IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

WSN Life Time Enhancement using Fuzzy Clustering and Intrusion Recognition with EAS

M. Nagarajan[1], T. Dhanapalan[2] and S. Jayanthi[3]

[1] Department of Computer Science and Engineering, Valliammai Engineering College, Chennai, Tamilnadu, India.

[2] Department of Placement & Training, Valliammai Engineering College, Chennai, Tamilnadu, India.

[3]Department of Computer Science and Engineering, SMK FOMRA Institute of Technology, Chennai, India Chennai, Tamilnadu, India.

Abstract

Wireless sensors networks performing as essential role in today's globe. The key disadvantage is consumption of the energy. Energy is heart of the sensor node. The Fuzzy cluster method is the proposed to address the energy concern; this method can enhance the energy of the WSN nodes Fuzzy cluster mathematical approach involves dealing with several variables and parameters at a time. . In a WSN environment most of chances for hacking the data from the remote place of the network, to address this issue, the Intrusion Detection mechanism is implemented to detect the false node and cluster head. EAS is the efficient authentication system thought this system can prevent the unauthorised access of nodes

Keywords: Author Guide, Article, Camera-Ready Format, Paper Specifications, Paper Submission.

1. Introduction

In a wireless sensor network the nodes are distributed and they are connected with the base station. Every transition taken place of the base station. In typical environment data transmission is sending is costly than receiving.

Let us consider the example node A, B, C, D, E situated a net work Node A is want to sent a data to E in between two node are presented in the transmission. Even though there is no direct communication between nodes B and D, there will be lose of energy due to the data transmission. They have contributed as a mediator for the transmission.

The figure.1 is indicated that the normal data transmission between two nodes but apart from that some of the other nodes are also participated the transmission. To address the above problem the clustering techniques was proposed.

The clustering concept is grouping the nodes and the each group will have a cluster head [1]. The cluster head will do the all the transaction every nodes are directly connected with the cluster head.

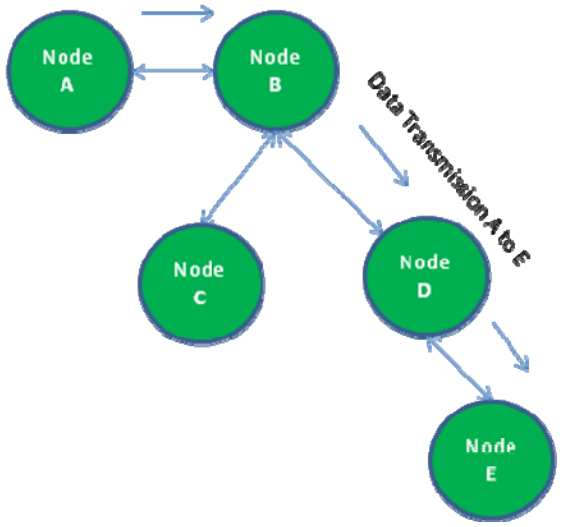

Fig.1 WSN Data Transmission

1.1. Fuzzy Logic:

Fuzzy logic is the set of predefined rules and representing in the form of mathematical terms of input. A form of knowledge representation suitable for notions that cannot be defined precisely, but which depend upon their contexts [3].

1.2. Intrusion Detection System:

In a typical wireless environment there may be lot of chances for steel the data from a remote pc. The main

ISSN 2348 – 7968

thing of the intrusion is attempting break in to or misuse the computer. The intruder may be outside of the of the network or inside the network.

1.3. Types of Intrusion:

- Buffer Overflow
- Unexpected Combination
- Unhandled Input
- Race Condition

1.4. Efficient Authentication System:

The efficient authentication system generate a pass code that pass code can be created using elliptical cure cryptography system. The communication can be exhibited by change of the pass code in a trusted manner.

2. Intrusion Detection System

The intrusion detection security is detected and prevents the intruder in the sensor network by implementing MAC address based intruder tracking system.

2.1. Base Station Function

1. The Base Station (BS) is located within the range of Access Point.
2. The Base Station has contained the information about the location of each node.

2.2. Cluster Head Function

3. All nodes are able to send data to BS via Cluster Head.
4. Base station has all the information about Cluster
5. The removal or addition of any node in a Cluster is monitored by the Base Station
6. Cluster Heads keep track of each node and sends periodic status information to the Base Station.
7. Cluster Heads (CHs) transmits data to Base Station after performing data reception and compression

2.3. Achievable Intrusion

Possibility 1 – Intruder tries to tie with one of the nodes in a cluster

Possibility 2 – Intruder tries to tie with a Cluster Head of a cluster

2.4. Intrusion Possibility 1:

The intruder identifies the nearest possible nodes. The intruder tries to communicate with one of the nodes with hidden MAC address in listen mode only. Finally the intruder identifies node in the first cluster to be the nearest node. it tries to communicate with the node with hidden MAC address in listen mode only. It successfully bonds with node in listen mode keeping its identity hidden. The intruder has the capability of interpreting the packets being sent and received by node.

2.5. Intrusion Possibility 2:

The intruder identifies Cluster Head as the nearest possible node. The intruder tries to communicate with one of the Cluster Head with hidden MAC address in listen mode only. Finally the intruder identifies Cluster Head in the first cluster to be the nearest Cluster Head. it tries to communicate with the Cluster Head with hidden MAC address in listen mode only. It successfully bonds with Cluster Head in listen mode keeping its identity hidden. The intruder has the capability of interpreting the packets being sent and received by Cluster Head. the Cluster Head is instructed to block the receiving and sending of data to ensure that the intruder can no longer infect the functioning of the wireless Sensor network

2.6. Intrusion Detection Possibility 1:

The Base Station collects all the information of the intruder. The Base Station issues a command to the intruder to grab its operation. After the intruder has gone down the Cluster Head revives the affected node.

2.7. Intrusion Detection Possibility 2:

Intruder tries to bond with a Cluster Head in a cluster; The Base Station collects all the information of the intruder. The Base Station issue a command to the intruder to grab its operation after the intruder has gone down the BS revives the affected Cluster Head.

3. Efficient Authentication System (EAS)

Efficient authentication scheme, which is suitable for low-power mobile devices. It uses an elliptic-curve-cryptosystem based trust delegation mechanism to

ISSN 2348 – 7968

generate a delegation pass code for WSN node authentication, and it can effectively defend all known attacks to mobile networks including the denial-of-service attack. Moreover

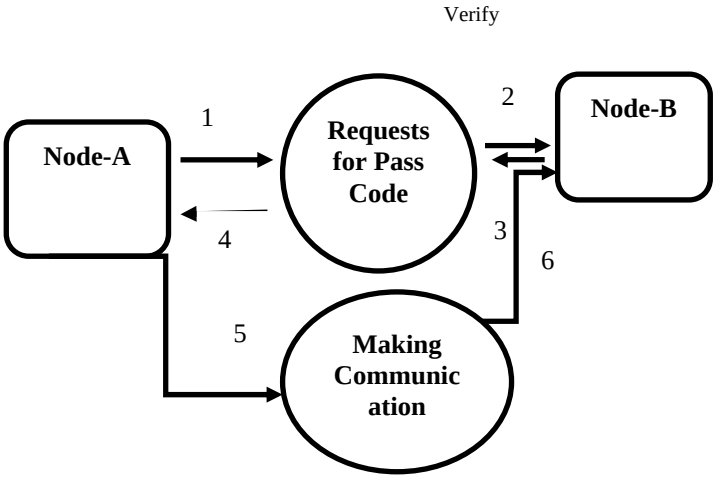

Fig.2. MAS Architecture

3.1. Procedure for EMAS:

Step-1: Node A Request for the communication key to Node B

Step-2: Node B verified the request whether authorised or not

Step-3: provide the pass code to the Node-A

Step-4: Establish the communication.

4. Fuzzy System Architecture

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.

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

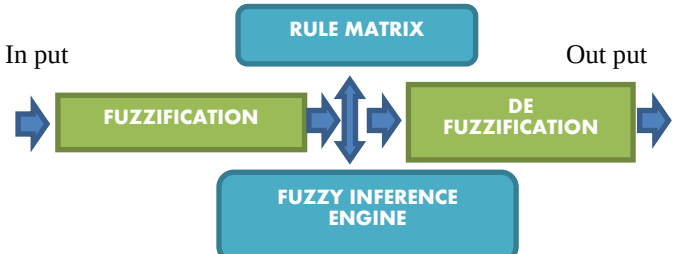

Fig.3 Fuzzy Architecture

4.1. 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''.

4.2. 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: N1, N2 , ... , Nn1
Conditions: C1, C2 , ... , Cn2
Rules: R1, R2 , ... , Rn3
Actions: A1, A2 , ... , An4

For rules such as:

R1: if (Node-1Energy) <= low then Node (A);
R2: if (Node-1Energy) = High < Node (B);
R3: if (Node-1Energy) < Low Node(C);

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.

ISSN 2348 – 7968

4.3. 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.

4.4. 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

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

4.5. 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.

4.6. 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.

4.7. 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 (def uzzification)

5. Conclusions

The importance technique in this paper is power strengthening to the sensor nodes for efficient transmission. The main problem with wireless sensor networks is power. We cannot produce to energy to address this issue we can increase lifetime of these networks and to reduce energy use for nodes. The fuzzy logic plays a vital role to enhance the energy of the sensor node. The most challenging thing in the WSN is security issues lot of security issue are penetrated by intruders, so to address in this kind of problem a intrusion detection mechanism is implemented to safeguard the nodes against

ISSN 2348 – 7968

the intruders and Efficient Authentication Mechanism will provide security for unauthorised access.

Acknowledgments

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.

References

[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,2012, Vol.3 No.1-2

[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, May 2014. Vol. 5 No. 05

[3]. M. Nagarajan, M. Mayuranathan, S. Jayanthi "Fuzzy clustering Life Span Fortification with Data Compression, Nearest Neighbour Technique and Elliptical Curve Cryptography in WSN", International Journal of Advanced Research in Computer Science and Software Engineering 3 (4),March - 2013, pp. 1-6

[4]. 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)2013, 694-703.

[5]. 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, April 2014, Vol. 3, Issue 4.

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

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

[8]. 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, July-2013. Vol. 2 Issue 7.

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

[10]. 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

First Author

Nagarajan. M., has completed his B.Sc -Computer Science and M.C.A at Annamalai University, M.Phil Computer Science and M.Tech(CSE) at Ponniya Institute of Science and Technology, MBA at Anna University. He has Published International few Journals in WSN.

Second Author

Dhanapalan.T., has completed his B.com & MBA at Madurai Kamarajar University, M.C.A-Master of Computer Application at Alagappa University. His interested areas are Analysis of Algorithms and its efficiency in real time systems.

Third Author

Jayanthi .S., has completed her B.Sc - Chemistry at Madras University, M.sc.IT & M.Phi(CS) at Bharathidasan University and M.Tech-CSE @ PRIST University, She is doing Ph.D in Manormaniyam Sundharanar University.