Securing Data Transmission in a Wireless Sensor Network Through Simple Recoverable Encryption Enabling Protocol

S.Rajarajesware[1]
(Research Scholar,Manonmaniam Sundaranar University,Tirunelveli,TN,India.
email:sivrajarajesware@gmail.com)
Dr.H.Abdul Rauf [2]
(Professor & Dean, Sree Sastha Institute of Engineering and Technology, Chennai, TN, India.
email:harauf@yahoo.com)
Dr.S.P.Victor[3]
(Dean of Science and Associate Professor,St.Xavier's College,Palayamkottai,TN ,India.
email:drspvictor@gmail.com)

Abstract: A wireless Sensor Network is a network of sensors to collect data on various parameters and to transmit them to a sink or base station in a secured manner, so as to maintain the confidentiality and integrity of the actual data generated by the sensors against the various possible threats to damage the originality of the data. In order to maintain the security of the generated data and to protect them during the transit time, a suitable solution is needed which should be viable to adopt, keeping in mind the minimal computing power and battery power availability of the sensor nodes. In this paper, a Simple, Recoverable Encryption Enabling protocol (SREE) is proposed to suit the WSN environment. To minimize computational costs, the encryption and decryption process involve only minimal computations. Also the original data can be recovered from the encrypted code without involving any keys. At the same time, this process has provision to ensure the confidentiality, integrity and authenticity of the data from the source to the destination.
Keywords: Sensor nodes, Data Integrity, Authentication, Confidentiality

1. Introduction

Wireless Sensor Network is simply defined as a large collection of sensor nodes, equipped with its own sensor, processor and radio transceiver. A wireless sensor network has been widely used in different application areas to know the battlefield situation data, monitoring building parameters and reports about malfunction in a system. [5]

The basic networked sensor devices in WSN are a radio, a power unit, sensor, embedded processor, memory etc. The ultimate aim of each sensors in WSN is to route collected data to high power sink/base station for user access through internet.

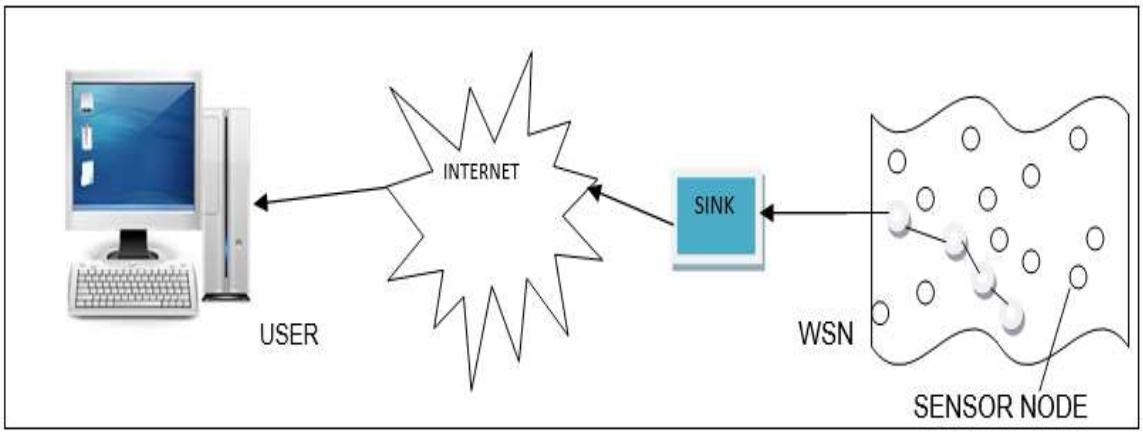

Fig 1: Communication architecture of WSN

The communication architecture of WSN is shown in figure1.WSNs are often deployed in public or otherwise untrusted and even hostile environments, which prompts a number of security issues which include the topics such as

key management, privacy, access control, authentication and DoS resistance etc[2]. A lot of attention has been devoted to communication efficiency issues. Since data transmission is a very energy-consuming operation, in order to maximize sensor lifetime, it is essential to minimize the sheer number of bits sent by each sensor device. One such approach involves aggregating sensor data as it propagates along the path from the sensors to the so called sink a node that collects sensed data. In order to support data aggregation through efficient network organization, nodes can be sometimes partitioned into a number of small groups called clusters. Each cluster has a coordinator, called a cluster head, and a number of member nodes. Clustering results in a two-tier hierarchy in which cluster heads (CHs) form the higher tier while member nodes form the lower tier. The member nodes report their data to the respective CHs. The CHs aggregate the data and send them to the Sink/base station directly or through other CHs. In WSN, the sensing nodes are deployed densely in ad- hoc manner and each node has contact with several other nodes for data collection and communication. The ad-hoc nature of large scale network unreliable communication channel, broad cast nature and uncontrolled operation results a new class of network management, routing and security issues. While the deployment of sensor nodes in unattended hostile, physically unprotected environment make the network vulnerable to a variety of potential attack, the inherent power and memory limitation of sensor node makes the conventional security system infeasible [6].

The aggregated value is a single value representing a list of values. It minimizes the number of transmissions involved in transmitting all the original values generated by the sensors. But at the receiving end, this single aggregated value does not bring back all the original values it represents. This is undesirable in many cases. Therefore in order to maintain the integrity and authenticity of the sensor data at both the ends, a new protocol SREE is proposed, which will encrypt the sensor data with minimal computations. At the receiving end the original data will be recovered from the encrypted data, which overcomes the limitation of the aggregation process.

2. Literature survey

C.Castelluccia et al [2005] proposes a simple and provably secure homomorphic stream cipher that allows efficient aggregation of encrypted data. This only uses modular additions (with very small moduli) and says it is well suited for CPU-constrained devices. It is shown that aggregation based on this cipher can be used to efficiently compute statistical values such as mean, variance and standard deviation of sensed data, while achieving significant bandwidth gain.

Doug Reitz [2006] states that wide variety of WSNs has a corresponding variety of security concerns. [7] Many of the initial WSN research was focused on efficiency without consideration for security. Many of the security defense approaches are limited in the threats they address and require certain network topology constraint assumptions. Threats can take on many forms and the papers thus surveyed had different focuses but fall into the following categories: denial-of-service (DoS), data-disruption, and data-snooping. DoS is considered as any type of threat or attack that attempts to disrupt the operation of a WSN by preventing it from providing meaningful data to the intended user. DoS can be accomplished in a variety of ways: physical damage, radio jamming, collision, flooding/exhaustion etc., Data-disruption is similar to DoS and many of the routing threats listed in DoS also can be applied to data-disruption where the attack is focused on corrupting the data by preventing the WSN from sensing of something or by interjecting false data into the network without an attack being identified by the WSN. Data-snooping threats are those where the WSN is used by an enemy or other entity to collect the same valid data as the intended user. Most threats should fall into one or more of these three categories.

The goals of security in WSNs is to prevent relevant threats from succeeding in their intended purpose. For some WSNs many of the possible threats can be dismissed. For example a weather reading station WSN for a specific area can typically dismiss concerns of covert attacks to prevent it from operating, to have it provide false information, or to covertly monitor it's output. These threats may have a low probability of occurrence due to lack of motive or potential enemies. This does not mean that a weather monitoring WSN is immune to these types of attacks. It is conceivable that if the WSN was providing critical data to monitor annual temperature changes for global warming

research that radical environmentalists might want to ensure that the temperature readings increased each year, or a massive coal burning consortium wants to ensure temperature readings drop each year, or perhaps the weather readings were used for the basis of a military operation, or other. The point of this illustration is that technological solutions cannot address all of the security threats. A threat analysis must be performed. The relevant threats should then be addressed or minimized using the technological defenses already presented in research papers or through the design and use of new defense solutions. Not all possible threats can be defended against in every WSN. With the limitation that the defenses cannot handle all conceivable threats, the security goals can be categorized into the following categories partially adopted from

•Availability ensures that the WSN remains operational despite DoS attacks

• Integrity ensures that the information reported by the WSN is accurate.

• Confidentiality ensures that the information collected by the WSN only goes to the intended user and is not intercepted.

The three security goals are counters to the three threats: denial-of-service (DoS), data-disruption, and data-snooping respectively. All three goals may not all apply to a particular WSN. The three fundamental security threats, DoS, data-corruption, data-snooping are countered by the fundamental security goals availability, integrity, and confidentiality.

Abu Shohel (2009), specifies the [8] Special security considerations for WSN with regard to Resource Consumption as WSN has storage, memory and power limitations. An effective security mechanism should have limited size for the code and algorithm. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. In addition, when implementing a cryptographic protocol within a sensor the energy impact of security code must be considered. Energy consumption usually derives from two areas: computational costs and communication costs. Computational cost relates to the cost incurred by calculation of hash functions and primitives while communication cost derives from additional byte transfer among sensor nodes. Usually communication cost is much higher than computational cost.

S.Ozdemir et al. [2011], states that the privacy homomorphism-based secure data aggregation schemes do not provide data integrity or allow hierarchical data aggregation if more than one encryption key is used in the network. This had led them to present a novel integrity protecting hierarchical concealed data aggregation protocol that allows the aggregation of data packets that are encrypted with different encryption keys. This scheme employed an elliptic curve cryptography-based homomorphic encryption algorithm to offer data integrity and confidentiality along with hierarchical data aggregation.

C.M. Chen et al. [2012] states that several data aggregation schemes based on privacy homomorphism encryption have been proposed and investigated on wireless sensor networks. These data aggregation schemes provide better security compared with traditional aggregation since cluster heads (aggregator) can directly aggregate the ciphertexts without decryption; consequently, transmission overhead is reduced. However, the base station only retrieves the aggregated result, not individual data, which causes two problems. First, the usage of aggregation functions is constrained. For example, the base station cannot retrieve the maximum value of all sensing data if the aggregated result is the summation of sensing data. Second, the base station cannot confirm data integrity and authenticity via attaching message digests or signatures to each sensing sample. Hence they tried to overcome the above two drawbacks through their Recoverable Concealed Data Aggregation scheme. In their design, the base station can recover all sensing data even these data has been aggregated. This property is called “recoverable.” The design has been generalized and can be adopted on both homogeneous and heterogeneous wireless sensor networks.

Alok Ranjan Prusty et al (2012) reveals that the security goals are classified as primary and secondary [6]. The primary goals are known as standard security goals such as data confidentiality, data authentication, data integrity, data availability and the secondary goals are data freshness, self-organization, time synchronization, secure localization etc.

A. Data Confidentiality: Confidentiality is the ability to conceal messages from an attacker so that any message communicated via the sensor network remains confidential. Confidentiality protection ensures that an attacker cannot

read data being transferred. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess.

B. Data Authentication: Authentication ensures the reliability of the message by identifying its origin. Authenticity protection tells that the source of the data is possible to trace. Attacks in sensor networks do not just involve the alteration of packets, adversaries can also inject additional false packets. Data authentication verifies the identity of the genuine senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys

C. Data Integrity: Data integrity ensures and confirms that a message sent from one node to another is not tampered, altered or modified by malicious intermediate nodes. The integrity of the network will be in trouble when:

1) A malicious node present in the network injects false data.

2) Unstable conditions due to wireless channel cause damage or loss of data.

D. Data Availability: Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station/sink or cluster head's availability will eventually threaten the entire sensor network. Thus availability is of primary essential for maintaining an operational sensor network.

Haythem Hayouni et al [2016], says that data aggregation security solutions can be classified into two categories namely the hop-by-hop solutions and end-to-end solutions. In the first category, cryptography is applied hop-by-hop, which the security services are checked in each step, the intermediate nodes decrypt each received message and calculate the aggregate before encrypt it. This method allows a simple implementation of aggregate functions, and it imposes no limits on their nature (sum, average, variance, maximum, minimum, etc.) and two types of encryption can be used. Also, these solutions incur significant delay and this is due to the encryption/decryption effort performed by the intermediate nodes. These problems were solved by end-to-end solutions based on a special property of encryption algorithms called privacy homomorphic encryption, allowing direct calculation (addition and/or multiplication) in the encrypted data. The main advantage of these solutions is that they can provide end-to-end privacy and they do not need to perform cryptographic operations at intermediate nodes, and so far only two operations are possible. They have presented the secure data aggregation schemes based on homomorphic primitives for WSNs, showing how well these schemes can satisfy the security requirements and performance metrics of sensor networks.

From the above survey it is identified that even if aggregation minimizes the number of transmissions, it has the limitation that at the receiving end it is unable to get back all the original data values that the single aggregate value represents.

3. Objective

The main objective of this paper is to identify a suitable encryption protocol in such a way that it should provide confidentiality and integrity to the environment provided it should suit to the minimal processing, memory and battery capacities of the sensor nodes. Also it should incur minimal computational and communicational costs. It should be capable to defend threats and should enable the receiver to identify and get alerted if any malfunctions occur due to the threats.

4 Proposed Work

To inculcate the above objective, this Simple, Recoverable Encryption Enabling (SREE) protocol is proposed. This protocol involves simplified encryption strategy but is aimed at providing better security against threats. Also at the receiving end, the original data is recoverable from the encrypted data based on the protocol.

5 Design and Implementation

Our new protocol called Simple, Recoverable Encryption Enabling Protocol works as follows:

This protocol takes every data generated by the sensor and encrypts it by applying a circular shift operation to it. Also to ensure the authenticity of the data at the receiving end, a security ensuring byte is formed by means of taking a particular bit from each one of consecutive 8 data. Considering that the sensors being low capacity devices, it is considered that they generate 8 bit data. At the receiving end, the reverse operation is done to recover the original data from the encrypted data and also the security byte is formed. This is compared with the received security byte. If both are same then the originality of the sent data is ensured.

Here as an example, let us consider the first 8 data generated by the sensor as A0 to A7. For each data (8 bit size) generated by the sensor, the following SREE protocol is applied:

i. For A0 a circular left shift is applied and the new combination of bits is taken as α0.

ii. Before circular shifting, bit at position b7 of A0, i.e. the MSB of A0 is copied to the LSB position i.e. bit position b0 of a new byte formation β.

iii. In each sensor, a mapping table M is maintained which contains 2^8=256 entries. Each of the entry is represented by a unique symbol. Now α0 is mapped with the entries in M and the entry which matches is identified and the corresponding symbol will be taken as the encrypted code for α0.

iv. Likewise, for the subsequently arriving 7 data, after applying circular left shift, and mapping process with M, their corresponding encrypted code will be identified and sent to the receiving node. During this process, before applying circular left shift operation, the sub sequent bits for β will be formed by copying the bits at MSB position of each data i.e. A1…A7, to occupy the bit positions from right to left in β. Now β will contain b0-b7, a new byte, which will be sent along with its preceeding 8 data i.e. encrypted equivalents for α0, α1, α2, α3, α4, α5, α6, α7 and then β.

v. Here β is used to ensure the authenticity and integrity of the preceeding 8 data. This is achieved by the reverse process at the receiving end, where the same mapping table M is used. That is for the encrypted code representing α0 the corresponding bit combination is retrieved from M by the mapping process and circular right shift is applied to it to get the original data A0.

vi. The process applied to α0 is repeated for the remaining data received at the receiving end, namely α1, α2, α3, α4, α5, α6, α7 to get the original data A1,A2,A3,A4,A5, A6, and A7 respectively. Then the bit at MSB of each of these data i.e. A0-A7 is copied into bit positionsbo-b7 to form a new byte γ.

vii. Then, β and γ are compared. If both are same then it is ensured that A0 to A7 sent from the sensor are properly received at the destination end as generated by the sensor originally.

viii. Otherwise, if β and γ are not same, then it means the data received are not the original ones, some intrusions might have taken place. If the same thing continues for the next sets of data also, then it is confirmed that some malicious act is there and actions should be taken to get rid of that.

This is depicted as below:

Let us consider A0 -A7 as 30, 226, 7, 50, and 35,225,6,80 respectively. On applying SREE protocol:

Step i: A0 $\rightarrow 30_{10} \rightarrow 00011110_2 \rightarrow$On applying Circular Left Shift $\rightarrow 00111100_2 \rightarrow 60_{10} \rightarrow \alpha 0$.

Step ii: Bit at position b7 of A0 is 0. It occupies bit position b0 of β. i.e.

							0

Step iii: After mapping α0 with the mapping table M the encrypted code will be identified and sent.

Step iv: Steps i to iii will be repeated for A1 to A7, and subsequent bits for β will be inserted. The same process will be repeated for the subsequent sets of data, wherein each set contains 8 data.

Steps v to vii: The decryption process at the receiving end includes the reverse operation. I.e. For each set of 8 data, this includes, identification of bit combination from mapping table M for the encrypted code received. Applying circular right shift to it. Copying MSB into bit position starting from b0 of a new byte γ.

Step viii: Then γ will be compared with the received β. If both are same then it ensures the authenticity of the received set of 8 data.

6 Experimentation and Results:

Applying SREE protocol for data encryption and decryption or recovery of original data from the encrypted code is a viable solution in a wireless sensor network, because it provides security with minimal computational and processing overheads, which is more or less like sending the original sensor data, but this simplified encryption methodology makes it possible with better security, with the available constraints in the processing, storage capacities and battery power of the sensor nodes. Also integrity and authentication of the received data is ensured. This is depicted by the following table and the corresponding graph.

S.NO	TEMPERATURE	VOLTAGE	CURRENT	RPM	SAMPLING TIME(Sec)	DATA UPLOAD WITHOUT ENCRYPTION (ms)	DATA UPLOAD WITH ENCRYPTION (ms)
1	30	226	7	50	3	0.12	0.124
2	35	225	6	80	5	0.13	0.134
3	35	229	6	80	7	0.11	0.113
4	40	230	6	150	9	0.12	0.124
5	45	228	6	150	11	0.11	0.113
6	50	230	6	150	13	0.15	0.154
7	55	227	6	300	15	0.09	0.092
8	60	226	6	300	17	0.13	0.134
9	60	226	6	300	19	0.12	0.123
10	60	228	6	300	21	0.09	0.091

Table 1: WSN Data generated by household equipment and is uploaded with 300Kbps bandwidth

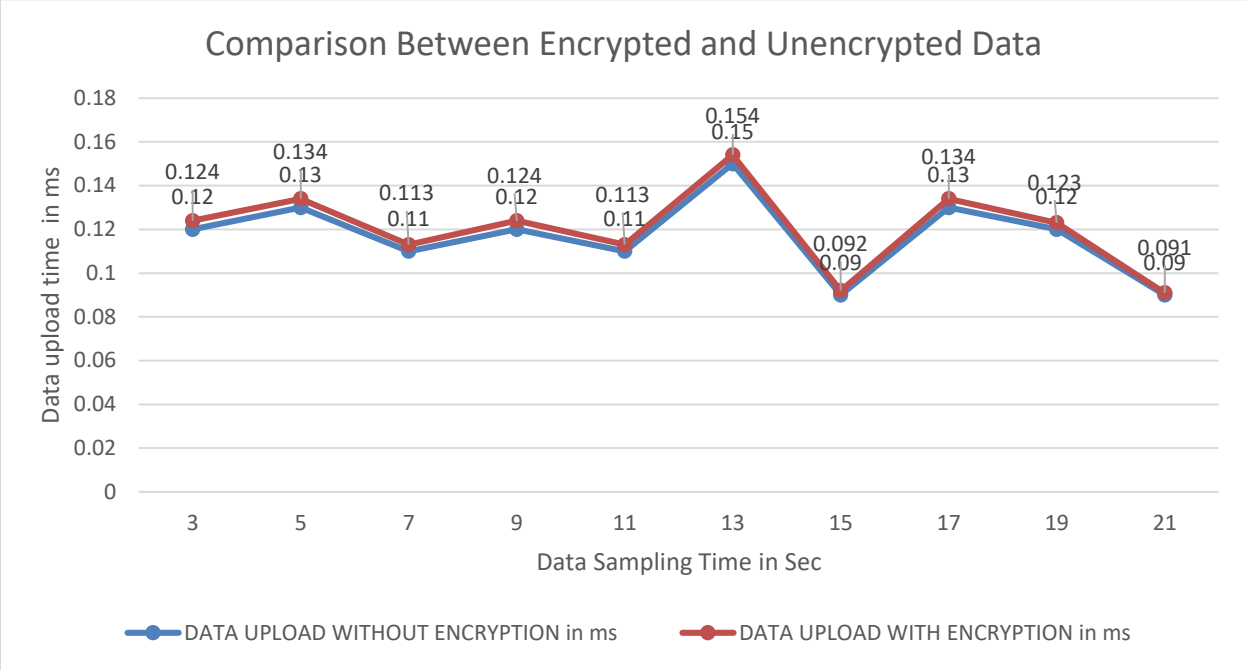

Fig 2: Graph showing the time taken for transmitting data without encryption and for transmitting data with encryption using SREE protocol.

In this protocol, the security can further be improved by periodically shuffling the mapping table entries and reassigning symbols. This should be updated in all the sensor nodes and at the receiving end. Also, periodically the circular shifting can be varied at intervals, like instead of circular left shift at the sensor side, it can be changed as circular right shift. Then at the receiver side the reverse operation should be implemented. Such modifications will yield more security because the adversary may find it difficult, if no fixed standardization is maintained in the protocol, resulting in more and more secured data transmissions.

7 Conclusion

In this paper, a new methodology is proposed, by which the data generated by the wireless sensor networks will be encrypted based on SREE protocol. This provides better security with minimal computational and communication costs. It ensures integrity, authentication and confidentiality of the data sent from the sensor nodes. Also, this protocol can identify if any malicious act is affecting the sensor data and alerts to take actions against such threats.

8 Future Work

However, depending on the security requirements, additional changes can be incorporated without considerable increase in the computational costs for the benefit of providing additional improvements in the security.

9 References

[1] Secure Data Aggregation with Homomorphic Primitives in Wireless Sensor Networks: A Critical Survey and Open Research Issues, Haythem Hayouni, Mohamed Hamdi, Proceedings of 2016 IEEE 13th International Conference on Networking, Sensing, and Control Mexico City, Mexico, April 28-30, 2016.
[2] C.Castelluccia, E.Mykletun, and G.Tsudik, Efficient Aggregation of Encrypted Data in Wireless Sensor Networks, MobiQuitous, 109-117, 2005.
[3] S.Ozdemir, and Y.Xiao, Integrity protecting hierarchical concealed data aggregation for wireless sensor networks, Computer Networks, Vol.55, 1735-1746, 2011

[4] C.M.Chen, Y.H.Lin, Y.C.Lin, and H.M.Sun, RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks, IEEE Transactions on Parrallel and Distributed Systems, Vol. 23, 2012.
[5] Sensor Data Encryption Protocol for Wireless Network Security, Bharat Singh, Parvinder Singh & Dr. V.S. Dhaka, Global Journal of Computer Science and Technology Volume XII Issue IXVersion I, April 2012
[6] AlokRanjanPrusty et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, 4028 – 4037. The Network and Security Analysis for Wireless Sensor Network: A Survey
[7] Survey of Wireless Sensor Network Security, Doug Reitz, Binghamton University, May 2006
[8] An Evaluation of Security Protocols on Wireless Sensor Network Abu ShohelAhmed,Helsinki University of Technology, TKK T-110.5190 Seminar on Internetworking, 2009-04-27