Application of Cryptography in Wireless sensor network

Mampi Saha
RTC Institute of Technology,Ranchi, India
Awadhesh Kumar
Ranchi University, Ranchi, India
B.P.Verma
BN Jalan College, Sisai, India

Abstract

Wireless sensor network (WSN) operate at a restricted range, where the sensor node communicates with other nodes of the network. Since its network area is limited. A series of networks are created to transmit the information from one node to another. If one of the networks gets corrupted, the whole series of network will get terminated. Hence the information will not be able to transmit. In this paper, with the help of cryptography, we write a sequence of codes using Laplace- Mellin Integral Transformation to ensure secure management and transfer of information even if a network gets degenerated. If we talk about the recent statics, there is a drastic increase in cyber crime level worldwide, this paper will help us overcome this difficult situation. Our main concern is to provide the users a relatively futuristic concept with regard to secure network which can work even if one of the many networks gets interfered.

Key word : Cryptography, Encryption, Decryption, Laplace-Mellin integral transformation

I. Introduction

Wireless sensor network (WSN) is regarded quite worthwhile considering the node to node transmission. It is precisely efficient in detecting the physical and environmental attributes such as temperature, humidity, wind intensity and direction. Which are then transmitted as signals to weather forecasting department, disaster management and also aid in tracking location. Specifically node to node transmission can occur in 2 ways, single hop and multi hop. Single hop network refers to direct transmission of information from first node to second node without the interference of any other node to convey the information whereas in multi hop more than 2 nodes are utilized, information is transmitted from first node to second node. Then, again it is transmitted to 3rd node and more nodes if required. It is mainly used for information transmission along a long distance but in comparison to single hop, it requires more energy and is time consuming. The main concentrations of the paper is route optimization and secure transmission of information.

Cyber crime has started an uproar in recent years. Before the global crisis of Covid-19 that struck us in December 2019 there were comparatively negligible reported cases of cyber crime. It is after the lockdown due to Covid-19 that there is substantial increase in the reported cases. During the lockdown, addiction to smart phones is the major reason for such cases. India ranks 80th in case of cyber crime everywhere there is a substantial increase in rate of cyber crime from 3,477 reports in 2012 to 65,893 reports in 2022. Our main aim is to transmit that information securely using multi-hop.

There is a rich history of cryptography to go into. Kryptos means "hidden" and graphia means "writing" in Greek. It means "art of writing in secret characters" in modern Latin. Our texts, messages, and other communication operations are secured by cryptography from being viewed by unscrupulous parties who might damage them. These days, cryptography is applied at a far higher level since it protects private data, portfolios, etc. Without realizing , people use cryptography all across the world to secure their communications and data. The field of cryptography is vastly beneficial and has much room for advancement.

Dall'Anese et al. [3] Packets are randomly routed according to outage probability in a unique approach to multihop routing for cognitive random access networks, which takes into consideration the unpredictability of propagation channels and interference levels in hierarchical spectrum sharing. The cross-layer optimization framework that is produced offers optimal routes, transmission probabilities, and transmit powers by utilizing channel and interference level statistics. This allows for the thoughtful adjustment of routing, medium access, and physical layer parameters to the propagation environment.

According to Jose et al. [7], device fingerprinting is one method of ensuring home automation security. These solutions can be used to identify the devices that connect to or request to be connected to the home automation system, but there are still issues with timeliness and authentication delay with this method. Enhancing the security of home automation systems can be sufficiently supported by focusing on the state and context of operation [8].

No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Prime no.	71	61	59	53	47	43	41	37	31	29	23	19	17	13	11	7	5	3	2

Prime number table (Table –I)

We define a table for the codes used below :

SPECE(-)	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

V	*W*	*X*	*Y*	*Z*	0	1	2	3	4	5	6	7	8	9	:	-	/	@
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40

Table –II

Initial step is route optimization

Here we take an example in which we consider a series of local network. We require to send an information from one node that is N_a to node N_p.

(i) N_a will search for the nearest network. For example, it has 10 to 20 network near it, the one to send it back the fastest reply in the form of 6- digit OTP, The message will be sent to that network.

(ii) Let's consider N_b sends the fastest response to N_a. Then N_a will send back the message to N_b with a 16 digit password P_{ab} encrypted by using Laplace Mellin integral transformation.

(iii) Then N_b will have to decode the encrypted 16 digit password, applying inverse Laplace Mellin integral transformation when the password is decoded.

(iv) It will search for the nearest network in forward direction. For example, let N_c be the nearest network, it will then again follow the same process.

(v) After N_c receives the message, it will then again be forwarded and this process will repeat itself towards N_p direction, till the message reaches its destination.

Where, N_a , N_b , N_c , … N_p all are nodes in a network. P_{ab} is encrypted password send between N_a to N_b .

Formula for Laplace - Mellin Transform to encrypt password

$$\mathfrak{LM}[f(l,m)] = F(s,p) = \int_0^\infty \int_0^\infty \frac{t^n}{(1+m)^n} e^{-sl} m^{p-1} dldm = \frac{\mathcal{T}(p)\mathcal{T}(n-p)}{\mathcal{T}(n)} \frac{\mathcal{T}(n+1)}{s^{n+1}} = \frac{n\mathcal{T}(p)\mathcal{T}(n-p)}{s^{n+1}}$$

When $p = 2$ and $s = 2$ (Code – 22)

Old no.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
New no.	41	40	39	27	16	19	27	37	6	20	35	11	29	5	26	4	28	9	30	14	38
New code	@	/		U	P	S	0	:	F	T	8	K	2	E	Z	D	1	I	3	N	-

Old no.	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
New no.	23	8	33	17	3	32	18	7	36	24	13	1	31	22	12	2	34	25	15	10
New code	W	H	6	Q	C	5	R	G	9	X	M	A	4	V	L	B	7	Y	O	J

Table –III

When $p = 3$ and $s = 2$ (Code – 23)

Old no.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
New no.	41	40	39	5	25	33	34	1	9	17	24	36	13	21	38	16	30	11	26	7	22
New code	/	@		E	8	6	7	A	I	Q	X	9	M	U	-	P	3	K	Z	G	V

Old no.	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
New no.	6	23	8	29	12	32	18	37	20	10	31	19	4	27	15	2	25	14	3	28
New code	F	W	H	2	L	5	R	:	T	J	4	S	D	0	O	B	Y	N	C	1

Table –IV

Process to convert password and code

Step 1: We generate a 16 digit password with the aid of 6 digit OTP. To create this password we sum up the 6 numbers and divide it with 3. Then apply the greatest integer function.

Step 2: The result we get will undeniably lie between 0 to 18 that is, it has 19 numerals in it, and with the use of prime table we analyze the data.

Step 3: By applying modulus 41 concept, we calculate the remainder from every step and arrange it in a lower triangular.

Step 4: With the application of number 2 table in the lower triangular form, we need initiate our password.

Step 5: We encrypt the password by using Code 22 and code 23 table. These 2 codes: code 22 and code 23 table are made with the help of Laplace Mellin integral transformation.

Step 6: Now we send 2 things to the receiver

i) An encrypted password ii) A code

Step 7: Now the receiver will decode the encrypted password. With the help of the code and apply it to retrieve the message once it retrieves the message, it becomes a sender and sends the message forward. This process will repeat itself till it reaches its destination securely.

Example-

$$\text{(i)} \quad \begin{array}{l} 71^0 + 0 = 1 \\ 71^1 + 0 = 71 \\ 71^2 + 0 = 5041 \\ 71^3 + 0 = 357911 \\ 71^4 + 0 = 25411681 \\ 71^5 + 0 = 1804229350 \end{array} \qquad \begin{array}{ccccc} 1 & & & & \\ 30 & & & & \\ 39 & 40 & & & \\ 22 & 37 & 7 & & \\ 4 & 0 & 29 & 40 & \\ 37 & 6 & 9 & 20 & 23 \end{array}$$

$$1 = 41 \times 0 + 1 \qquad 71 = 41 \times 1 + 30$$

$$\begin{array}{c} 5041 = 41 \times 122 + 39 \\ 122 = 41 \times 2 + 40 \end{array} \qquad \begin{array}{c} 357911 = 41 \times 8729 + 22 \\ 8729 = 41 \times 212 + 37 \\ 212 = 41 \times 5 + 7 \end{array}$$

$$\begin{array}{c} 25411681 = 41 \times 619797 + 4 \\ 619797 = 41 \times 15117 + 0 \\ 15117 = 41 \times 368 + 29 \\ 368 = 41 \times 8 + 40 \end{array} \qquad \begin{array}{c} 1804229350 = 41 \times 44005593 + 37 \\ 44005593 = 41 \times 1073307 + 6 \\ 1073307 = 41 \times 26178 + 9 \\ 26178 = 41 \times 638 + 20 \\ 638 = 41 \times 15 + 23 \end{array}$$

Password – A3/@V:GD 2@:FITW

New encrypted password with code 22 - /XOJH7:P@9J70T-6

New encrypted password with code 23 - @J1WYA8/T1Y7QVH

$$\text{(ii)} \quad \begin{array}{l} 3^0 + 9 = 10 \\ 3^1 + 9 = 12 \\ 3^2 + 9 = 18 \\ 3^3 + 8 = 35 \\ 3^4 + 9 = 90 \\ 3^5 + 9 = 252 \end{array} \qquad \begin{array}{ccccc} 10 & & & & \\ 12 & & & & \\ 18 & \_ & & & \\ 35 & \_ & \_ & & \\ 8 & \_ & \_ & \_ & \\ 6 & \_ & \_ & \_ & \_ \end{array}$$

$$10 = 41 \times 0 + 10 \quad 12 = 41 \times 0 + 12 \quad 18 = 41 \times 0 + 18 \quad 35 = 41 \times 0 + 35 \quad 90 = 41 \times 1 + 8 \quad 252 = 41 \times 6 + 6$$

Password – JLR0800H000F0000

New encrypted password with code 22 – 823@L@@F@@@0@@@

New encrypted password with code 23 – XMZ/O//I///7///

Now we comparing End to end delay and Latency using some data.

Simulation configurations

Variable	Value
Area	1000×1000 m^2
No. of node	50-400
Range of node	50m-100m
Connection	Wireless
Size of massage	100Kb-220Mb
Speed	2-15 km/h
Processing time	90s

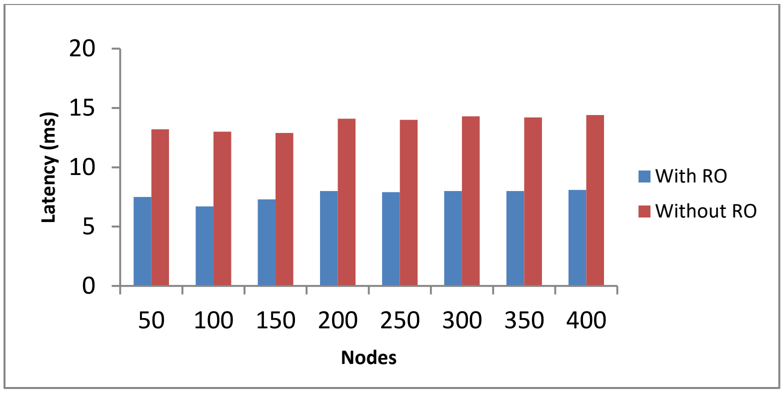

Fig. 1.

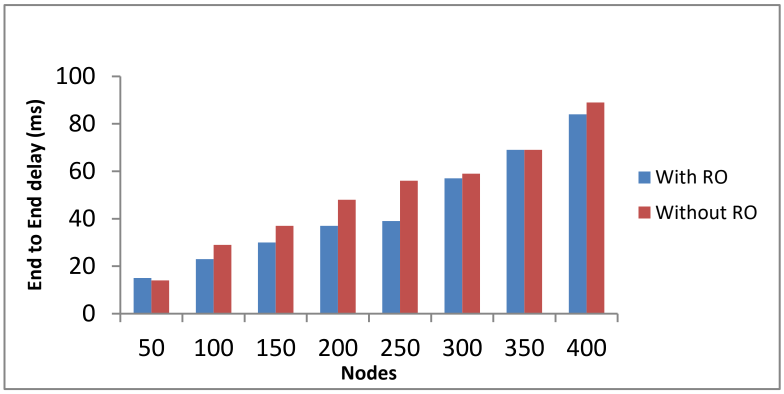

Fig. 2.

After comparing we get Fig. 1. By maximizing a network's bandwidth, this latency can be further managed. According to the findings, the suggested method offers 41% less handover latency than the default setting when RO is not used. The suggested approach's maximum delay is 7.71 ms, while the default scenario's maximum value is 13.7ms. The proposed strategy allows for 12.1% fewer delays than the default scenario when traffic is carried out via the network using the specified methodology, as illustrated in Fig. 2

Conclusion : In this paper, we deal with the secure node to node transmission with the help of cryptography. The proposed paper is entirely based on multi hop root optimization with the aid of Laplace Mellin integral transformation. The put forward approach shows that it is capable of providing secure transmission by overcoming the degenerate problem that is, damage of a network in the series of network would result breakdown of the whole network.

Reference :

[1] Koblitz n, Algebraic aspects of cryptography, springer-velag ,Berlin Heidelberg New York 1998.

[2] M.M.P. Singh and Mampi Saha, “Application of Laplace-Mellin Transform to cryptography”, International Journal of Mathematical Archive Vol 8(7), 2017, pp-143-146.

[3] E. Dall’Anese and G. B. Giannakis, “Statistical Routing for Multihop Wireless Cognitive Networks”, IEEE Vol.30(10). 2012,pp-1983-1993.

[4] D. Shin , V. Sharma , J. Kim, S. Kwon and I. You, “Secure and Efficient protocol for route optimization in PMIPv6- based smart home IoT networks”, IEEE Access, Vol 5(17). pp-11100-11116.

[5] A. C. Jose, R. Malekian and N. Ye, “Improve home automation security; integrating device fingerprinting into smart home”, IEEE Access. Vol. 4, pp-5776-5787, 2016.

[6] S. Madakam and H. Date, “Security mechanisms for connectivity of smart device in the internet of things”, in connectivity frameworks for smart Device. Cham, Switzerland: Springer, 2016,pp 23-41.

[7] A. C. Jose, R. Malekian, and N. Ye, ‘‘Improving home automation security; integrating device fingerprinting into smart home,’’ IEEE Access, vol. 4, pp. 5776–5787, 2016.

[8] Z. W. Kennedy et al., ‘‘Home security system with automatic contextsensitive transition to different modes,’’ U.S. Patent 9 501 924 B2, Nov. 22, 2016.