Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fuzzy Clustering Life Span Fortification with Data Compression, Nearest Neighbour Technique and Elliptical Curve Cryptography in WSN

M. Nagarajan* Department of CSE Valliammai Engineering College
M. Mayuranathan Department of CSE Valliammai Engineering College
S. Jayanthi Department of CSE FMK Fomra Inst. of Tech.

Abstract— Today WSN plays the essential role in the field of information and communication. The foremost drawback is consumption of the energy. Energy is heart of the sensor node. The Fuzzy cluster method is the proposed to address the energy concern, Fuzzy cluster mathematical approach involves dealing with several variables and parameters at a time. The Data compression is another strategy to reduce the number data element in a transmission. Nearest neighbour algorithm is also another strategy to enhance the life time of sensor nodes. The elliptical curve cryptography is also implemented for provide security to the data to avoid the unauthorized access of data in the network.

Keywords— Fuzzy Clustering, Data Compression, NNF, Elliptical Curve Cryptography

I. INTRODUCTION

The sensor nodes are facing the Energy consumption problems, Load Balancing, Network Coverage Wireless sensor networks nodes are connected with a base station. It is spatially distributed autonomous sensor to cooperatively monitor physical or environmental condition, such as temperature, sound, vibration, pressure, motion or pollutants. The main objectives of wireless sensor are event detection and transmission of data to the destination node. The major challenges of wireless sensor networks are Transmission of data without data loss, Efficient routing techniques, Limited Communication bandwidth. In a wireless sensor network all the nodes are work under the principles of battery power. Generally we cannot the produce the energy instead of this we can maximize the usage of energy. So each and every operation brings the node close to death. Our contribution in this paper is life time plays crucial roles in WSN [1]

A. Fuzzy cluster:

Clustering techniques are mostly unsupervised methods that can be used to organize data into groups based on similarities among the individual data items. Most clustering algorithms do not rely on assumptions common to conventional statistical methods, such as the underlying statistical distribution of data, and therefore they are useful in situations where little prior knowledge exists [3].

B. Data Compression:

Data compression reduces the size of data frames to be transmitted over a network link. Reducing the size of a frame reduces the time required to transmit the frame across the network. Data compression provides a coding scheme at each end of a transmission link that allows characters to be removed from the frames of data at the sending side of the link and then replaced correctly at the receiving side. Because the condensed frames take up less bandwidth, we can transmit greater volumes at a time [8].

C. Nearest Neighbour Technique:

The principle behind *nearest neighbour* methods is to *find* a nearest node from the destination node. In wireless sensor network there may be the collection in the network so the data pockets are transferor to the nearest node from the destination node.

D. Elliptical Curve Cryptography:

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers[10].

II . PROPOSED METHOD

A. ***Fuzzy Clustering:***

In this method the Cluster-heads are elected by the base station in each round by calculating the chance each node has to become the cluster-head by considering three fuzzy descriptors. The model of fuzzy logic control consists of a Fuzzifier, fuzzy rules, fuzzy inference engine, and a Defuzzifier.

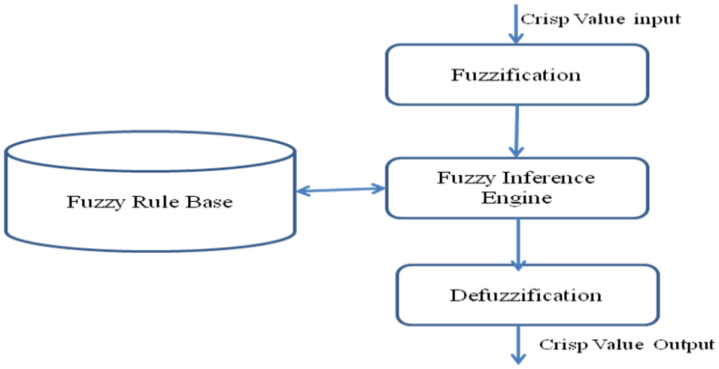

Fig.1 Fuzzification

In Fuzzifier, inputs with crisp value change into a fuzzy set and results are transferred to Defuzzifier through fuzzy inference engine and fuzzy rules base. Defuzzifier changes a fuzzy set to crisp value. Models are interpreted according to fuzzy logic

***B. Fuzzification**:*

The Fuzzification comprises the process of transforming crisp values into grades of membership for linguistic terms of fuzzy sets. The membership function is used to associate a grade to each linguistic term. For the fuzzification of the Node energy value has the two membership functions, which characterize a low and a medium speed fuzzy set, respectively. The given speed value of belongs with a grade of to the fuzzy set ``low" and with a grade of to the fuzzy set ``medium".

C. Fuzzy Inference Engine:

To execute a rule-based fuzzy system using the method of forward chaining we merely need to fire (or execute) actions whenever they appear on the action list of a rule whose conditions are true. This involves assigning values to attributes, evaluating conditions, and checking to see if all of the conditions in a rule are satisfied. A general algorithm for this might be: while values for attributes remain to be input read value and assign to attribute evaluate conditions fire rules whose conditions are satisfied. A model of an inference engine for a rule-based system whose basic components are:

Attributes: X1, X2 , ... , Xn1
Conditions: C1, C2 , ... , Cn2
Rules: R1, R2 , ... , Rn3
Actions: A1, A2 , ... , An4
For rules such as:
R1: if (Node-1Energy) <= low then A1;
R2: if (Node-1Energy) = High < LowA2;
R3: if (Node-1Energy) < LowA3;
we pre-process with the parser and form the conditions:
C1: Node-1Energy <= low
C2: Node-1Energy = High < Low
C3: Node-1Energy < Low
Then the various lists are set up and the rules and the relationships between the attributes, conditions, rules, and actions may be presented as the in figure 2.

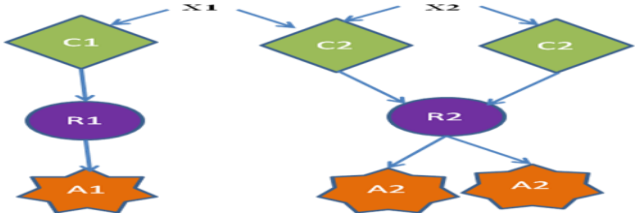

Fig.2 Fuzzy Data Structure

***D. Fuzzy Rule Base**:*

A particular type of reasoning which uses "if-then-else" rule statements. As mentioned above, rules are simply patterns and an inference engine searches for patterns in the rules that match patterns in the data. The "if" means "when the condition is true," the "then" means "take action A" and the "else" means "when the condition is not true take action B." Here is an example with the rule PROBABLE CAUSE:

IF robbery is TRUE
AND
suspect witness identification is TRUE
AND
suspect physical evidence is TRUE
AND
suspect lacks alibi is TRUE

THEN
probable cause is TRUE
ELSE
round up usual suspects

Rules can be forward-chaining, also known as data-driven reasoning, because they start with data or facts and look for rules which apply to the facts until a goal is reached. Rules can also be backward-chaining, also known as goal-driven reasoning, because they start with a goal and look for rules which apply to that goal until a conclusion is reached.

E. Defuzzification:

Fuzzy logic is a rule-based system written in the form of horn clauses (*i.e.*, if-then rules). These rules are stored in the knowledge base of the system. The input to the fuzzy system is a scalar value that is fuzzified. The set of rules is applied to the fuzzified input. The output of each rule is fuzzy. These fuzzy outputs need to be converted into a scalar output quantity so that the nature of the action to be performed can be determined by the system. The process of converting the fuzzy output is called defuzzification. Before an output is defuzzified all the fuzzy outputs of the system are aggregated with an union operator. The union is the *max* of the set of given membership functions and can be expressed as

$$\mu A = U(\mu_i(x)) \qquad (1)$$

F. Centroid Defuzzification Technique:

This method is also known as center of gravity or center of area defuzzification. This technique was developed by Sugeno in 1985. This is the most commonly used technique and is very accurate. The centroid defuzzification technique can be expressed where x^* is the defuzzified output, $\mu_i(x)$ is the aggregated membership function and x is the output variable. The only disadvantage of this method is that it is computationally difficult for complex membership functions.

G. Fuzzy logic Approach to Cluster-Head Selection

Cluster-heads are selected by the base station in each round by calculating the chance each node has to become the cluster-head by considering three fuzzy descriptors. During the setup phase the cluster-heads are determined by using fuzzy knowledge Processing and then the cluster is organized. After the cluster-heads have been calculated at the base station, base station broadcasts cluster-head ID for each node in the cluster. If a match occurs between the node ID and the cluster-head ID the node is a cluster-head. Otherwise the nodes obtain the TDMA time slots for transmitting the data to the cluster-head.

H. Procedure

1. Define the linguistic variables and terms (initialization)
2. Construct the membership functions (initialization)
3. Construct the rule base (initialization)
4. Convert crisp input data to fuzzy values using the membership functions (fuzzification)
5. Evaluate the rules in the rule base (inference)
6. Combine the results of each rule (inference)
7. Convert the output data to non-fuzzy values (defuzzification)

III. DATA FUSION

Collected sensor data packets are aggregated, combined into single packet, and redundancies in the data packets are removed to minimize data transmission. The collected data is in the form of a tuple of three values as shown in Data Frame Format, Figure 3.

SOURCE ID	SEQ. NO	HOP COUNT	ENERGY THRESHOLD	SIGNAL STRENGTH THRESHOLD	SINK ID

Fig.3 Data Frame Format

data item produced by a sensor node. The compression is done by checking all the most significant bits of the packets and combining the packets which have the same most significant data bits.

A. Huffman Algorithm for Data Fusion:

Huffman coding deals with data compressions of ASCII characters. This is one of many techniques for compressing data. This method is most commonly used for emails over the internet.

B. Algorithm for Huffman coding:

1. Compute the probability of each character.
2. Sort the set of data in ASCENDING order.
3. Create a new node where the left child is the lowest in the sorted list and the right is the second lowest in the sorted list.
4. Chop-off those two elements in the sorted list as they are now part of one node and add the probabilities. The result is the probability for the new node.
5. Perform insertion sort on the list with the new node.
6. REPREAT STEPS 3, 4, 5 UNTIL you only have 1 node left.

C. Pseudo-code of the encode algorithm:

encode (di,Table)
IF di = 0 THEN
SET ni TO 0
ELSE


```
SET ni TO _log2(|di|)_ //compute category
ENDIF
SET si TO Table[ni] //extract si from Table
IF ni = 0 THEN //build bsi
SET bsi TO si //ai is not needed
ELSE
IF di > 0 THEN //build ai
SET ai TO (di)|ni
ELSE
SET ai TO (di − 1)|ni
ENDIF
SET bsi TO _ si, ai _ // build bsi
ENDIF
RETURN bsi
```

IV. SPREADING TECHNIQUES

A. Multi-hop Delay Tolerant:

In WSN data is transmitted from the source to designation, if any network traffic or network collation occurs the data packets will be lost, Once again the sender has to send the data, again there is an energy lose. To address this issue we proposed scheme called Spreading Techniques. As important challenging issues, the ensuring of each link's quality on the end to-end pathways, and enabling the data conveyance on WSN where the end-to-end route does not always exist can be listed. We developed the module that prevents weak links to be chosen as a route. This module decreases unexpected packet losses. also, we introduced multi-hop delay tolerant transfer" that chooses the best intermediate node as the next data carrier.

B. Nearest Neighbour Search:

Algorithm Multistep NN (Q,K)

1. Retrieve the k NNs(P1,…..Pk) of Q According to DST
2. RS = {P1,……..,Pk), sorted according to DST
3. DST_{max} = DST (Q1, Pk) // the current k^{th} NN DST
4. P = next NN of Q according to dst
5. 5. While DST(Q,P) <DST_{max}
6. If DST(Q,P)< DST_{max}
7. Insert P into RS and remove previous k^{th} NN
8. Update DST_{max} over RS
9. P=next NN of Q according to dst

V. ELLIPTICAL CURVE CRYPTOGRAPHY

The ECC is the public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

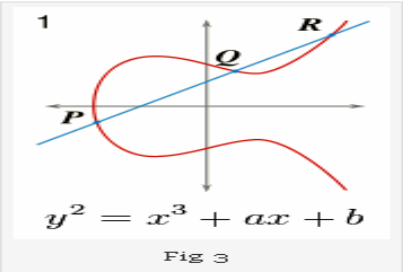

Fig. 5 Elliptical Curve Cryptography

A. Key Generation:

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number**'d'** within the range of **'n'**.

Using the following equation we can generate the public key

$Q = d * P$ (2)

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.
'Q' is the public key and 'd' is the private key.

B. Encryption:

Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.
Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].
Two cipher texts will be generated let it be C1 **and** C2**.**

$C1 = k*P$ (3)

$C2 = M + k*Q$ (4)

C1 and C2 will be sending.

C. Decryption:

We have to get back the message 'm' that was send to us,

$M = C2 – d * C1$ (5)

M is the original message that we have send.

D. Proof:

How does we get back the message,

$M = C2 – d * C1$ (6)

'M' can be represented as 'C2 – d * C1′

$C2 – d * C1 = (M + k * Q) – d * (k * P)$ (C2 = M + k * Q and C1 = k * P) (7)

$= M + k * d * P – d * k * P$ (canceling out k * d * P)

= M (Original Message)

The Elliptical curve cryptography provide the security when the data in nearest neighbor for a longer period the data might the hacked by some other person to address the issue the Elliptical curve cryptography provide the security for the data.

VI. CONCLUSION

In this paper we have proposed techniques for energy fortification to the sensor nodes for efficient transmission with elliptical cryptography. The main problem with wireless sensor networks is energy. We cannot produce to energy to address this issue we can increase lifetime of these networks and to reduce energy use for nodes. In this paper we have we have introduced the concepts of Data compression which reduce the number of data elements. Clustering and Spreading Techniques which enhance the transmit the data efficiently with the less energy conception.

ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and deep regards to our Principal Dr. B. Chidambara rajan, Vice Principal Dr. M. Murugan, I would like to express my special thanks of gratitude to my Head of the Department Dr. B. Vanathi, and I also take this opportunity to express a deep sense of gratitude to Mr. M. Senthil Kumar Assistant Professor/CSE, for their continuous encouragement. Lastly, I thank almighty, my grandparents and friends for their constant encouragement without which this assignment would not be possible.

REFERENCE

[1]. M. Nagarajan, T. Geetha, "Wireless Sensor Network's Life Time Enhancement With Aid of Data Fusion, LEACH-C and Spreading Techniques**",** International Journal of Information Technology and Engineering, Vol.3 No.1-2 2012.

[2]. M. Nagarajan, S. Jeyanthi, T. Dahanapalan, "Highly Secured WSN Life Span Fortification with Data Compression, NNF Technique and ECC Method", International Journal of Computer Science & Engineering Technology, Vol. 5 No. 05 May 2014.

[3] S. Abbas Karimi, M. Abedini1, Faraneh Zarafshan, S.A.R Al-Haddad, Cluster Head Selection Using Fuzzy Logic and Chaotic Based Genetic Algorithm in Wireless Sensor Network, J. Basic. Appl. Sci. Res., 3(4)694-703, 2013.

[4]. Swati Atri1, Dr. Nasib Singh Gill, Jaideep Atri, Fuzzy Logic Implementation of Ant colony Based Cluster head Selection Algorithm, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 4, April 2014.

[5] S. Nithya, R. Manavalan, An Ant Colony Clustering Algorithm Using Fuzzy Logic, International Journal of Soft Computing And Software Engineering, Vol.2,No.5, 2012.

[6] Dr. Sami Halawani, Abdul Waheed Khan, Sensors Lifetime Enhancement Techniques in Wireless Sensor Networks - A Survey, Journal of Computing, Volume 2, Issue 5, May 2010.

[7] Ankit Sharma, Jawahar Thakur, An energy efficient network life time enhancement proposed clustering algorithm for Wireless Sensor Networks, International Journal of Enhanced Research in Management & Computer Applications, Vol. 2 Issue 7, July-2013.

[8] Roopali Garg, Deepika Gupta, Network Lifetime Enhancement in Wireless Sensor Network-A Review paper, International journal of advances in computing and information technology, December 2012

[9]. Li Li, Jian Li, Research of Compressed Sensing Theory in WSN Data Fusion, Computational Intelligence and Design, Fourth International
Symposium, PP 125 – 128, 2011.

[10]. Capo-Chichi, J.M. Friedt, J.M, H. Guyennet, Using Data Compression for Delay Constrained Applications in Wireless Sensor Networks
Sensor Technologies and Applications, Journal of Sensor Communication, PP
101 – 107, 2010.

[11]. Haodong Wang, Bo Sheng and Qun , Elliptic curve cryptography-based access control in sensor networks, Int. J. Security and Networks,
Vol. 1, Nos. 3/4, 2006.

