Journal of College of Education for Pure Sciences
Volume 8, Number 2, June 2018
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

Encryption of Data Transmitted Through Structure-free Wireless Sensor Networks

Zainab Shaker [1] ,KhaldunI.Aref[1] and Hussain Kamel Chaiel[2]

Zainab_alhassney@yahoo.com[1],Khaldun.i.a.2014@gmail.com[2],hkchaiel@Eng.utq.edu.iq[3]

(1) Thi-Qar University, College of Education for Pure Sciences, Computer Science Department

(2) Thi-Qar University, College of Engineering, Department of Biomedical Engineering

Abstract

Recently, the technology has been developed and wireless networks have received great interest in drawing the world's attention to the family. Wireless sensor networks are a set of sensor nodes specific resources that collaboratively working on the transfer or follow different phenomena(Chemical and physical) such as (sound, heat ... etc) and then transmit the information monitored wirelessly by connecting sensor nodes with each other until they reach the base station. There are two types of building mechanisms for wireless sensor network (WSN);structure-based and structure-free. The first is suffering from many problems which can be overcome when dealing with the other type. Most of the environments that deal with wireless sensor networks are difficult to reach and dangerous. Therefore, they are subject to many security breaches. These violations can lead to severe consequences and difficult to deal with in case they occur. Therefore, security must be provided through the network in one way or another taking into account that achieving security through the network is not easy because of the resources identified, especially as the security is the main issue and the first in many applications.

In this paper, the structure-free typeis applied and in order to achieve security, data transmitted through the network is encrypted using the Elliptic Curves Diffie-Hellman(ECDH) and the Rivest-Shamir-Adleman(RSA) algorithms.Simulation results demonstrate that the power consumption of the structure-free wireless sensor network with data encrypted by ECDH and RSAalgorithms.The results show that the power consumption by ECDH algorithm is better that RSA type with nearly 13%.

Keywords:WSN,Base Station, Encryption ,RSA,ECDH .

مجلة كلية التربية للعلوم الصرفة - جامعة ذي قار
المجلد ٨، العدد ٢، حزيران ٢٠١٨
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

Encryption of Data Transmitted Through Structure-free Wireless Sensor Networks

Zainab Shaker [1] ,KhaldunI.Aref[1] and HussainKamel Chaiel[2]

Zainab_alhassney@yahoo.com[1],Khaldun.i.a.2014@gmail.com[2],hkchaiel@Eng.utq.edu.iq[3]

(1) Thi-Qar University, College of Education for Pure Sciences, Computer Science Department

(2) Thi-Qar University, College of Engineering, Department of Biomedical Engineering

الخلاصة

في الآونة الاخيرة تطورت التكنلوجيا ولاقت شبكات الاستشعار اللاسلكية اهتماما بالغا لفت انتباه العالم بأسرة . انها عبارة عن مجموعة من عقد الاستشعار محددة الموارد (الطاقة والذاكرة ... الخ) التي تعمل بشكل تعاوني على نقل او متابعة الظواهر المختلفة (الفيزيائية او الكيميائية المحددة) مثل (الصوت والحرارة ... الخ) من ثم نقل تلك المعلومات المرصودة لاسلكيا من خلال تواصل عقد الاستشعار مع بعضها البعض لحين وصولها الى المحطة الاساسية . هناك نوعين من اليات بناء شبكات الاستشعار اللاسلكية هما structure- based و structure- free. اولهما يعاني من العديد من المشاكل والتي يمكن تجاوزها عند التعامل مع النوع الاخر . اغلب البيئات التي تتعامل شبكات الاستشعار اللاسلكية صعبة الوصول وخطيرة لذا فهي معرضة للعديد من الخروقات الامنية وهذه الخروقات قد تؤدي الى نتائج وخيمة وصعبة المعالجة في حال حدوثها لذا ولابد من توفير الامن خلال الشبكة بطرقة او بأخرى مع الاخذ بعين الاعتبار ان تحقيق الامن خلال الشبكة ليس بالهين مطلقا بسبب الموارد المحددة . خصوصا وان قضية تحقيق الامن هي القضية الاساسية والاولى في العديد من التطبيقات.

خلال هذا البحث تم العمل على مبدأ structure-free ولغرض تحقيق الامن تم تشفير البيانات المنقولة خلال الشبكة باستخدام خوارزمية Elliptic Curves Diffie-Hellman و Rivest-Shamir-Adleman. تستخدم اختبارات المحاكاة الحاسوبية لإظها راستهلاك الطاقة في structure-free wireless sensor network عند تشفيرالبيانات المنقولة خلال الشبكة بواسطة خوارزمية ECDH,RSA. وأظهرتالنتائجأناستهلاكالطاقةفي خوارزمية ECDH أفضلبنسبة ١٣٪ تقريبا مقارنتا مع خوارزمية RSA. تم استخدام MATLAB R2017-a خلال المحاكاة .

1. Introduction

Wireless sensor networks represent a distinct qualitative shift from traditional personal contacts between people in the physical world as well as in telecommunications. Traditional sensor networks have been identified as one of the most important 21st century technologies and are expected to be used more widely and meet more interest in various fields and will revolutionize the observed in the near future. In recent years the desire for communication has been the cause of the exponential growth of wireless communications, providing wireless sensor networks bridge between virtual and real world .Wireless sensor networks today are widely used in military areas, commercial areas, environmental monitoring, surveillance, health care and others[1]. WSNs have the ability to follow various phenomena in the real world as they have the ability to generate new scientific suggestions.It is expected to have a much larger spread than now.

Wireless sensor networks (WSNs) consist of a wide range of sensor nodes whose characteristics differ depending on the application used. They are usually small, cheap, and spread in different geographic locations to monitor events in the observation area and work on the cooperative transfer of information until the information reaches the base station .This sensor nodes is usually deployed in areas of great importance. The deploymentis either random, especially if the area is unsafe (dangerous) or is deploymentregularly (non-random) if the area we are working on is safe and human access is easy. These small sensor nodes transmit information by means of cooperation between each other (sensor nodes communicate with one another using radio signals). The size of these sensor nodes varies depending on the application you are working on. Their size may be small in battlefield monitoring, for example[2],…. .Sensor node consists of sensing unit, processing unit, communication unit and power unit [3]. These node sensors specific resources such as energy, memory and others. So the biggest challenge in wireless sensor networks is how to keep these resources as long as possible because once consuming those resources fully means the entire network stops monitoring information. The only source of sensor node life is the battery fitted or supplied. The mechanisms of building the sensor networks are two types of structure-based [4] and the other is structure-free [5]. Protocols to which the mechanism of building a structure-based suffer many problems . These problems can be overcome through the other, structure-free.

In recent years, wireless technology has evolved significantly, so it was necessary to provide security for information transmitted wirelessly. With the increased use of wireless sensor networks in various fields such as health, commercial and military, the security of the data transmitted during the wireless sensor network is very important.Information security is used to prevent unauthorized access to information and to perform various operations on such information, such as the use,

disclosure, disabling, destruction or modification of such information. Information security has many objectives in relation to the protection of information against any risks to which such information may be exposed. The type of risk to which the data is exposed varies by application [6].Information security can be defined as the set of controls or safeguards that are placed on the data for the purpose of protecting it against the risks that may arise. Because any change in these data can lead to serious consequences where the importance of this information comes from the characteristics of that information and therefore any change in that information may result in something very dangerous. Also, this information may be important and confidential and should not be viewed by all people so there must be a set of controls on those data to protect it. To ensure the security of information and to ensure that such information is fully secure, it must be protected from any potential breach, change or violation .Since the sensor networks have taken on a large scale and have become very important in recent years as they are considered to be the most advanced technologies. Messages sent through this type of network are wireless and make them vulnerable to many attacks and security breaches . As wireless sensor networks are used to monitor or follow up information, such information may be important and should not be viewed by any person who is not authorized to have access to such information.Wireless sensor networks that are specific materials have developed many techniques in recent years to deal with these specific resources and design a number of security protocols [7].

The main security goals for WSNs are data confidentiality ,data integrity and authentication, data availability , Data freshness , self-organization , time synchronization and secure synchronization [8]. Confidentiality can be achieved through encryption. Security information uses encryption to transform information from a usable concept into an incomprehensible form that is difficult to use by any unauthorized person called encryption. The process of converting encrypted information into information that is understandable as its original form is called decryption.

The works in [9]-[13]represent of the using of different encryption algorithms in structure-basedwireless sensor networks which suffers from many disadvantages. In this paper ,ECDH and RSA algorithms are used to encrypt data transmuted through the other type (structure-free) wireless sensor networks.

2.Encryption algorithms

2.1.**RSA**

The original RSA algorithm was publicly illustrated in 1977. The toxicity of this RSA algorithm was attributed to its three inventors, Ron Rivest, AdiShamir, and Leonard Adleman.In short, this algorithm consists of three stages namely key generation , encryption and finally the decoding stage. RSA is one of the cryptographic algorithms, which are of a non-symmetric type and thus need a pair

of keys, one of which is used for encryption and may be non-confidential, the other is the key to decryption, which is private and confidential and authorized only authorized to decrypt the data sent. This algorithm employs two large prime numbers, p and q. The strength of this scheme is based on the difficulty of finding these large initial numbers that are indispensable for finding the secret key while the public key can be freely distributed . The phases of the RSA algorithm and the steps of each phase are as follows[14],[15]:-

A . Key Generation Algorithm

Step 1.Select or generate two large random prime numbers, p and q .

Step 2.Compute $n = p \times q$ (1)

Step 3.Compute $\emptyset = (p-1) \times (q-1)$ (2)

Step 4. Select random integer e , $1 < e < \emptyset$, such that$GCD\ (e, \emptyset) = 1$.

Step5. Compute d , Where $d = e^{-1}\ mod\ \emptyset$ (3)

Step 6. Public Key: (e, n) .

Step 7. Private Key: (d).

B. Encryption process

Step1: Suppose entity R needs to send message m to entity S . When m : plain text .

Step2: Entity S should send his public key to entity R.

Step3: Entity R will encrypt m as $C = m^e\ mod\ n$ (4)

and will send C to entity S.

where$C$: Cipher text .

C. Decryption Process

Step1: Entity S will decrypt the received message as $m = c^d mod\ n$(5)

2.2. Elliptic Curves Diffie-Hellman (ECDH)

Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems almost 33 years ago, independently by Victor Miller of IBM (International Business Machines) and Neal Koblitz of the University of Washington [16]. At that time, elliptic curves were already being used in various cryptographic contexts, such as integer factorization and primality proving.Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in

the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography. For the purpose of cryptography, an elliptic curve can be thought of as being given by an affine equation of the form

$$y^2 = x^3 + ax + b \quad (6)$$

where a and b are elements of a finite field with p elements, where p is a prime larger than 3. (The equation over binary and ternary fields looks slightly different.) The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x andy satisfy the relation given by the equation defining the curve. The set of points on an elliptic curve with coordinates in a finite field also form a group, and the operation as follows: To add two points on the curve Q 1 and Q 2 together, a straight line is passed through them and looked for the third point of intersection with the curve , R1. Then point R1 is reflected over X-axis to get $-R1$. That means the sum of Q 1 and Q 2 results $-R1$. The idea behind this group operation is that the three points Q 1, Q 2, and R1 lie on a common straight line, and the points that form the intersection of a function with the curve are considered to add up to be zero[16] Figure 1 .

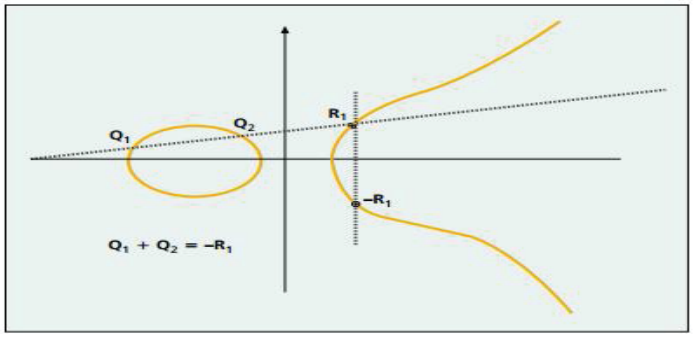


Figure 1: Group law on an elliptic curve.

Most wireless sensor environments are insecure and difficult to connect so the ability to safely exchange keys in such environments is very difficult. Diffie-Hellman Key is one of the EC types that provides this service or solves the problem described. Where the two parties exchange keys but these keys are subject to certain operations by the same party after switching until it becomes a key encryption by that party. The principle of power in Diffie-Hellman Key lies in the difficulty of guessing the type of operation and the digits in which the layer of research led to this exit[17].

To implement the Diffie-Hellman Key Exchange with an elliptic curve group, many iterations of the group operation must be performed. Therefore, it is important to optimize the implementation of the group operations. Many approaches have been explored, but choices about how to optimize the elliptic curve group operation often depend on the relative costs of operations such as multiplication and division of elements in the underlying field[16],[17] . That there are some points to be represented on an elliptic curve with affine coordinates as described above. Then to add two points Q1 = (x1, y1) and Q 2 = (x2, y2), where x1 ≠ x2, it is necessary to compute the slope of the line passing through then as :

$$\lambda = (y_2 - y_1) / (x_2 - x_1) \quad (7)$$

This requires one division in the underlying finite field. Then solving for the third point of intersection of the line with the curve, it is found that $-R1 = (x_3, y_3)$, where

$$x_3 = \lambda^2 - x_1 - x_2 \quad (8)$$

and $y_3 = (x_1 - x_3)\lambda - y_1$ (9)

So forming the sum requires 1 division, 1 squaring, and 1 multiplication in the underlyingfinite field (p ≠ 2 or 3) when adding two affine points with distinct x-coordinates, and ignoring the cost of addition or subtraction in the field. Alternative representations for an elliptic curve and the points on it are also available. Projective and weighted projective (also called Jacobian) coordinates are sometimes used, especially in cases where division in the underlying field is costly. Weighted projective coordinates work with triples of coordinates (x, y, z), corresponding to the affine coordinates (x/z2, y/z3) whenever z ≠ 0. The advantage of weighted projective coordinates is that point addition on the elliptic curve can be done in 16 field multiplications, avoiding all field divisions[16],[17].The steps of ECDH algorithm may be summarized as :-

1- select a number (P) which must be primary and larger than 3 .

2 - Select two numbers (a, b)

Where

$$\left((4a^3 + 27b^2) mod\ P \neq 0\right) \quad (10)$$

3 – Find the set of points (G) on the elliptic curve through the following equation

$y^2=x^3+ax+b$ over **Z**(6)

The addition rule.

i)$P + Q = Q + P$ for all P ∈ E(Z_p) .

ii) $If\ P = (x, y) \in E(Z\ p), then\ (x, y) + (x_1 - y) = Q.$

(the point (x_1-y) is denoted by –p, and is called the negative of P; op-serve that –p is indeed a point on the curve).

iii)$Let\ p = (x_1, y_1) \in E(z_p)\ and\ Q = (x_2, y_2) \in E(z_p), wher\ p \neq -Q.$

then $p + Q = (x_3, y_3)$,where

$$x_3 = \lambda_2 - x_1 - x_2 (8)$$

$$y_3 = \lambda (x_1 - x_3) - y_1 \quad (9)$$

And

$$\lambda = (y_2 - y_1)/(x_2 - x_1) if\ p \neq Q \quad (7)$$

$$\lambda = (3x_1^2 + a_1)/2y_1 \quad if\ p = Q \quad (11)$$

Then a random point is chooses from set of points (G) from set of points

4 - The choice of a large number is n

5- User A Key Generation

i)select private n_A with a condition $n_A < n$

ii)calculate public $p_A p_A = n_A \times G$ (12)

6- User B Key Generation

i)select private n_B with a condition $n_B < n$

ii)calculate public $p_B p_B = n_B \times G$ (13)

7- The two sides exchange keys (p_A ,p_B)

8- Calculate the Secret Key by User A

$K = n_A \times p_B$ (14)

9- Calculate the secret Key by User B

$K = n_B \times p_A$(15)

10 - Convert the packet data to a set of points (P_m). And then encrypt them using the following law .

A encryption p_m

$C_m = \{kG, P_m + kP_B\}$ (16)

11- The decryption uses the following law

B decryption C_m **compute**

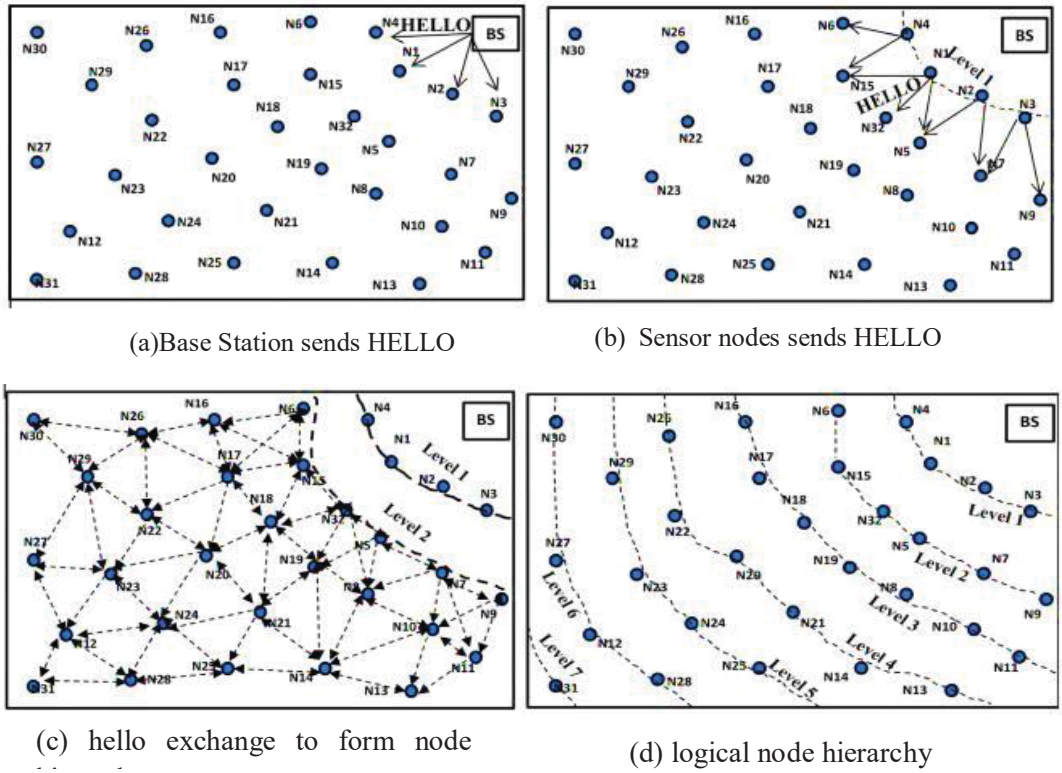
$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(KG) = P_m$ (17)

3.Topology Building Structure-free Network

The control of topology reduces the problems that becan developed with many nodes and their dense distribution. Topology control maintains contact with the use of minimal energy. During the

formation or construction phase of the network topology, each sensor must be known to be located in the control area of its own position, the position of its adjacent nodes and the base station (BS).Each node has its own (ID) sensor and after the deployment of the sensor contract begins the stage of the composition of the network topology begins the formation of topology by the base station (BS).The BS station sends a message regardless of the content of the message. The sensor nodes that receive this message transmit or send this message as well. Thus, each node receives or receive this message again transmits the data to other nodes with network levels. The levels are very important and depend on the transmitter range.

The message transmitted from the base station contains hop-count (hc) = 0 (zero). The set of sensor nodes receiving this message sent from the base station has a hop-count with one (hc = 1). Hold the sensor that has (hc = 1) (in turn send a message again and the sensor node receives this message will be (hc = 2) and so on. Thus, the levels are formed. The formation of these levels depends mainly on the extent of the transmitter. The nodes that have the (hc=1) form the first level and the nodes that have (hc=2) are the second level. Figure 2 illustrates the composition the levels.



(a)Base Station sends HELLO (b) Sensor nodes sends HELLO

(c) hello exchange to form node (d) logical node hierarchy

Figure 2: Logical topology constructions in a sensing field

The composition of this topology is once in the beginning and does not have to be repeated. The sensor node selects another sensor node at a lower level than the sensor node that operates to transmit the information based on so called the cost function (CF) .

3.1. Monitoring the events

Various events can be monitored from areas that are difficult to reach, and are almost impossible, at times, through wireless sensor networks. Where a growing interest has recently been generated to detect various events through wireless sensor networks [18].When a particular event occurs in the observation area through the sensors, the sensor node will be the location of the event within the range of its sensor that can sense the event. The relational factor (Rf) of the sensor-sensitive contract is calculated by

$$Rf = (\mathrm{SL} - \mathrm{dEvent\_sensor})/\mathrm{dEvent\_sensor} \quad (17)$$

WhereSL: is the sensitivity of the sensor node , dEvent_sensor : is the dimension between the event and sensor node. The sensor node with the largest relativity factor (Rf) compared to the rest of the event is the one that has the luck to monitor the event .This node that received the data of that event in turn select another node within the field to send the data to it and from one to another also until eventually reach the base station. In the mechanism of selection of the next sensor node to receive data from the sensor node that monitored the event is detailed in the next paragraph .

3.2. Next-hop node selection

Each sensor node selects the next sensor node to transmit the information to it by cost function.The cost function is calculated from the residual energy , buffer space (memory) available for the next jump node and the strength of the link between the current sensor node and sensor node in the next jump. Each sensor node defines the sensor holding group that is a neighbor and selects one of these neighbors during the data redirection based on the same cost function. Each node has its own information table of sensor, that information is the node's id, the buffer available (Buffst), the link strength (Ls), and the residual power (Eresd).When a certain node senses data or receives data packet from the top-level nodes , it redirects it to a node at the lower level and so on until it reaches the base station (BS) . The node calculates the cost function for all the following lower-level node j (Nj) sets the next jump node i (Ni) with the maximum value of the cost function (CFmax). The cost function is calculated by [18].

$$\mathrm{CF\ max} = max_{(i \in N)}\{\ \alpha\ (\mathrm{Eresd.i} + \mathrm{Buff\ aval.i} + \mathrm{Ls.i})\} \quad (18)$$

Where α is the inverse of the distance between Ni and Nj and are calculated according to :-

$$\alpha = 1/\sqrt{(N_{j.x} - N_{i.x})^2 + (N_{j.y} - N_{i.y})^2} \quad (19)$$

The residual energy in node i (Ni) is calculated by

$$\text{Eresd.i} = \text{Elevel.i} - ((\text{Etx(k, dtran)} + \text{ERX(k)}) + \text{Eagg}) \quad (20)$$

where:-Elevel.i : Current energy in the sensor node ,dtran : is the maximum transmissions range of the sensor node.The Etx(k,dtran) : is the energy required to transmit k bits to a distance dtran .ERX(k) : is energy spent for receiving a packet which is computed as ERX(k)= Eelec × k ,andEagg : is energy spent to aggregate n_p number of packets.

The available buffer space is computed from the current buffer status and the expected number of packets to be transmitted from neighborhood of Nj, through the following equation :-

$$\text{Buffaval.i} = \text{Buffst.i} - 2 \times \text{Number of neighbors} \quad (21)$$

The link strength (Ls) is the signal to interference noise ratio (SINR) for the link between Nj and Ni , Ls are calculated by equation .

$$Ls.\text{i} = \frac{Rec \text{ signal power}}{Rec \text{ no.of bits}} \quad (22)$$

Recno.of bits :- is the number of bits present in an acknowledgment packet from the neighbor node Ni.

The Rec signal power is computed as given by [19].

$$\text{Rec signal power} = -10\,\beta \log\left(\frac{\text{Pr(d)}}{\text{Pr(d0)}}\right) + \text{xdb} \quad (23)$$

where Pr(d) is the mean received power at distance d, which is computed relative to a reference power Pr(d0) at distance d0. β is the path loss exponent and **X**db is a zero mean Gaussian random variable .

4. Simulation parameters and algorithm flow chart

Throughout this work, the following simulation parameters are used to calculate the energy consumed in transmission of data through thestructure-free wireless sensor networks.

Table .1 Simulation parameters

Area of sensor field	500×500 m^2
Number of sensor nodes	400
Type of distribution	random
Packet length	60 bytes
Buffer length	65 packets
Initial node energy	70 J

Bandwidth	200 Kb/s
Sensing length	50 m
Radio range	40 m
Propagation model	Two ray
Eelec	50 nJ/bit
Esense	0.083 J/s
Eagg	5 nJ/bit/signal
Consumption energy for addition operation	50 nJ/addition
Consumption energy for Subtraction operation	50 nJ/subtraction
Consumption energy for Process mod	5×50 nJ/Process mod
Total run time	35 minute
Number of run attempts per 35 minutes	25 run

While Figure 3 shows the flow chart of the structure free algorithm to generate the required levels and nodes to transil data trough the wireles sensor network.

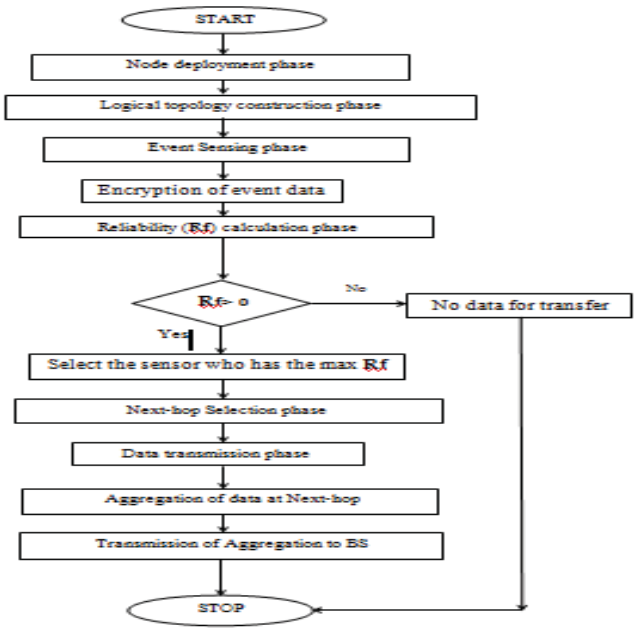


Figure 3: Key action steps.

5.Computersimulationresults

In this section, structure free with encrypted event data of the wireless sensor network with encrypted data is described. The RSA and ECDH algorithms (sections ٢.1. and ٢.2) are used to encrypt the transmitted data through that network . Computer simulation tests withMATLAB R2017-a are used to show the effect of encryption operation on the energy consumed of the network sensors.In all there tests , the number of transmitted packets are taken randomly between 1 and 60.Figure 4 to Figure 7 describe the power consumptionrelative to event period,data rate , number of nodes ,number of sensors respectively.

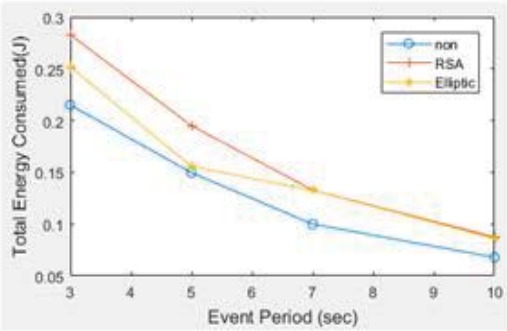


Figure 4:The total energy consumed with respect to event period for different types of encryption.

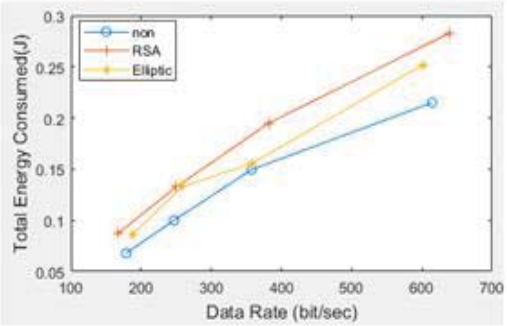


Figure 5: The total energy consumed with respect to data rate for different types of

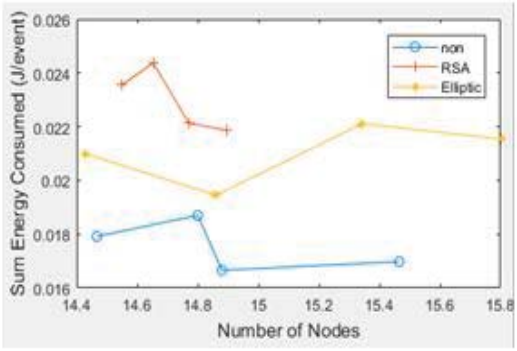


Figure 6: Total energy consumed with respect to number of node into different number of event for different types of encryption.

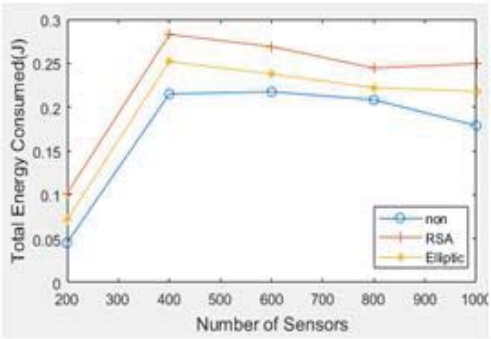


Figure 7:The total energy consumed with respect to number of sensor for different types of encryption .

During Encryption operation, the energy consumption is increased comparative with conventional structure-free (without encryption) . For RSA algorithm, the increment percentage is 27.586% (at 3 sec event period) , 25% (at 400 data rate) , 24.137% (at 400 sensor nodes) and 24% (at highest path followed) . While for ECDH algorithm, the percentage is 12%(at 3 sec event period) , 12.5%(at 400 data rate) , 20%(at 400 sensor nodes) and 13.636% (at highest path followed). Such results are

expected because the encryption requires set of mathematical operations to convert the transmitted data to non-understandable type.

6.Conclusions

structure freewireless sensor network has an advantage of choosing the proper path for transmitting the data from the sensors to the basestation.The power consumption of encryption during the encryption operation is increased as a tax to make the data transmitted over thestructure free network secure. The results of this paper show that the ECDH encryption algorithm is better than RSA from the energy consumption point of view because ECDH algorithm takes the data to be encryptionbyte by byte while RSAalgorithm takes the same data to be encrypted bit by bit ,which in surlyreduces the number of mathematical operations .Therefore, one can conclude that it is necessary to design a special type of elliptic curve algorithm (special equation) to further reduction in the mathematical operations , which in turn reduces the power consumption required to encrypt the datatransmitted through structure-free wireless sensor networks.

7.References

[1] Ivan Stojmenov*"Handbook of Sensor Networks Algorithms and Architectures"*, A John Wiley & Sons, Inc.,2005, http://www.wiley.com/go/permission.

[2] M. Mehdi Afsar and Mohammad-H. Tayarani-N " Clustering in sensor networks: A literature survey", *Journal of Network and Computer Applications* ,2014 , www.elsevier.com/locate/jnca.

[3] Santar Pal Singh and S.C.Sharma " A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks" ,2015 Elsevier B.V. doi. 10.1016/j.procs.2015.03.133,http://creativecommons.org/licenses/by-nc-nd/4.0/.

[4] Mr.Parth D. Patel, Pranav B. Lapsiwala and Ravindra V. Kshirsagar "Data Aggregation in Wireless Sensor Network", ISSN: 2249-0558 ,*International Journal of Management*, IT and Engineering, 2012, http://www.ijmra.us.

[5] Chih-Min Chao and Tzu-Ying Hsiao "Design of structure-free and energy-balanced data aggregation in wireless sensor networks" , 2013, *Journal of Network and Computer Applications* , http://dx.doi.org/10.1016/j.jnca.2013.02.013 .

[6] Jongdeog Lee , KrasimiraKapitanova and Sang H. Son " The price of security in wireless sensor networks", 2010 Elsevier B.V. , doi:10.1016/j.comnet.2010.05.011.

[7] An Liu and Peng Ning " TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks" , *International Conference on Information Processing in Sensor Networks* , USA , doi. 10.1109/IPSN.2008.47.

[8] Yashaswini R, Nayana HG, BinduAThomas " Wireless Sensor Network Security using Cryptography" , *International Journal of Advanced Research in Computer Science & Technology* , Vol. 4, Issue 2 (Apr. - Jun. 2016), ISSN : 2347 - 8446 (Online) ISSN : 2347 - 9817 (Print) , http://www.ijarcst.com/.

[9] M. RazviDoomun and KMS Soyjaudah " Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security", *International Journal of Network Security*, Vol.9, No.1, PP.82–94, 2009.

[10]MansoorEbrahim , Shujaat Khan and Umer Bin Khalid " Symmetric Algorithm Survey: A Comparative Analysis" , *International Journal of Computer Applications* (0975 – 8887), Volume 61– No.20, January 2013.

[11] Mohamed Elhoseny, HamdyElminir, AlaaRiad and Xiaohui Yuan " A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption" , *Journal of King Saud University – Computer and Information Sciences,* http://dx.doi.org/10.1016/j.jksuci.2015.11.001 1319-1578.

[12]Shailesh N. Sisat and Prof. Shrikant J. Honade "Security and Privacy in Wireless Sensor Network Using RC6 Algorithm" , *International Journal of Advanced Engineering Research and Science (IJAERS),* Vol-3, Issue-5 , May- 2016, ISSN: 2349-6495.

[13] Shiva Prakash and Ashish Rajput " Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks" , *2 nd International Conference on Computer, Communication and Computational Sciences, Gorakhpur*, India, 2017 .

[14] Surekha and Anita Madona " Analysis of RSA and ELGAMAL Algorithm for Wireless Sensor Network" , *International Journal of Computer Techniques* ,Volume 2 Issue 4, July- Aug 2015.

[15] S.Hemalatha and Dr.R.Manickachezian "Security Strength of RSA and Attribute Based Encryption for Data Security in Cloud Computing", *International Journal of Innovative Research in Computer and Communication Engineering* , Vol. 2, Issue 9, September 2014 , ISSN(Online): 2320-9801 , ISSN (Print): 2320-9798.

[16] Kristin Lauter and Microsoft Corporation "The Advantages of Elliptic Curve Cryptography for Wireless Security" , *IEEE Wireless Communications*, February 2004.

[17] Ram RatanAhirwal and ManojAhke " Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network" , *(IJCSIT) International Journal of Computer Science and Information Technologies*, Vol. 4 (2) , 2013, 363 – 368.

[18] PrabhudduttaMohanty and ManasRanjanKabat "Energy efficient structure-free data aggregation and delivery in WSN" , *Egyptian Informatics Journal* (2016) 17, 273–284 , http://dx.doi.org/10.1016/j.eij.2016.01.002.

[19] CharalambosSergiou, VasosVassiliou and AristodemosPaphitis "Hierarchical Tree Alternative Path (HTAP) Algorithm for Congestion Control in Wireless Sensor Networks" , *Ad-Hoc Networks*, October 27, 2013;11:257–72.