JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-3, Issue-5 E-ISSN: 2347-2693

New Cryptography Algorithm to Provide Security for Wireless Sensor Network

Satyajeet Shinge[1*] and S. S. Sambare[2]

[1*,2]*Department of Computer Engineering, Pimpri-Chinchwad College of Engineering,*
Savitribai Phule Pune University, India.

www.ijcseonline.org

Received: May/02/2015 Revised: May/10//2015 Accepted: May/24/2015 Published: May/30/ 2015

Abstract— Wireless Sensor Network contains tens to hundreds of nodes used to monitor the environment conditions. The data monitor by these nodes is sent to the main location. This data can be humidity, pressure, temperature, density, etc. Current applications of WSN are area monitoring, Health care monitoring, Forest fire detection, Water quality monitoring, battlefield monitoring, etc. Many of these applications can have sensitive data to transfer to the base station. This data can be forged by the adversary during its transfer. Hence security is one issue in Wireless Sensor Network. The recent research shows that the security can be improved using modified cryptographic algorithms in the sensor network. In this paper, we propose one simple cryptographic algorithm using ASCII values of original data. This algorithm can be used to encrypt the sensed data before its transfer.

Keywords—WSN; cryptography; security; ASCII

I. Introduction

Wireless sensor networks have gained immense importance over the years due to their low cost and useful applications. WSN consist of very small sensor nodes, which senses the change in physical or environmental conditions [1]. The energy, the storage capacity and communication capability of sensor nodes are very limited [2].Wireless sensor networks are used in the fields of medical care, battlefield monitoring, and environmental monitoring, surveillance and disaster prevention. All these applications of sensor networks require that the network should be efficient, fault tolerant, tamper resistant and secure. Wireless Sensor Network transfers the sensitive data to the base station. Any attacker can monitor the traffic flow and interrupt, modify or fabricate data during transfer and can provide wrong information to the base stations or sinks. Security is a broadly used in term of [3]:

- Data Authentication: It ensures that the data is initiated from the exact source.
- Data Confidentiality: It ensures that only authorized sensor nodes can get the content of the messages.
- Data Integrity: It ensures that any received message has not been modified when it is sent by unauthorized parties.
- Availability: It ensures that the services offered by WSN or by a single node must be available whenever necessary.
- Data Freshness: It ensures that no old data have been replayed.

For the secure transmission of information over Sensor networks, several cryptographic, stenographic and other techniques are used which are well known [9]. In this paper, we propose a simple symmetric encryption algorithm using ASCII values of Data. The data encryption algorithms used in WSN is generally divided into three major categories: symmetric-key algorithms, asymmetric-key algorithms, and hash algorithms. Our proposed algorithm uses same key for encryption and decryption, hence it is called symmetric key encryption algorithm.

II. Related Work

In paper [4] author proposed a secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) to find the multiple paths between the source and destination based on the rate of energy consumption and filled queue length of the node. It addresses different security threats like spoofing or altering the route information, selective forwarding, sinkhole attack, Sybil attack and Byzantine attack. Security is provided by using the digital signature crypto system. This crypto system uses the MD5 hash function and the RSA algorithm.

In paper [5] author proposed a randomized multipath routing algorithm. In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent. As a result, a large number of routes can be potentially generated for each source and destination. To intercept different packets, the adversary has to compromise or jam all possible routes from the source to the destination which is practically not possible. It uses three phase for securing the data in WSN, secret sharing of Information, randomized propagation of each information Share, and normal routing.

In paper [6] author proposed modified version of the EENDMRP (mEENDMRP) by adding a transmission range adjustment to improve the energy efficiency. This protocol has two phases: Route construction phase and Data transmission phase. In Route construction phase routing table construction, distance exchange and public key exchanges will be done. In Data transmission phase multiple paths are found based on the primary path and the data is transmitted.

In paper [7] author proposed a secure cluster based multipath routing protocol (SCMRP) which is a combination of clustered sensor networks and multipath sensor networks. Clustered sensor networks to increase the efficiency i.e. increase system throughput, save energy and decrease system delay by data aggregation and multipath sensor networks to increase the resilience and reliability of the network. SCMRP uses a cryptographic algorithm to provide security to the sensor network. SCMRP provides security against various attacks like altering the routing information, selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack etc.

In paper [8] proposed the key techniques and probabilistic multi-path redundancy transmission (PMRT) to detect wormhole attacks. Id-based key management scheme is used for wireless sensor networks to build security link and detect wormhole attack. The proposed approach reduces the communication overhead as well as saves node energy.

In paper [9] a secure routing scheme for heterogeneous sensor networks. In the proposed scheme, routing tables are generated with multipath routing. Base station generates inter-cluster routes and cluster head generate intra-cluster routes. This minimizes the computation load on cluster nodes. It also provides light-weight broadcast authentication used for secure routing table generation and data communication; and to reduce communication overhead.

III. PROPOSED WORK

The main motivation behind the cryptographic algorithm is to provide security in WSN when data or information is transfer to the main location. Each of the nodes should provide security enough by using simple and more efficient algorithm. In this paper we proposed a cryptographic algorithm to encrypt data using its ASCII value. The main aim of this algorithm is to encrypt the data in less time.

A. Algorithm to perform encryption in proposed algorithm

Encryption steps are as follows:

1. Convert all characters of input plaintext into its ASCII values and store it in asciiArray.

Input	h	e	l	l	o
asciiArray	104	101	108	108	111

2. Find minimum value minValue from asciiArray.
3. Now Perform modulus operation on each value of charArray by minValue and store result into charMod

asciiArray	104	101	108	108	111
charMod	3	0	7	7	10

4. Automatically generate a key having length equal to the length of plaintext and store it to charKey array.

asciiArray	104	101	108	108	111
charMod	3	0	7	7	10
charKey	R	T	L	J	H

5. Convert all the character from charKey array into ASCII value and save it to asciiKey array.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72

6. Find minimum value minKey from asciiKey.
7. Perform modulus operation on each value of asciiKey by minKey and store result into keyMod array.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72

8. Now add keyMod array into charMod to form encrypted key encKey.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72
keyMod	10	12	4	2	0
encKey	13	12	11	9	10

9. Now add minValue to each value of encKey array to get ciphertext of plaintext.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72
keyMod	10	12	4	2	0
encKey	13	12	11	9	10
asciiCiphertext	114	113	112	110	111
ciphertext	r	q	p	n	o

B. Algorithm to perform decryption in proposed algorithm

Decryption steps are as follows:

1) Convert all characters of ciphertext into its ASCII values and store it in decArray.

ciphertext	r	q	p	n	o
decArray	114	113	112	110	111

2) Now substract value of final encrypted key encKey from value of decArray.

ciphertext	r	q	p	n	o
decArray	114	113	112	110	111
difference	101	101	101	101	101

3) Add decArray and charMod to generate original plaintext.

ciphertext	r	q	p	n	o
decArray	114	113	112	110	111
difference	101	101	101	101	101
asciiPlaintext	104	101	108	108	111
Plaintext	h	e	l	l	o

IV. RESULTS AND DISCUSSION

Table 1 shows the result of proposed algorithm for different size of strings. It shows that execution time require to encrypt those strings is very less. This result is compared with existing algorithm [11]. Result shows that proposed algorithm has very less execution time as compared to existing algorithm. Table 2 shows the different plaintext and their automatically generated keys.

Size of plaintext	Execution time for existing algorithm in ms	Execution time for proposed algorithm in ms
2	322	15
4	3679	15
6	3861	16
8	4748	16
10	5543	30

Table 1: Comparison of Execution Time between Existing Algorithm and Proposed algorithm.

PlainText	Automatically generated Key	CipherText
Abcd	BJWU	ajxw
Abcdef	WRGQSL	qmcnqk
Abcdefghi	LCFNAQDMP	ldhqevjtx

Table 2: Results of Proposed Algorithm for different Plaintext

V. CONCLUSION AND FUTURE WORK

In this paper, a simple cryptographic algorithm is proposed to encrypt the data or information stored in sensor nodes. This algorithm gives good result in less time and works on Low power and Energy. Hence it provides security as well as it will help to save the energy of sensor nodes.

This algorithm supports only text data. In future we will improve the algorithm to support multimedia data

REFERENCES

[1] Hasan Tahir and Syed Asim Ali Shah, "Wireless Sensor Networks – A Security Perspective", Multitopic conference, INMIC 2008, IEEE International, **2008**, pp.**189-193**.

[2] Satyajeet R. Shinge, S. S. Sambare, " Survey of different Clustering Algorithms used to Increase the Lifetime of Wireless Sensor Networks", International Journal of Computer Applications, **2014,** vol. 108, pp. **15-18**.

[3] Hero Modares, Rosli Salleh and Amirhossein Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks", Third International Conference on Computational Intelligence, Modelling & Simulation, IEEE **2011,** pp**.308-311.**

[4] Shiva Murthy G, Robert John D'Souza and Golla Varaprasad "Digital Signature-Based Secure Node disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE Sensors Journal, VOL. 12, Issue-10, **2012**, pp.**2941-2949**.

[5] G.Rohini, "Dynamic Router Selection and Encryption for Data Secure in Wireless Sensor Networks, Information Communication and Embedded Systems (ICICES), IEEE 2013 International Conference on , **2006**, pp. **256 - 259**.

[6] Sangeetha R. and Yuvaraju M. "Secure Energy-Aware Multipath Routing Protocol with Transmission Range Adjustment for Wireless Sensor Networks", Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on, **2012**, pp. **1-4**.

[7] Suraj Kumar Sharma and Sanjay Kumar Jena, "SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks," Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), **IEEE 2010**, pp. **1-6**.

[8] Guiyi Wei and Xueli Wang "Detecting Wormhole Attacks Using Probabilistic Routing and Redundancy Transmission," International Conference on Multimedia Information Networking and Security**, IEEE 2010**, pp. **496-500.**

[9] Aasma Abid, Mukhtar Hussain and Firdous Kausar, "Secure Routing andBroadcast Authentication in Heterogeneous Sensor Networks", International Conference on Network-Based Information Systems, IEEE **2009**, pp. **316-320**.

[10] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong. "Security in Wireless Sensor Networks: Issues and Challenges", 8th Conference on Advanced Communication Technology, IEEE **2006**, pp. **1043-1048**.

[11] Akanksha Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJCSE), **2012**, Vol. 4, pp. **1650-1657**.