Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks by using Fuzzy Technic

T. Senthamizhchudar
PG Student: Department of CSE
Arasu Engineering College,
Kumbakonam, India

J. Ganesh
Assistant Professor: Department of CSE
Arasu Engineering College
Kumbakonam, India

***Abstract*— Recent advances in wireless sensor networks(WSNs)make them more important to apply. AHIDS makes use of cluster-based architecture with enhanced LEACH protocol that intends to reduce the level of energy consumption by the sensor nodes.In this paper,to identify the malicious node in wireless sensor network using fuzzy logic. WSN security faces a lot of challenges. The malicious node is one of the security. The result of this papaer,Fuzzy theory represending linguistic construct such as high,low,medium.**

Keywords*— Wireless Sensor Network, Hybrid Intrusion Detection System,LEACH.

I. INTRODUCTION

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The (WSN) consists of base station and a number of wireless sensor nodes

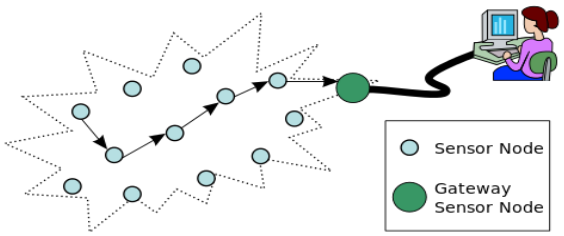

Fig. 1. Wireless sensor network

Wireless sensor networks(WSNs) are a recent technology and have received huge attention among researchers. Normally,the WSN environment comprises low power, low cost, and a huge number of sensors that are distributed arbitrarily over the target location or are redeployed manually.Wireless sensor networks have become a powerful and familiar technology due to their potential features and applications such as healthcare, monitoring, domestic applications, surveillance systems, and disaster management.

A WSN consists of many different components of which a sensor node is an important yet small part. The IDSs designed for wired or ad hoc networks cannot be implemented directly in the WSN. Fig. 1 Wireless sensor network. Wireless sensor network is a self-organizing network with a huge number of sensor nodes which consumes less power and is of low cost.

II. RELATED WORK

Here, we take some of the papers related to identify malicious node using various advanced techniques and some of them shown below,

In paper[1], author described as we propose a hybrid, lightweight intrusion detection system for sensor networks. Our intrusion detection model takes advantage of cluster-based architecture to reduce energy consumption. This model uses anomaly detection based on support vector machine (SVM) algorithm and a set of signature rules to detect malicious behaviors and provide global lightweight IDS. Simulation results show that the proposed model can detect abnormal events efficiently and has a high detection rate with lower false alarm.

In paper [2], author discussed LEACH (Low Energy Adaptive Clustering Hierarchy). LEACH forms small clusters of some sensor nodes of which one is the cluster head and others are the cluster members. The cluster members send their sensed data to the cluster head and cluster head in turn send this data to the sink by aggregating all the received data from its cluster members, in order to reduce the redundancy. LEACH protocol is a secure protocol as compared to the more conventional multi-hop protocols.

In paper [3], author discussed about the system should be such that it secure the information of modes and make sure that the messages reaches from source to destination without the loss of integrity.Malicious Nodes: Main aim of malicious nodes is to damage other nodes by causing network outage by partitioning whose priority is not for saving battery life.Selfish Nodes: They do not cooperate but use the network. Their priority is to save their battery life for their own communications and they do not damage other nodes directly.

In paper [4] author describes a neural network using probabilistic robust learning algorithm for neural networks with random weights (NNRWs) to improve the modeling performance. The robust NNRW model is trained by optimizing a hybrid regularization loss function according to the sparsity of outliers and compressive sensing theory. The important and useful to develop advanced learning algorithms for building robust learner models from uncertain data, in particular, a special class of noise data referred as outliers.

III. PROPOSED METHODOLOGY

WSNs and applied it to routing and intrusion detection to detect selfish or malicious nodes.In group based scheme sensor network is partitioned in groups. Sensor nodes in each group are physically close to each other. Attacker is detected using multiple attribute of the sensor nodes. Network traffic is analyzed and a mechanism is defined for detecting attacks. Both intrusion detection and prevention scheme are implemented with less communication overhead and low energy consumption.In this paper, we are discussed to use recent identify the malicious node in wireless sensor network using fuzzy logic.

A. CLUSTER FORMATION

Clustering is grouping physical network nodes into a small number of logical assemblies and maintaining them during the network operation. The logical assemblies are called clusters. It can identify compromised nodes and remove them during the initial cluster formation. Removing the compromised nodes during the cluster formation is the first defense line for secure clustering. The clustering is driven by the minimization of energy for all the sensors. Here, there are two clusters formed and totally twelve sensors and two cluster head.

B. CLUSTER HEAD SELECTION

The WSN divides clusters, each having a coordinator (cluster head) responsible for gathering the data from the nodes and sending it to the sink (base station). Sensors are often deployed densely to satisfy the coverage requirement, which enables certain nodes to enter the sleep mode thereby allowing significant energy savings. The cluster heads can be selected randomly or based on one or more criteria. Selection of cluster head largely affects WSNs lifetime. The ideal cluster head is the one which has the highest residual energy, the maximum number of neighbor nodes, and the smallest distance from the base station. Here there are two cluster and cluster head for each cluster.

C. INTRUSION DETECTION AT SN LEVEL

Cluster head Base station send and receive nodes Maximum number of neighbor nodes Malicious node Large number of nodes to attempt Broadcast a routing WSN The trust value of SN who has state transition between monitoring and active is evaluated preferentially. After the deployment of WSN, the formation and initialization of clustersare conducted. Before evaluating the trust of SNs, a CH observes, if there exists state conversion of SNs between monitoring and active. If it exists, the CH calculates the trust of SNs with different parameters according to the state context. Then, the trust of other SNs in the cluster is calculated, and the threshold of SN trust is not selected until all SNs in the cluster are traversed. Finally, the trust of each SN is compared with the threshold, below which the SN is regarded as a malicious one and measures should be taken to avoid its further damage.

D. INTRUSION DETECTION AT CH LEVEL

The intrusion detection at CH level is conducted by BS b, reducing the possibility of being deceived by CHs and decreasing the energy consumption of CHs. The trust calculation of each CH is different from SN since there is no state transition of CHs in this work. Malicious CH detection is similar to the malicious SN discovery, which also detects by a threshold of trust of CHs. The BS b computes and maintains the trust value of each CH j and selects a threshold trust TCth as the where CHS is the set of CH in WSN, and avg is the average function. The BS b compares the trust of each CH in WSN to the threshold calculated and considers the CH whose trust value is less than the threshold as malicious or compromised.

IV. EXPERIMENTAL RESULT

In our system processing starts with fuzzy logic.The fuzzy logic is a mathematical tool for dealing with uncertainty.

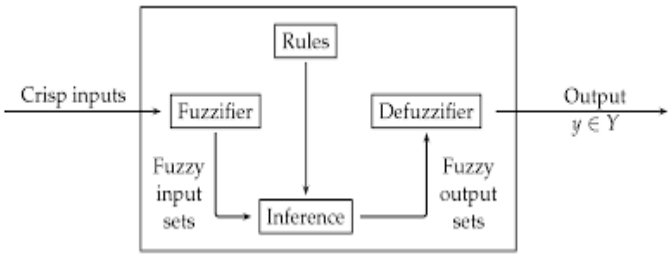

Fig 2.fuzzy logic

Fig 2 represent a fuzzy system basically consists of three parts: fuzzifier, fuzzy inference engine, and defuzzifier. The fuzzifier maps each crisp input value to the corresponding fuzzy sets and thus assigns it a truth value or degree of membership for each fuzzy set. The fuzzified values are processed by the inference engine, which consists of a rule base and various methods for inferring the rules. The rule base is simply a series of IF-THEN rules that relate the input fuzzy variables with the output fuzzy variables using linguistic variables, each of which is described by a fuzzy set. The defuzzifier performs defuzzification on the fuzzy solution space. That is, it finds a single crisp output value from the solution fuzzy space.

E. FUZZY SETS

A fuzzy set is a set with a smooth boundary.a set in classical set theory always has a sharp boundary because member ship in a set is a black and white concepts.an objects either completely belongs to the set or does not belong to the set at all. A fuzzy set theory overcomes this limitation by allowing membership in a set to be a matter of degree.The degree membership in a set is expressed by number between 0 and 1.

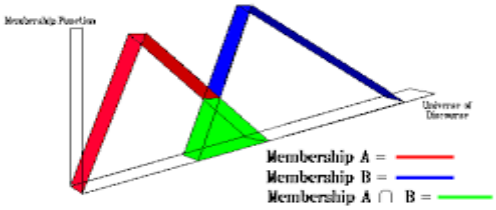

Fig 3 Fuzzy sets

F. LINGUISTIC VARIABLES

Linguistic variable and fuzzy inference system.fuzzy set. A fuzzy set is defined by its membership function.During reasoning the variables are referred to by the linguistic terms so defined, and thefuzzy sets determine the correspondence with the numerical values. Example :fast,slow,moderate,very slow etc.,Fig 4 shows example of linguistic variables.

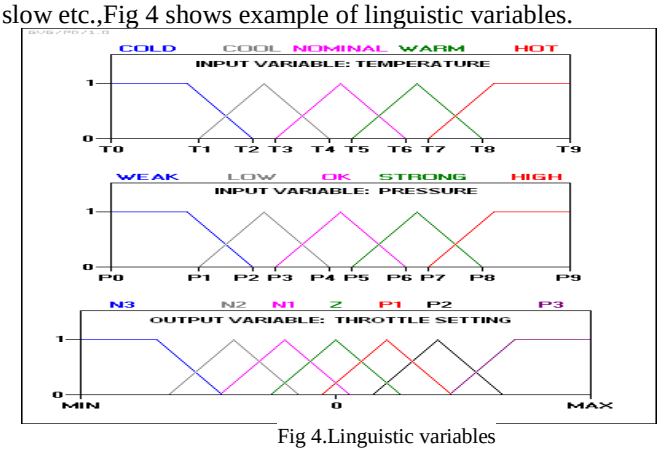

Fig 4.Linguistic variables

G. POSSIBILITY DISTRIBUTION

When a fuzzy set is used to represent what is known about the value of a singly-valued variable, the degree related to a value expresses the degree of possibility that this value is the true value of the variable. Fuzzy set F is then seen to be a possibility distribution

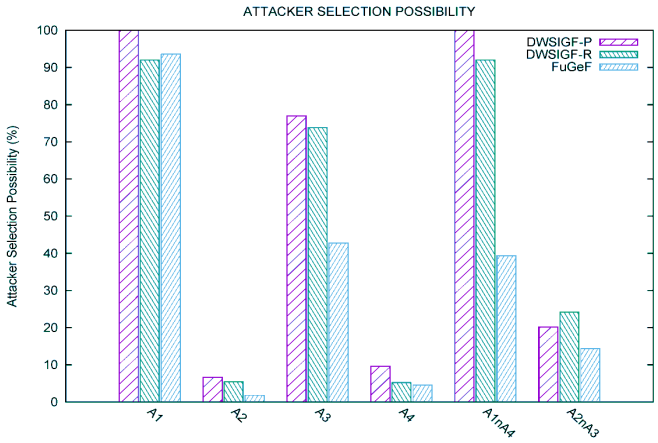

Fig 5.possibility distribution

H . IDENTIFY MALICIOUS NODE

Identify malicious neighboring nodes by monitoring their behaviors and identify target node as malicious if the trust values provided from introducer.A malicious node that broadcasts a routing beacon with an extra high power could lead a large number of nodes to attempt to use it as their next hop in their route to sink. But those sufficiently far away would be simply sending their messages into the oblivion. A similar scenario results from a wormhole attack. Fig 6 shows example of identify malicious node.A malicious node could convince nodes that are normally multiple hops from the sink node that they are just one hop away. These nodes would try to send their packets directly to the sink node, which would not able to hear them.

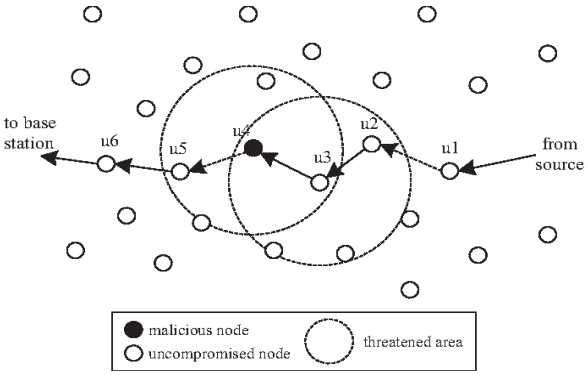

Fig 6.Identify malicious node

The objective of our fuzzy-logic-based routing is to determine the energy optimized routing based on the parameters defined previously, such that the network lifetime is maximized. The fuzzy rule base has been tuned so as not only to minimize energy consumption but also to balance data traffic among sensor nodes effectively.

The input fuzzy variables are Degree of Closeness of node to the Shortest Path (DCSP), Degree of Closeness of node to Sink (DCS), and Degree of Energy Balance (DEB). The first two variables reflect the measure of energy efficiency for selecting one node as next hop, and the last variable shows the measure of energy balance for routing decision. The rule base consists of 27 (33) rules. There is a single output fuzzy variable, namely, chance, the defuzzified value of which determines the chance for one forwarding neighbor which has been selected as next hop.Fig 7 represent fuzzy algorithm using assign the nodes.

1: initialize the number of nodes n
2: **for** $i \leftarrow 1$ to n **do**
3: generate a random number m_i from 0 to $10^n - 1$
4: **if** $m_i/10^n < p_b$ **then**

5: ask all the nodes (including node i) to provide evidence about node i
6: **if** BasicDetection($i, \$_{task}, \$_{forward}, [t_1, t_2], \mathcal{R}, \mathcal{D}$) **then**
7: give a punishment C to node i
8: **else**
9: pay node i the compensation w
10: **end if**
11: **else**
12: pay node i the compensation w
13: **end if**
14: **end for**

Fig 7.Fuzzy algorithm

The fuzzified values are processed by the inference engine, The rule base is simply a series of IF-THEN rules that relate the input fuzzy variables with the output fuzzy variables. defuzzification on the fuzzy finds a single crisp output value from the solution fuzzy space and finally end of the algorithms

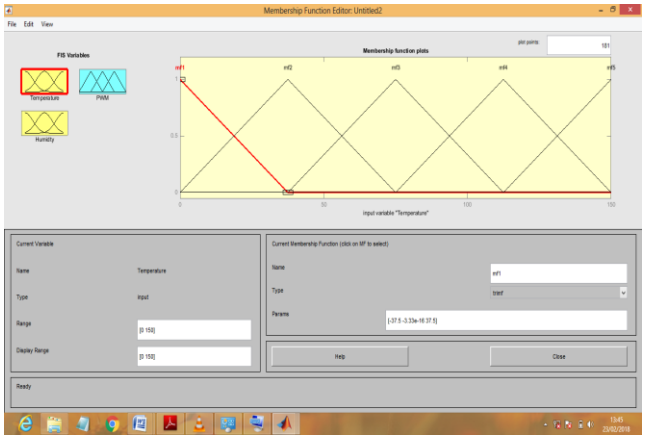

Fig 8.Membership function editor

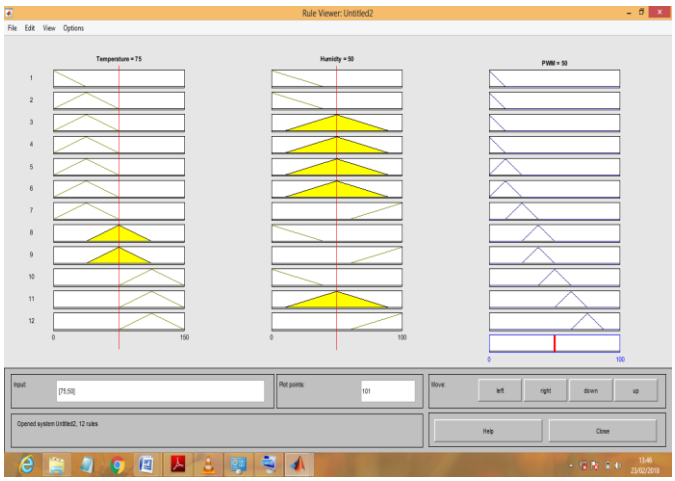

Fig 9.Rule editor

CONCLUSION

The combination of these two techniques is used to provide an Advanced Hybrid Intrusion Detection System with a high detection rate and low false positive rate. The detection mechanism is incorporated in a cluster-based topology with LEACH protocol, to decrease communication costs and energy consumption, which leads to an increase in the network lifespan, improving the lifetime of the network.The simulation results showthat the proposed Intrusion Detection System is capable of attaining high,low,medium,cold,warm,hot. The results also prove that the proposed system is fuzzy based identify malicious node.

]

REFERENCES

[1] Y. Maleh, A. Ezzatib, Y. Qasmaouic, and M. Mbidac, “A global hybrid intrusion detection system forwireless sensor networks,”*Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.

[2] Y. Shen, S. Liu, and Z. Zhang, “Detection of hello flood attack caused by malicious cluster heads on LEACH protocol,” *International* Journal of Advancements in Computing Technology, vol.7, no. 2, pp. 40–47, 2015.

[3] J. Rupareliya, S. Vithlani, and C. Gohel, “Securing VANET by preventing attacker node using watchdog and Bayesian network theory,” in Proceedings of the International Conference on Communication, Computing and Virtualization, vol. 79, pp.649–656, Mumbai, India, February 2016

[4] F. Cao, H. Ye, and D. Wang, “A probabilistic learning algorithm for robust modeling using neural networks with random weights,” *Information Sciences*, vol. 313, pp. 62–78,2015

[5] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, “Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information,” *Expert Systems with Applications*,vol. 42, no. 21, pp. 7560–7572, 2015.

[6] S. Magotra and K. Kumar, “Detection of HELLO flood attackon LEACH protocol,” in Proceedings of the IEEE International Advance Computing Conference (IACC ’14), pp. 193–198, Gurgaon, India, February 2014.

[7] V. K. Arora, “A survey on LEACH and other’s routing protocols in wireless sensor network,” International Journal for Light and *Electron Optics*, vol. 127, no. 16, 2016.

[8] P. Amish and V. B. Vaghela, “Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol,” in Proceedings of the 7th International Conference on Communication, Computing and Virtualization (ICCCV ’16), vol. 79, pp. 700–707, February 2016.

[9] I. Butun, S. D. Morgera, and R. Shankar, ―A Survey of Intrusion Detection Systems in Wireless Sensor Networks,IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 234-241.,May 2014.

[10] F. Bao, I. Chen, M. Chang and J. Cho, ―Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection,‖ IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169-183,Jun 2012.

[11] O. Khalid, S. Khan. S. Madani and M. Khan, ―Comparative study of trust and reputation systems for wireless sensor networks,‖ Security and Communication Networks, vol.6, no. 6, pp. 669-688, 2013.

[12] Y. Yu, K. Li, W. Zhou and P. Li, ―Trust mechanisms in wireless sensor networks : Attack analysis and countermeasures,‖ Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880,May 2012.

[13] A. Abduvaliyev, S. Lee, Y.K Lee, “Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks”, IEEE International Conference on Electronics and Information Engineering, 2010

[14] Y. Maleh, A. Ezzati, “A review of security attacks and intrusion detection schemes in wireless sensor network”, International Journal of Wireless& Mobile Networks (IJWMN) Vol. 5, No. 6, December 2013.

[15] H. Sedjelmaci, S.M Senouci“A Lightweight Hybrid Security Framework for Wireless Sensor Networks”, IEEE ICC, Sydney, 2014.

[16] K. Q. Yan, S. C. Wang, S. S. Wang, C. W. Liu, “Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network”, Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology, China, pp. 114-118, 2010