SECURED DATA AGGREGATION USING FIBONACCI NUMBERS AND UNICODE SYMBOLS FOR WSN

Mohamed Yacoab
Assistant Professor, Department of Computer Science
MEASI Institute of Information Technology Chennai, India

Mohammed Sha
Assistant Professor, Department of Computer Science
Prince Sattam bin Abdulaziz University, Saudi Arabia

Mohamed Mustaq Ahmed
Academic Advisor, Edgeover Technologies, Chennai, India

ABSTRACT

Wireless Sensor Network is a combination of one or more nodes basically used for data collection and data aggregation. The collected data is aggregated through a data aggregator and it will be sent to bases station. While data transfer takes place, the intruders sniff the data that are being transmitted from one node to another. In order to prevent data sniffing by the intruder a study is made to prevent data sniffing and data breaching its boundaries. A two-fold cryptographic method is proposed using Fibonacci number and Unicode systems. The proposed method is two-fold viz, converting the normal simple text to secret message ii) convert secret message to Unicode text. The proposed method uses a two-fold security key encryption algorithm for transfer of data in the Wireless sensor networks and a decryption algorithm is also provided to convert back to its normal plain text.

Keywords: Cipher Text, Data Aggregation, Sensor Networks, Fibonacci Number System, Unicode Symbols.

Cite this Article: Mohamed Yacoab, Mohammed Sha and Mohamed Mustaq Ahmed, Secured Data Aggregation using Fibonacci Numbers and Unicode Symbols for WSN, International Journal of Computer Engineering and Technology, 10(1), 2019, pp. 218-225.

http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=10&IType=1
1. INTRODUCTION

A collection of tiny electronic devices capable of send and receive messages between themselves is known as Wireless Sensor Network (WSN). WSN is organized and used in many applications such as weather forecasting, oil exploration, agriculture, farming, smoke detectors and military operations etc, [1]. It provides solutions potentially in low-cost for the issues of defense and general public applications which enhances monitoring the Warfield, precise target tracking, ecological and health care monitoring, detection of forest fire, and traffic monitoring [2]. Every sensor node in a WSN has a limited power and computation capability. [3]. The unique characteristics of WSN are: deployment of sensor nodes, sensor nodes are operated under battery-powered, dynamically configurable at need of hour. [4].

The cryptography techniques consist of two processes namely encryption and decryption methods. Most of the cryptographic techniques use patterns, standard RS-232 algorithms to convert plain text to cipher text and vice versa. Cryptography had a wide range of uses namely in espionage, secured data communication, military data transfer and in steganography operations. Today in the internet world, data transfer is of prime importance; to secure the data over transmission on the internet we need to use cryptography techniques. [14]

![Figure 1 Wireless Sensor Network diagram](image)

2. EXISTING DATA AGGREGATION TECHNIQUES

The Wireless Sensor Network consists of low-cost and energy restricted sensor nodes. The data transmission between the sensor nodes should be considerably reduced because of the limited energy available in the sensor nodes. The energy of the nodes, node’s lifetime and the bandwidth can be utilized efficiently by reducing the number of the data transmissions. A lot of data aggregation techniques have been developed, and some of them are going to be discussed in this section.

Huseyin Ozgur Tan et al [5] have suggested that the protocols developed are basically centralized algorithms where the base station computes the routing information. The Energy competent Data gathering and Aggregation procedure works on the basis of the assumption that the locations of all nodes are known previously by the base station.

Qiang Ma et al [6] have suggested a design that smoothly integrates the data collected by data aggregation techniques applied on the nodes into WSNs and presented a single error correction algorithm for data aggregation by fully utilizing the intrinsic correlations that is present between sensor nodes. Their work does not affect the existing data aggregation algorithms and can improve the reliability of aggregation algorithms.

Kai-Wei Fan et al [7] have suggested implicit methods are used in data aggregation to collect data from the sensor nodes. A robust method is highly needed for efficient aggregation in which the data node packets need to meet at the particular node at a particular similar time.

Jio Gao et al [8] have analyzed the problem of data aggregation from a limited set of nodes in a WSNs. The ability of sensor nodes to find the similar nodes in the network which
Secured Data Aggregation using Fibonacci Numbers and Unicode Symbols for WSN

needs to exchange a data between nodes at a particular time is highly dependent on the distance between the nodes.

Zhenzhen Ye et al [1] have proposed a new distributed method to reduce data communication in WSN based on fuzzy logic numbers and weighted average operators. The core idea of their method is that every sensor node preserves an approximation of the aggregated data value. By analyzing the aggregated data value the sensor node make a decision whether a new data value to be calculated by the sensor nodes or the data values to be received by a communication message that communicated along the sensor network.

Cunqing Hua et al [9] have suggested a best routing algorithm and a efficient data aggregation plan for WSNs. A method is devised for the optimization problem by combining the data aggregation techniques with the designed routing plan to obtain a smoothing approximation function. To meet the above criteria, a novel algorithm is designed with the all the vital conditions to achieve the optimization.

Prakash G L et al [10] made an effort to support network scalability, with a method that works well with Tree on DAG (ToD) approach. The method forwards the data packet in a robust manner on the construction made of various minimum path trees. The standard working idea of this approach is that the nearby sensor nodes will be in the next tree level when the data aggregation completes early. They have proved that their semi-structured approach can provide well-organized data aggregation in vast scale sensor networks.

Bo Yu et al [11] have suggested a data aggregation procedure using a collision-free distributed method for WSNs. By using the greedy method, the time delay of the data aggregation schedule be is minimized.

Tharini et al [12] have proposed a modern method to collect the data from then sensor nodes by using the time based correlation coefficients approach. Instead of collecting data by data the algorithm collects the data in a compressed way so that the sink will receive more data at a particular time period.

2.1. Forming of Tree structure

To create a data aggregation tree, a random number is selected by each node from the value provided as weight to that sensor node. In the sensor network, certain nodes are believed that they have detected something of interest and are considered as 'hot' nodes. The data aggregation tree is created by the values (weights) of the hot nodes. Thus for the following data aggregation, a spanning forest is created with the hot nodes which all are connected to the sensor network boundary.

2.2. Data Aggregation

Once the spanning forest is created, it is necessary to have a full check of data flow on all the data nodes in the sensor network. The data aggregation procedure had a feature to integrate data aggregation and spanning forest ration at the same time. By choosing the minimum hot nodes, the spanning forest achieved the tree structure for data aggregation.

2.3. Features of cryptograph

The features of cryptography consist of a numbers of parameters. Some of the important and most used parameters are listed below [13]

Authentication: this process gives the information to the data about the sender

Privacy: In this feature the data is encapsulated and available only to the authorized stake holders
Integrity: binds the data associated within and subsequently leads to tamper-proof data transfer

Non-repudiation: confirms the source of data from which point the data has been sent

2.4. Different crypto algorithms

Symmetric Cryptographic Algorithm

The Symmetric cryptographic algorithm employs a single key for encryption and decryption of the data. The limitation of the symmetric key is the sender and receiver should know the key used for encryption and the same is used for decryption.

Asymmetric Cryptographic Algorithm

This algorithm uses a two key system called key-pair namely a couplet [public key, private key]. The public key is made openly available to all. On encryption the algorithm uses two key to encrypt namely the public key and private key. On the receiving end, the process of decryption uses the same public key and it uses a private key which is known only between the sender and the receiver. The limitation of this algorithm is if the private key is not known to the receiver he cannot decipher the text.

Hash Function Cryptographic Algorithm

The hash function algorithm works with fixed key encryption method to convert the plain text to cipher text. For example, in digital finger print of file can be accomplished by the use of hash functions that cannot be altered at any cost by the intruder.[18]

3. PROPOSED SOLUTION USING FIBONACCI NUMBERS AND UNICODE SYMBOLS

Encryption is carried out by using Fibonacci numbers the input which is of plain text is converted to ciphertext. The cipher text is again encrypted to Unicode symbols and the output will be saved in a text file. The Unicode symbols are converted to cipher text by the decryption process and the subsequent procedures involved to convert the cipher text to plain text. The figure will explain the process of encryption and decryption process clearly.[15]

![Diagram of Encryption and Decryption using Fibonacci-Unicode Symbols Algorithm](image)

**Figure 2** Process of Encryption and Decryption using Fibonacci-Unicode Symbols Algorithm

3.1. Algorithm Phase -1: Plain Text To Cipher Text by using Fibonacci series system

1. Let the Fibonacci series be 1,2,3,5,8,13,21………
2. Let the security key be [ a,b,c,d,e,f,g,h,I,j,k,l,m,n,o,p,q,r,s,t,u,m,v,w,x,y,z ]
3. Let the inputs are made to split as individual data. Chose any character from the alphabet as security key for the first data. Then subsequent data will be following the security chosen. As we are using round-robin once, once security key reaches its final...
Secured Data Aggregation using Fibonacci Numbers and Unicode Symbols for WSN

key, then it will prompt the first key and this process will be repeated till all the data will get the security key.

4. Then assign the first Fibonacci number to the key. The first Fibonacci will point the first key in the key list; second key will point the subsequent key; third will point the next key. And the next key will be taken based on the Fibonacci series until all the values are taken in to cipher text.

5. Repeat the above process until all the security key is assigned to the individual data on the input.

3.2. Algorithm Phase -2: Cipher text to Unicode using ASCII key

1. For each cipher text find the ASCII code.
2. Find and obtain the ASCII codes for the previous character and next character.
3. Add the all the above said ASCII values with ASCII value of the original node data.
4. The decimal data obtained after adding all the four ASCII values are converted in to hexa-decimal to obtain the Unicode.
5. The node sends the Unicode key will be sent along with the data in to unsecured channel of transmission.

3.2.1. Example demo of how node’s data is encrypted using the Fibonacci-Unicode two – fold algorithm

Input text: SMART
Character list: a,b,...z
Chosen Security key : v
Here a random key v selected as security key and assign to H; subsequently the remaining keys are allotted
Fibonacci number: 1,2,3,5,8
Once security key is chosen the numbering starts from 1,2,3,... when the security reaches the last key then by round-robin points to first character till it reaches the end.

| a | b | ... | v | w | x | y | z | a | b | c | ...
|---|---|-----|---|---|---|---|---|---|---|---|-----|
| S | M | A | R | T |
| 1 | 2 | 3 | 4 | 5 |
|   | v | w | x | z |
|   |   |   |   | c |

The generated cipher text : vwxzc
Now applying algorithm -2 ASCII code we derive the UNICODE

\[ v \rightarrow \text{ASC}(u) + \text{ASC}(v) + \text{ASC}(w) + \text{ASC}(S) \]
\[ = 98 + 99 + 100 + 83 = 380 = 17C \text{ (Hex)} \]
\[ w \rightarrow \text{ASC}(v) + \text{ASC}(w) + \text{ASC}(x) + \text{ASC}(M) \]
\[ = 98 + 99 + 100 + 77 = 374 = 176 \text{ (Hex)} \]
\[ x \rightarrow \text{ASC}(w) + \text{ASC}(x) + \text{ASC}(y) + \text{ASC}(A) \]
3.3. Encryption steps
1. The sender sends a message to the receiving node
2. The algorithm will be dynamic depends what user selects a security key from the alphabet list. The data is converted to cipher text by using Fibonacci methods.
3. The encrypted cipher text will be converted to Unicode symbols and the written to a file
4. Then the data will be transferred in a secured way to its recipients
5. The recipients will collect the data and encrypted to get the original message

3.4. Decryption steps
The file after encryption which contains the encrypted key will be sent to the decryption process. When the node receives the text file it reads the contents of the file gets the hex values. Then it reads the hex value and converts the hex to decimal. Using the ASCII key values the decryption algorithm converts to plain text.

4. ADVANTAGES OF THE PROPOSED SYSTEM
The algorithm uses such a method only the encryption method and the decryption method can able to understand the process. The algorithm is two-fold process. In first phase, the data is converted to cipher by maenads of implementing the Fibonacci series algorithm. In second phase, the cipher text is converted to Unicode symbols. Any intruder who sniffs to takes the node data wills not be able to decode because of high-security implementation carried out by complicated crypto algorithms. It is very hard to decode the data transfer implemented by means of Unicode Symbols. While transferring the data in an unsecured medium the intruder do not have any idea where the key had kept because transmission are done via the text file which contains only Unicode symbols.

5. SIMULATION SETUP
The simulation table is created with the necessary input data.

Table 1 summary of the simulation parameters used

| Total no of Nodes | 20,40…100 |
|-------------------|------------|
| Size of the area  | 520 x 520  |
| MAC               | 802.11     |
| Time taken for simulation | 50 seconds |
| Input Traffic Source | CBR     |
| Size of the data packet | 512          |
| Node Transmitting power | 0.660 watts |
| Node receiving power  | 0.395 watts  |
| Initial Energy at node | 3.10 Joules |
| Range set for transmission | 75 Meters |

http://www.iaeme.com/IJCET/index.asp 223  editor@iaeme.com

Electronic copy available at: https://ssrn.com/abstract=3537630
5.1. Parameters for measuring Performance

The quality of suggested algorithm SDFU is weighed against with ToD [10] protocols. The quality of the algorithm is rated based on the following metrics viz., control overhead, delay and packet deliverance ratio.

The results of varying nodes from 20-100 for SDFU and ToD techniques are tabulated in Table 2

| Nodes | Delay SDFU | Delay ToD | Delivery Ratio SDFU | Delivery Ratio ToD | Overhead SDFU | Overhead ToD |
|-------|------------|----------|---------------------|-------------------|--------------|--------------|
| 20    | 2.044958   | 2.663457 | 0.98655             | 0.861353          | 2203         | 2961         |
| 40    | 2.142764   | 3.147126 | 0.97239             | 0.811273          | 2424         | 3269         |
| 60    | 2.218459   | 3.215348 | 0.96876             | 0.743528          | 2669         | 3594         |
| 80    | 2.273687   | 3.312915 | 0.92342             | 0.708927          | 2734         | 3866         |
| 100   | 2.366057   | 3.400764 | 0.87316             | 0.670825          | 2975         | 4071         |

![Figure 3: Nodes Vs Delay](image1.png)

![Figure 4: Nodes Vs Packet Deliverance Ratio](image2.png)

![Figure 5: Nodes Vs Overhead](image3.png)

6. CONCLUSION

WSNs are used widely in the field of wearable devices, military operations, high security installations, government installations to transfer the data in a aggregated manner either spatial or temporal. Cryptography is the widely used to secure data communications. The algorithm used in our research paper will provide the concepts of data hiding, integrity, and authentication of data transfer between nodes in the WSN in a secured communication. The data transfer not only sends the data to the next node it also carries the vital information of the cryptographic keys which will be easy for the receiving node to decrypt the data sent by the
sender. Finally the Fibonacci – Unicode symbol algorithm implementation will provide a high quality secured communication in a unsecured communication of WSNs.

REFERENCES

[1] Croce, S., Francesco Massimo, "Minimising the power consumption in WSNs using a novel appr. to data aggregation", Computer Journal, vol. 51, no. 2, 2008.
[2] Ozdemir, Suat, “Secure data aggregation in WSNs: A comprehensive overview”, Comp. Nets, vol. 53, no. 12, 2009
[3] Cam, H. Energy-efficient and secure pattern-based data aggregation for WSNs s”, Procs of IEEE, vol. 2, pp. 732-736. 2003.
[4] Shio Kumar Singh, “Routing Protocols in WSNs –A Survey”, Intl Journal of Computer science and Engineering, Survey vol. 1, no. 2, pp. 63-83. 2010
[5] Tan, H. Ö., & Körpeoğlu, I, Power efficient data gathering and aggregation in WSNs. ACM SIGMOD Record, 32(4), 66-71. 2003
[6] Ma, Q., & Yoon, W. S. Data aggregation with error correction for WSNs. Inform. Technol. J. 4, 462-464, 2005
[7] Kai-Wei Fan, K. W., Liu, S., & Sinha, P, Structure-free data aggregation in sensor networks. Mobile Comp, IEEE Trans on,6(8), 929-942, 2007
[8] Gao, J., Guibas, L, Milosavljevic, N & Hershberger, J, Sparse data aggregation in sensor networks. In Procs of the 6th Intl conf on Infn Processing in sensor networks (pp. 430-439). ACM, 2007, April.
[9] Hua, C., & Yum, T. S. (2008). Optimal routing and data aggregation for maximizing lifetime of WSNs. Networking, IEEE/ACM Transactions on, 16(4), 892-903.
[10] Prakash, G. L, Tree-on-dag for data aggregation in sensor networks. In proc of World Academy of Science, Engg and Techy (Vol. 37). 2009.
[11] Yu, B., Li, J., & Li, Y. (2009, April). Distributed data aggregation scheduling in WSNs In INFOCOM 2009, IEEE (pp. 2159-2167). IEEE.
[12] C.Tharini and P. Vanaja Ranjan, “An Efficient Data Gathering Scheme for WSNs”, European Journal of Scientific Research, Vol.43 No.1 (2010), pp.148-155
[13] http://media.wiley.com, Chapter 1, Basics of Cryptography
[14] I. Venkata Sai Manoj, —Cryptography and Steganography, Intl Jourl of Computer Appl (0975 – 8887), Volume 1 – No.12
[15] Michał Kosmulski, Introduction to Unicode, http:// www. linux. com/ archive/ articles/39911
[16] B. B. Zaidan, On the Differences between Hiding Infn and Cryptography Techniques: An Overviewl, Journal of Appl Science (2010).
[17] A. Joseph Raphael and Dr. V.Sundaram, Secured Crypto-Stegano Comm. Through Unicode World of Computer Science and Infn Tech Journal Vol. 1, No. 4,138-143, 2011.
[18] Dipto Kapoor Sarmah, Neha bajpai, Proposed System for Data Hiding Using Crypto. and Stegano, Intl Journal of Computer Appl, Volume 8 – No. 9, 2010.