& Head in the Department of Electrical and Electronics Engineering at Hindustan Institute of Technology and Science, Chennai, India. He is an interdisciplinary and guiding 9 Research scholars. Earlier he served as Senior Scientific Officer at Bhabha Atomic Research Centre Facilities, Department of Atomic Energy. His research interests are Real-time Embedded Systems, Real-time Signal Processing, Robotics and Automation and Industrial Automation.

Dr. G Muthukumaran, received M.E degree in Computer Science and Engineering from Government College of Technology, Coimbatore and pursuing Ph.D. in Robotics and Control Engineering at Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as Professor in the Department of Electrical and Electronics Engineering at Hindustan Institute of Technology and Science, Chennai, India. He is an interdisciplinary and guiding many Research projects at graduate and under graduate level. Earlier he served as Automation Engineer at PSG group of Industries. His research interests are Embedded Systems, Robotics and Automation.