IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 9, September 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 9, September 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1109011 |

WSN Security Using 1-Wire Authentication IC

Selbi M U[1], Santhosh Kumar P C[2]

Lecturer, Dept. of Computer Engineering, Govt. Polytechnic College Kalamassery, Ernakulam, Kerala, India.[1]

Technical Officer, O/o Controller of Technical Examination, Kaimanam, Trivandrum, Kerala, India.[2]

ABSTRACT: Security is the main pre concern to socialize the wireless sensor network for common usage. The deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks. The inherent power and memory limitations of sensor node make conventional security solutions unfeasible. This technology implements a hardware authentication solution for a WSN node using 1-wire authentication IC. This 1-wire authenticator can be attached to a sensor node which is to be authenticated.

KEYWORDS: Wireless Sensor Network;1-wire device; Authentication IC; Sensor node; Hardware Security; SHA-1 Algorithm.

I. INTRODUCTION

Wireless Sensor Network is an emerging technology provides low cost solution to variety of real world challenges.WSN is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions such as temperature sound, vibration, pressure, motion or pollutants at different locations.WSN have great potential to be employed in critical situations like battle fields, military surveillance and commercial applications such as building traffic control, habitat monitoring, medical monitoring and home automation.

The field of sensor network is well known due to its popularity in research community. However WSN suffer from many constraints including low computation capabilities, small memory, limited energy resources, susceptibility to physical capture and the use of unsecure wireless communication channels.

One of the major challenges WSN face today is security. Security is important and crucial to the success of applying WSN. For example when sensor network is used for military purpose, it is very important to keep the sensed information confidential and authentic.

One of the most important tools for ensuring the security of the network and its services are the security primitives. For making the WSN secure, cryptography plays an important role. Since the sensor nodes are not so wealthy in terms of resources, therefore complex cryptographic algorithms cannot be played over it.

1-wire is a device communication bus system. It is typically used to communicate with small inexpensive devices. 1-wire devices are available as single components in integrated circuits (IC's) and in some cases a portable form called iButton that resembles a watch battery. 1-wire provides a lot of security solutions in the form of IC's.

This technology presents a hardware authentication solution for a WSN node using 1-wire authentication IC. This 1-wire authenticator can be attached to a sensor node which is to be authenticated.

II. RELATED WORK

Wireless Sensor Network (WSN) is an emerging technology and have great potential to be employed in critical situations like battle fields and commercial applications such as traffic surveillance, habitat monitoring and many more scenarios. A WSN is a group of highly-constrained hardware platforms called sensor nodes that collaborates towards a set of common goals. All the functionality of sensor network depends on the individual capabilities of the sensor nodes. Due to significant advances in miniaturization, low power circuit design but reasonably efficient to carry the sensitive information through wireless communication, WSN have attracted attention a lot in recent years. A single sensor node has built-in sensors, a processor with limited computational capabilities, power unit and a communication system to communicate to other WSN components through a wireless channel.

One of the most important tools for ensuring the security of the network is using cryptographic algorithms. Due to the well accepted limitations, WSN is not able to deal with traditional cryptographic algorithms. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time and power consumption.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 9, September 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1109011 |

The commonly used cryptographic algorithms are public key cryptography and symmetric key cryptography. The constraints on computation and power consumption in sensor nodes limit the application of public key cryptography in WSNs. Symmetric key cryptography algorithms and hash functions are faster, and consumes much less computational energy than public key algorithms. When a subsystem component has limited processing power and memory, advanced cryptography is usually not possible. Secure exchange of data and peer-authentication requires secrets, and microcontrollers are not very good at keeping secrets from clever hardware and software attacks. The solution is to move the cryptographic task to a device that is specially designed to perform these tasks well.

1-Wire memory devices contain fast, powerful cryptographic engines. These devices can be used with small microcontrollers and limited resources to provide strong small-message encryption and peer-to-peer authentication between subsystems. 1-Wire devices that perform SHA-1 hash functions to provide a low-cost, low-overhead cryptographic solution for small message encryption and authentication.

Authentication is a process with the objective to establish proof of identity between two or more entities. In the case of one-way authentication, just one party is involved proving its identity to another. With two-way authentication, both parties prove their identity to each other. The most commonly used method of authentication is the password. The main problem with passwords is that they are exposed when used, making them vulnerable to spying.

III. PROPOSED SYSTEM ARCHITECTURE

Secure WSN system

To develop a secure authentication WSN system requires all the sensor nodes should have authenticated. To provide a 1-way authentication between an edge router/ host system with a sensor node, sensor node is attached with 1-wire secure authenticator and provide necessary interfacing. The host system also should have the same cryptographic algorithm used in the 1-wire IC attached in the sensor node. **Figure 1** shows the system architecture.

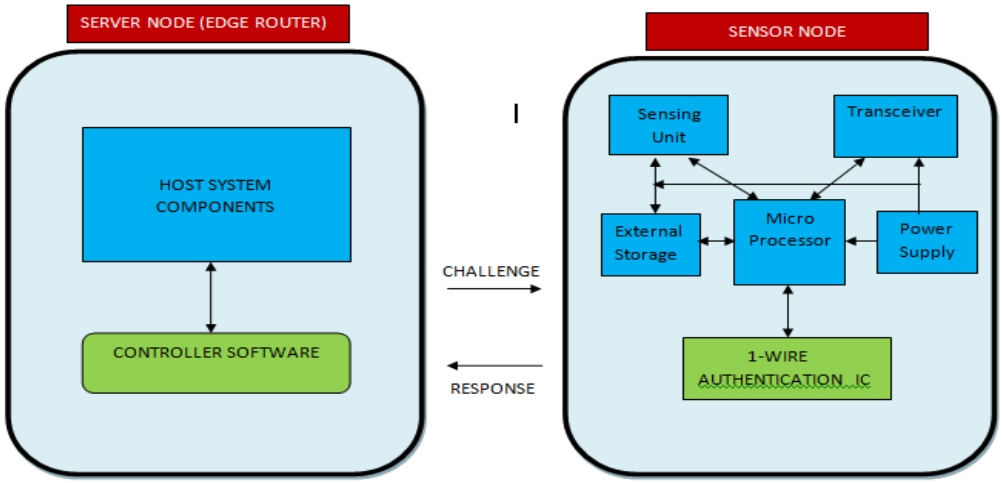

Fig.1. The proposed system architecture.

IV. SENSOR NODE AUTHENTICATION PROCESS

1. Secure Challenge- Response Authentication Device Architecture

The SHA engine of SHA-1 and SHA-256 devices can be operated in three different ways depending on the operation to be performed. In all cases, the engine receives input data and computes a MAC result. For each operation type, there are differences in the SHA engine's input data based on the targeted use of the MAC result. For any SHA operation, as a fundamental requirement of symmetric key-based secure systems, the host must either know or be able to compute the secret stored in the slave device in order to be authenticated.

The primary purpose of SHA-1 and SHA-256 secure authenticators is challenge-and-response authentication. The host sends a random challenge and instructs the slave device to compute a MAC response from the challenge, the secret, user memory, and additional data that together constitute the "message".

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 9, September 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1109011 |

2. Secure Authentication IC's process details

The major data elements and the data-flow paths of the SHA-1 secure coprocessor IC with 1-Wire interface are shown in **Figure 2**. Easily recognized are the 8-byte secret key and the buffer memory (scratchpad), which temporarily stores the challenge. Data elements not mentioned previously are the unique device ID number (a standard 1-Wire feature), four pages of user EEPROM, control registers, and system constants.

The device ID serves as a node address in 1-Wire networks, but also contributes to authentication. The user memory holds the major part of the to-be-authenticated "message". Seed constants are needed to meet formatting requirements and as padding to compose the 64-byte input data block for the SHA-1 computation. The control registers perform device-specific functions, such as optional write protection of the secret or EEPROM emulation mode; they do not contribute to the authentication process in general.

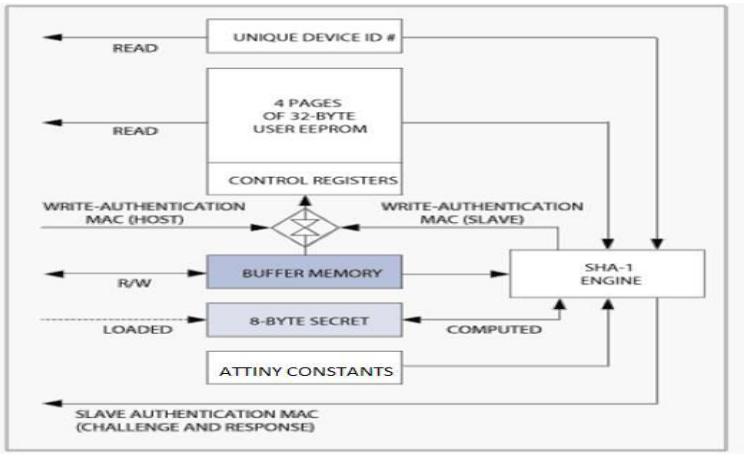

Figure 2 : 1-wire interface with coprocessor IC.

The primary purpose of the ATTiny85 is challenge-and-response authentication. The host sends a random challenge and instructs the ATTiny85 to compute a response MAC from the challenge, the secret, data from one of the memory pages selected by the host and additional data that together constitute the "message".

After it has finished computing, the ATTiny85 sends its MAC to the host for verification. The host then duplicates the MAC computation using a valid secret and the same message data that was used by the ATTiny85. A match of the MAC received from the ATTiny85 provides authentication of the device, as only an authentic ATTiny85 will respond to the challenge-and-response sequence correctly. It is crucial that the challenge is based on random data. A never-changing challenge opens the door to replay attacks using a valid static MAC that is recorded and replayed instead of a MAC that is instantly computed by an authenticATTiny85.

V. SYSTEM AUTHENTICATION MODEL

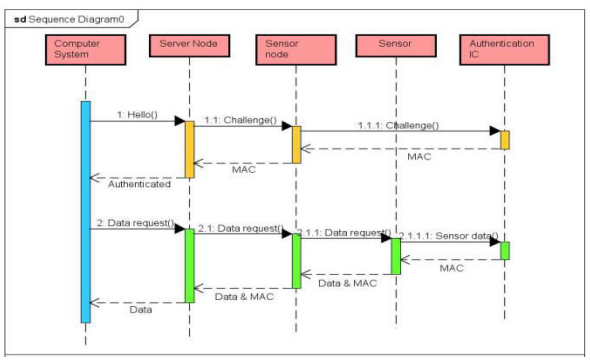

Figure 3 : System Authentication sequence

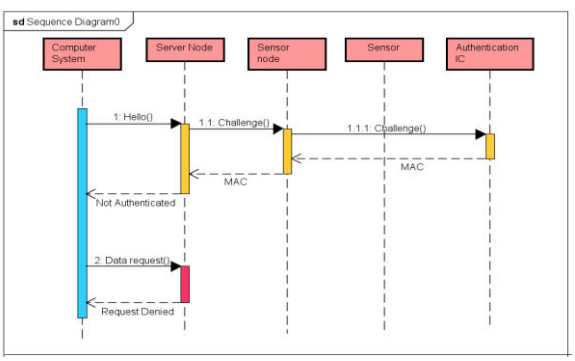

Figure 4 : System Non-Authentication sequence

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 9, September 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1109011 |

VI. CONCLUSION AND FUTURE WORK

Due to significant advances in miniaturization, low power circuit design but reasonably efficient to carry the sensitive information through wireless communication, wireless sensor network (WSN) have attracted attention a lot in recent years. WSN's are being used in many applications like health monitoring, military purposes, and home automation. Since WSN suffer from many constraints including lower processing power, low battery life, small memory and wireless communication channel, security becomes the main concern to deal with such kind of networks. Due to these well accepted limitations, WSN is not able to deal with traditional cryptographic algorithms. This project is proposed to give security to WSN nodes using hardware IC from 1-wire security solutions.

As future enhancement, a sensor network with multiple sensor nodes are introduced and the authenticated data transmission can be established between the cluster node and different sensor nodes in its network. So security can be implemented in a wireless sensor network, without much modification, which is already established.

REFERENCES

1. Jinat Rehana, "Security of Wireless Sensor Network", 2009.
2. Walters, J.P., Liang, Z., Shi, W. and Chaudhary, V. (2006), "*Wireless sensor network security: a survey*", in Xiao, Y. (Ed.), *Security in Distributed, Grid, and Pervasive Computing*, CRC Press, London, pp.367-410.
3. Yong Wang, GarhanAttebury, and Byravramamurthy: A survey of Security Issues in Wireless Sensor Networks – *IEEE Communications Surveys & Tutorials* 2006.
4. Dr. G padmavathy, Mrs. D shanmugapriya : A Survey of Attacks Security Mechanisms and Challenges in Wireless Sensor Networks.
5. Shilong Lu, XiHuang Li Cui, Member IEEE, Ze Zhao, Member IEEE, and Dong Li, Member IEEE : Design and implementation of an ASIC-based sensor Device for WSN Applications.
6. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges",International conference on Advanced Computing Technologies Page1043-1045, year 2006.
7. M.D.R. Perera, R.G.N. Meegama and M.K. Jayananda : *APAN* - Single Chip Solution with 1-Wire Communication Protocol to Interface Digital transducers to Sensor Networks
8. A. Liu, P. Kampanakis, P. Ning. Tiny ECC: Elliptic Curve Cryptography for Sensor Networks(Version 0.3). http://discovery.csc.ncsu.edu/software/TinyECC/, February 2007.
9. N. Sastry, D. Wagner.Security considerations for IEEE 802.15.4 networks.In proceedings of 2004 ACM Workshop on Wireless security (Wise 2004), Philadelphia (USA), October 2004.
10. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003.
11. Maxim :Protecting the R&D investment—two-way authentication and secure soft-feature settings JUNE 22, 2013.
12. Perrig, A., Stankovic, J., Wagner, D. (2004), "Security in Wireless Sensor Networks", Communications of the ACM, 47(6), 53-57.
13. A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of MOBICOM, 2001.
14. Maxim Application Note :Interfacing the DS18X20/DS1822 1-Wire® Temperature Sensor in a Microcontroller Environment.
15. John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipinchaudhary : WSN Security a Survey.
16. William Stallings (2003). 3 rd Ed. "Cryptography and Network Security - Principles and Practices". Pearson Education Inc. New Jersey.
17. Rodrigo Roman, Cristina Alcaraz, Javier Lopez: A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor network Nodes.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details