International Journal of Computer and Information Technology (ISSN: 2279 – 0764)
Volume 02– Issue 03, May 2013

Calculus Based Approach for Data Transmission in wireless sensor Networks

$Nayan^1$, $Swapnil\ Singh^2$ $Manoj\ Kumar^3$
[1] Tata Institute of Social Sciences,Mumbai, [2]Indian Institute of Management, Bangalore
[3] Icfai University, Dehradun , $India$,
Email:[1]$nayan@tiss.edu$,[2] $swapnil.singh@iimb.ernet.in$[3]$mimansak@gmail.com$

***Abstract*—Security and data are two inherent properties of wireless sensor networks. And when we are explaining about the transfer of data from sink node to base station it automatically acquires utmost importance. In this paper we have developed a novel approach to transmit gathered data from sink node to base station. We have applied different polynomial and algebraic functions with calculus method, so that all the logical intrusion can be challenged. Since, we are bind, not to use high complexity protocols because of the constrained resources. So, it is always a tough task to design and add all the features which is needed in a wholesome protocol. The part on which we are working is vulnerable, so there is need to design new and robust techniques which will be hard to spoofed.**

I. INTRODUCTION

Expanding knowledge creates space for many things. And from last two decades computer literacy has gained a pinnacle response from several areas. Particularly in computer networks wireless sensor networks has won the race because of this many new opportunities have mushroomed. Its advantages starts with data propagation technique as it needs unguided medium (i.e air) that is free. So it is an eye catching area also there is no any physical boundary for its expansion. These wireless sensor networks have created a web of information carrying networks. Wsns consist of small nodes which is a paradigm of small computers. It consist of memory space, a small processor and lifelong battery which works on solar power[8].

As there is no any any physical boundary so its applicability is enormous. Which ranges from normal houses, offices and most vulnerable military areas. Where to keep and transmit data is a daily challenge. The location of these nodes are remote in nature where it could not be updated or maintained. so it is a tough task for a network designer to implement wireless network protocols because of energy constrained and processing capability of these small processors. So, a basic method is followed in this paper (i.e) whole of the structure decentralized in different forms.

Pairwise keys which creates communication between two nodes and individual keys which creates communication link between sink node and base station play a crucial role behind data propagation. We have created a new method to gather data from tiny sensor nodes.And added a new concept to transfer data from sink node to base station. Our approach is quite mathematical in nature because we have applied calculus method and hide function which creates a shield for intruder to intrude in the network. In Data calculating section we have utilized the concept of matrix multiplication for data compilation which is quite new in nature.

These sensor nodes has a special type of sensor installed with them which works on heat ,light and pressure e.t.c. a light sensor communicate with another light sensor and in same fashion heat and pressure nodes works.The basic topology consist of large number of sensor nodes a sink node and base station. A sink node gathers data from all sensor nodes and transmits data to base station where all the data are organized and processed. Base station has a large memory space,more powerful processing units and robust security techniques.

The rest of the paper is organized as follows. Next section contains related work. The paper starts with basic assumption or normal topology which we have taken into account for writing the paper. After this, definitions are there which are utilized in this paper. It continues with the algorithm what we have proposed and also example is cited so that confusions can be eradicated. Finally Section 6,7 ends the paper with conclusion and Acknowledgement.

II. RELATED WORK

Different key schemes talks about there own advantages and disadvantages. Still new concept of communication still depends upon traditional Ecliptic curve schemes[5]. All new methods extend the old idea of Pairwise, individual and master key concepts. Also Determinstic key schemes include SNEP, TESLA,SPIN Which has their advantages and disadvantages. Neither of them has holistic approach to deal with wireless network. The new matrix based approach has given a new boost in the research of wireless sensor networks. Patricularly Park, Choi and Youn[3] proposed a new scheme called A noble

key pre distribution scheme with LU matrix for secure wireless sensor networks. This method is quite helpful in carrying the data from sensor nodes to base station.

Besides that Eschenauer and Gligor[2] plays a crucial by giving the formula for number of keys in any wireless networks. And Leonard Kleinrock and John Silvester [6] calculating wayback in 1976 that six is a magic number for wireless sensor network and till today it has been used which is shown my mathematical analysis with the help of probability in the paper Nayan, Swapnil Singh and Mahesh Kumar[8]. And without talking about Rene L Cruz [9] who have worked with calculus in wsns plays a crucial role . In fact through which we can know about the amount of data transferred from one point to another point.

III. Basic Assumption

There are different types of nodes situated on different distant places. The node distribution is static in nature means the location of nodes are fixed. The energy utilization from each node will be equal. Since the transmission lines is not secure so there will be continuous intrusion from outside. Each place is placed with different types of tiny nodes like pressure nodes, light nodes and temperature nodes. Data is carried from simple nodes with the help of different pairwise keys and individual keys method. Data is collected from these small nodes collected and transmitted to sink node, from it is again transmitted to base station. where all data are further processed and send to respective areas.

IV. Definitions

We start with a brief description of various concepts and definitions used in this paper.

- **Definition 1** : A hash function(H) is any well-defined procedure or mathematical function that converts a large, variable-sized amount of data into a small datum, usually a single integer and the value returned is called hash values.
- **Definition 2** :A Circular Reverse function(CRC) is a function that defines an operation of rearranging the entries in a tuple, by moving the final entry to the first position respectively. For example, CRC ((m, n, p, q) = (q, p, n, m).

V. Algorithm for carrying data from different nodes.

- **Step 1:** calculate number of nodes for carrying data.
- **Step 2:** carry out function and create a heterogeneous function which is used to carry data.
- **Step 3:** we will hide the whole function in new folder and then we will shuffle with CRC (circular function)
- **Step 4:** we will calculate the whole function with different val- ues which is gathered by the nodes which is installed in different locations
- **Step 5:** After this we will apply hash function which creates large data into small datum which is easy to carry and and transfer to base station.

A. *Method to create a new function for carrying data.*

Suppose we have to create a function for six nodes. We are taking six into account because six is considered to be magic number[6]in wireless sensor networks.

- **Step 1:** number of nodes = 6
- **Step 2:**

$$Y_(x) = Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 \tag{1}$$

Here each $Y_1..Y_6$represents different nodes. Y_1 can be pressure nodes,Y_2 may be temperature nodes. Hence for holistic data we have distributed each and every node with different mechanism of carrying data.

$$Y_1(x) = P_1x^2 \tag{2}$$
$$Y_2(x) = P_2x \tag{3}$$
$$Y_3(x) = P_3e^x \tag{4}$$
$$Y_4(x) = P_4log(x) \tag{5}$$
$$Y_5(x) = P_5sin(x) \tag{6}$$
$$Y_6(x) = P_6x^3 \tag{7}$$

It is visible that we have taken altogether different types of function. It ranges from quadratic, linear, logarithmic exponential and trigonometric functions. These functions are deployed with the complexity and sensitivity of the environment. Suppose place like military areas where latitude and longitude information are very important so these information can carried with the help of exponential function. Its complexity is quite high and at same time

data intrusion process is quite difficult. Another example information which is Boolean in nature (yes/no) or function which have values which is range bound .Then at that place trigonometric functions are used. Also while adding whole function we have used $\odot$ operator. We have used $P_1.....P_6$ as node identity so that it is used while identifying node and data writing.

- **Step 3:**Structure of whole function:-

$$Y_(x) = Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 \quad (8)$$
$$= P_1x^2 + P_2x + P_3e^x + P_4log(x) + P_5sin(x) + P_6x^3 \quad (9)$$

From here we can introduce a new approach where data writing can be done. Before that we are integrating this$Y_(x)$ and again $dy/dx(Z(x))$ .This will increase energy loss but still we will inculcate because regular intrusion will be going on to intrude data. Once the whole function will be integrated then additional constant will be added but once we differentiate it will reduces to zero hence all the additional things can be compromised and data can be correctly written on these function.

$$Z_(x) = \int \mathrm{Y}_(x)\,\mathrm{d}x \quad (10)$$

$=P_1x^3/3+c_1+P2x^2/2+c_2+P_3e^x+c_3+P_4x(logx1)+c_4P_5cos(x)+c_5+P_6x^4/4+c_6$

$=P_1x^3/3 + P_2x^2/2 + P_3e^x + P_4x(logx1)P_5cos(x) + P_6x^4/4+C$

Before entering into writing data block the whole function will be differentiated.

$$dy/dx(Z_(x)) \quad (11)$$

$=P_1x^3/3 + P_2x^2/2 + P_3e^x + P_4x(logx1)P_5cos(x) + P_6x^4/4+C$

$Y_(x) =P_1x^2+P_2x+P_3e^x+P_4log(x)+P_5sin(x)+P_6x^3$

Applying CRC on the $Y(x) = P_6x^3 + P_5sin(x) + P_4log(x) + P_3e^x + P_2x + P_1x^2 = CRC(x)$

- **Step 4:** This CRC(x) will be sending on the data writing center. So that data will be calculated there and it will be send to base station.

B. *Data calculating technique*

- **Step 1:**Once this CR(x) arrives to data writing center this is again rearranged and thus the calculation starts. Data tray formation takes place. All this data is arranged in matrix and hashing is done.
$Y_(x) = P_1x^2 + P_2x + P_3e^x + P_4log(x) + P_5sin(x) + P_6x^3$

- **Step 2:** Calculations

For node n_1 =[1, 2, 3, 4]: values= P_1 [1, 4, 9, 16]

Second noden_2 =[4, 9, 6, 8]:values=P_2[4, 9, 6, 8]

Third node n_3 =[0, 0.5, 3, 2]:values= P_3 [1, e. 5, e^3, e^2]

Fourth node n_4 =[10, 100, 54, 1]:values =P_4 [1, 2, 1.73, 0]

Fifth node n_5 = [900, 760, 540, 780]:values=P_5[1, .97, .80, .978]

Sixth node n_6= [1, 3, 5, 7]: values= P_6 [1, 9, 125, 343]

- **step 3:** creation of data tray: In this process we have formed two matrix. one matrix will contain the information of node id and second will contain the respective data.To distinguish which type of data is gathered by which node we will perform simple matrix multiplication.The advantage using this matrix multiplication is that data are separated and without having the prior knowledge of the node id matrix it is not possible to understand the compiled data.

$$d_1(x) = \begin{bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \\ P_6 \end{bmatrix}$$

$$d_2(x) = \begin{bmatrix} 1 & 4 & 1 & 1 & 1 & 1 \\ 4 & 9 & e^5 & 2 & .97 & 9 \\ 9 & 6 & e^3 & 1.73 & .80 & 125 \\ 16 & 8 & e^2 & 0 & .97 & 343 \end{bmatrix}$$

- **step 4:** Data compilation:

$$D_(x) = d_1 * d_2 \quad (12)$$

$$D_(x) = \begin{bmatrix} P_1 & 4P_2 & 1P_3 & 1P_4 & P_5 & P_6 \\ 4P_1 & 9P_2 & e^5P_3 & 2P_4 & .97P_5 & 9P_6 \\ 9P_1 & 6P_2 & e^3P_3 & 1.73P_4 & .80P_5 & 125P_6 \\ 16P_1 & 8P_2 & e^2P_3 & 0 & .97P_5 & 343P_6 \end{bmatrix}$$

- **step 5:** Applying hash on it:

$$H_D(x) = \begin{bmatrix} h_1 & h_5 & h_9 & h_{13} & h_{17} & h_{21} \\ h_2 & h_6 & h_{10} & h_{14} & h_{18} & h_{22} \\ h_3 & h_7 & h_{11} & h_{15} & h_{19} & h_{23} \\ h_4 & h_8 & h_{12} & h_{16} & h_{20} & h_{24} \end{bmatrix}$$

After hashing,we will send $H(D(x))$ to base station where all data will be gathered and further processed. Hashing will convert data into small data into datum base station will receive hash values and will apply $H^{-1}(D(x)) = D(x)$. from where all gathered data will be found. Since the unique identity will be used to further segregate data that from which type of node the data is calculated. Through- out this data transfer processes we have extensively used hide function. It will increase the traffic burden at the cost of energy but still it will be a challenge in terms of compromising security.

VI. Data transfer using calculus method

The best use of calculus in wireless sensor networks is that it gives the exact detail of the location or place. Basically when we are using the definite integration it means we are calculating Area under the curve. According to Rene L. Cruz[9].The amount of data from a stream that is transmitted on the link in the interval [x,y] is

$$A(x,y) = \int_x^y f(x)\,dx. \tag{13}$$

Here X and Y are the cordinates of location. For example when the location is like [3,8] on f(x)= $Y_1(x)$. $A(3,8)$ =

$$\int_3^8 Y_1(x)\,dx.$$

=

$$\int_3^8 P_1 x^2\,dx.$$

= $P_1$485/3
In case of data on co-ordinate axis it can be evaluated under trignometric function $[30\theta, 60\theta]$
=

$$\int_{30\theta}^{60\theta} P_5 sin(x)\,dx.$$

=$P_5$1.232
In this way we can use integration method to collect and compute data which is gatheredfrom distant places.

VII. Rules for construction of polynomial function:-

- It is advisable to keep the maximum length of polynomial function six. As six is considered as magic number[6] in wireless sensor networks.Beyond this transmission lines will degrade will effect the effeciency of wsns.

- It is advisable to follow ILATE principles before formulating of heterogeneous polynomial function. The ILATE stands for Inverse trigono- metric function, logarithmic, algebraic, Trigonometric and exponential. The complexity of function increases when we travel from left to right. As a safe network designer it is suggested that the more complex areas have more complex function so that it becomes a draconian affair for any intruder.

VIII. CONCLUSION

We have explained the process in which data transfer takes place from sink node to base station in robust way. However our approach is quite mathematical, so we have used different mathematical tools with hide function. Since, it enables the whole data to transfer without been figured out.The technique of formation of polynomial function with calculus method is a pragmatic approach which we have followed. We have tried to cover each and every aspect to enhance the security because of the importance of data transfer process. We will try to reduce the some complex functions without mitigating our main concern.

IX. ACKNOWLEDGMENT

The author wants to thank Mr. Gaurav Srivastava,Mr.Nishi Mani , Mr.Nakes Mani and Mr. Amit Kumar for there motivational support throughout this paper.

X. REFERENCES

References

[1] "Whitfield Diffie and Martin E. Hellman", *"New Directions in Cryptography", "IEEE Transactions on Information Theory",year = "1976",*

[2] "Laurent Eschenauer and Virgil D. Gligor". *"A key-management scheme for distributed sensor networks. In ACM Conference on Computer and Communications Security, pages 4147, 2002.*

[3] "Chang-Won Park, Sung Jin Choi, and Hee Yong Youn" *"A noble key pre-distribution scheme with lu matrix for secure wireless sensor networks. In CIS (2), pages 494499, 2005.*

[4] "Haowen Chan, Adrian Perrig, and Dawn Song" *"Random key predistribution schemes for sensor networks. In SP03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197, Washington,*

DC, USA, 2003. IEEE Computer Society.

[5] "Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and. D. Tygar." *"Spins: security protocols for sensor networks. In Mo biCom 01: Proceedings of the 7th annual international confer- ence on Mobile computing and networking, pages 189199, New York, NY, USA, 2001. ACM"*

[6] "Leonard Kleinrock and John Silvester" *"Optimum Transmission radii for packet radio Networks or Why Six is a Magic Number(1978) ieee.*

[7] "Nayan,Swapnil Singh,Mahesh Kumar Bhandari and Sanjay kumar" *"Pairwise keys generation using prime number function in wireless sensor networks In ACEEE International Journal on Network Security, pages 10-14,2011*

[8] "Nayan,Swapnil Singh and Mahesh Kumar" *"Revisiting graph theory with the help of probability in establishment of pairwise keys in wireless sensor networks,In 2012 International Conference on Information and Network Technology (ICINT 2012) IPCSIT vol. 37 (2012) IACSIT Press, Singapore.*

[9] "Rene L. Cruz *" A calculus for network delay, Part 1: Network Elements in isolation, IEEE transaction on information theory, vol:37, no.1 January 1991*