Development of Fuzzy Rule Based Secure and Reliable Routing Protocol for Heterogeneous Wireless Network

Mr.Vijaykumar Anandprakash Dixit
Department of Computer Science & Engineering
Nagpur Institute of Technology
RTMNU University, Nagpur ,India
Vijay.143dixit@gmail.com

Prof.Jagdish Pimple
Department of Computer Science & Engineering
Nagpur Institute of Technology
RTMNU University, Nagpur ,India
pimplejagdish@gmail.com

***Abstract*—**The network in which different type of devices such as PDA, laptop, tablets, cell phone etc are established a network for dispense information, communication and distributing files between nodes is called heterogeneous wireless network. In the heterogeneous wireless network the important problem is behavior of nodes .the nodes between sources to destination not only different hardware, energy capabilities but also may pursue different goals. The entrusted (malfunctioned) nodes drop the packet between source to destination and breaks the routing path .due to faulty hardware or software and responsible for disturbing the data transmission in the network .Here, we develop fuzzy rule based secure and reliable routing protocol for heterogeneous wireless network we used AODV as a based routing protocol so that in future if new nodes are inserted or any node is deleted in the network then our network does not disturb .we also used ESTAR protocol for finding the trusted based and energy aware nodes. ESTAR not only evaluates the node competency as well as reliability in relaying the packet with multidimensional trust values. We used this highly trusted node which has sufficient energy to reduce probability of breaking the routs due to the ESTAR routing protocol. the packet delivery ratio and routs stability is improved the trusted value of node calculated by the ESTAR based on the parameter of number of packets ,percent of sessions and the node ability to keep route connected which is theoretically possible but practically this wireless network parameter do not have a single valued but a set of value from which a decision has to takes place therefore we pass this trusted value to fuzzy ruled base and get practically possible trust nodes.

Keywords*-AODV, ESTAR , Fuzzy ruled base engine ,Heterogeneous Network.*

*****

I. INTRODUCTION

HWN is wireless network consists of devices like PDA, laptops, tabs, cell phones etc. with different potentiality or capabilities in terms of operating system, set of rules for communication and hardware and making network in between them .when source node or mobile node established a communication with destination node a remove station, it trust on other nodes in the network to reliable delivery of packets. Due to multichip packet transmission it increases the network

coverage area by using restricted power and help for improving spectral effectiveness. In HMWN the nodes mobility level and hardware/energy resource may vary greatly .HMWN implements in many useful application such as data dispense and multimedia data transmission. The node behavior is highly predictable in militarily and disaster recovery system because the network uses closed topology (like ring and mesh) and the nodes are controlled by one authority but in non-combatant, application the node can't predictable. In WSN nodes have different hardware and energy capabilities and may have different goals .untrusted nodes responsible for drop the packet and break the routing path due to faulty hardware or software. In HMWN some nodes may break routing path because they don't have sufficient energy to relay the source nodes packets and keeping the route connected due to this uncertainty in the nodes' behavior, randomly selecting the intermediate nodes will degrade the routes' stability. It will also so risky for reliability of data transmission and degrade the network performance in terms of packet delivery ratio (PDR). Only single intermediate node can responsible for break a route, and a small number of incompetent or untreated malicious nodes can continuously break routes. When a route is broken, the nodes have to rely on cycles of time-out and finding route for re-establishment of route. These route discoveries may incur network-wide flooding of routing requests that consume a considerable amount of the network's resources. In this project we developed a fuzzy rule base secure and reliable routing protocol for heterogeneous wireless network. We used a secure and reliable protocol for establishment of stable routes in HMWN. ESTAR determines the trusted value of the entire node between sources to destination. ESTAR determine the trusted values of nodes based on the parameter like number of packets, percent of session and the nodes ability to keep a route connected. This parameter has hard decision value which is very theoretical case but in practical wireless sensor network all this parameter that we discuss do not have a single value but they have a more than one values i.e. this parameter have different range of values from which a decision has to be take place. Therefore we used fuzzy ruled based routing protocol for getting most suitable route path. Fuzzy logic is an approach in which we calculate the result based on the degree of truthiness. It is different from binary logic. The problems which can't solve by using binary logic will easily solve using fuzzy logic. Fuzzy logic can be used to give the reasoning that is imprecise instead of fixed or exact. In fuzzy logic the truth value always between totally true and totally false. The rules is defined in the form of IF and Then. fuzzy logic are simple, flexible of combining conventional control techniques ,ability to model nonlinear function and imprecise information.

II. LITERATURE SURVEY

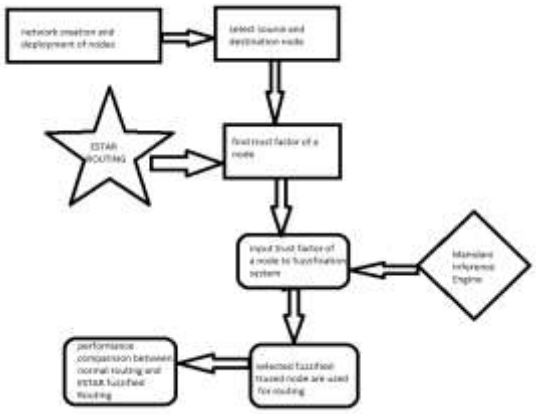
In [3] a reputation based scheme attempt to detect the untreated (malicious) nodes that drop packets with a route more than predefined threshold value in order to avoid them in routing .but reputation based scheme suffers from false accusation where trusted nodes that drop packets temporarily due to congestion, may be falsely identified as malicious by its neighbors .reputation based schemes also identify the black hole attackers that drop all the packets they are suppose to relay. By using a threshold to determine the trustworthiness of

a node is not effective in HMWNs because the nodes' packet-dropped rates vary greatly. Therefore, reputation schemes cannot guarantee route stability or reliability in HMWNs. Trust systems have been used in a various range of applications, including public key authentication, electronic commerce, and supporting decision making, etc., [4,5,6] incentive or payment schemes use credits (or micropayment) to encourage the nodes to relay on others packets [7,8,9]. Since relaying packets consumes the energy and other resources, packet relaying is treated as a service which can get credit point. The nodes earn credits for relaying others' packets and spend them to get their packets delivered. In Sprite [7], for every message, the source node signs the identity of the nodes in the route and the message. Each intermediary node verifies the signature and submits a signed receipt to trusted party to claim the payment. here the receipts overwhelm the network because one receipt is composed for each message. In order to reduce the receipts number, PIS [8] generated a fixed size receipt per route regardless of the number of messages. In ESIP [9], the payment scheme uses a transmission protocol that can transfer messages from the source node to the destination node with limited use of the public key cryptography operations for increasing the security. Public key cryptography is used for only one packet and then efficient hashing operations are used for next packets. Unlike ESIP that aims to transfer messages efficiently, E-STAR aims to establish stable and reliable routes. Although the proposed communication protocol in [9] can be used with E-STAR, here researcher uses a simple protocol due to space limitation. In [10], payment is used for thwart the rational packet-dropping attacks, where the attackers delete packets because they do not benefit from relaying packets. A reputation system is used to identify the irrational packet-dropping attackers once their packet- dropping rates exceed a threshold. The odorakopoulos and Baras [11] analyze the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, in which the edges correspond to the opinion that a node has about other node. The main goal is enable the nodes to indirectly build trust relationships using exclusively monitored information. In [12] Velloso et al. Proposed a human-based model which builds a trust relationship between nodes in the adhoc network. Without using the global trust knowledge, they have presented a protocol that scales efficiently for networks which is large in size. In [13], Lindsay et al. designed an information theoretic framework to quantitatively measure trust value and model trust propagation observed in local area network or other small networks. Trust is useful for measure of uncertainty and its value represented by entropy. The proof collected for malicious and benignant behaviors are probabilistically mapped by following a modified Bayesian approach method. The probabilistic estimate of Bayesian approach is then mapped with entropy. In [14], researcher developed a secure routing protocol with quality of service support has been proposed. The routing metrics are created by merging the requirements on the trust value of the nodes and the quality of service of the links along a route. [16] the researcher have found out the trust value of the node based on trust calculation without the false accusation .this calculation of trust is done with the help of ESTAR based system which takes into consideration the parameter of number of packets , percent of sessions and the nodes ability to keep a route connected. This parameter is considered in the paper are taken as hard decision value which is very theoretical case but in practical wireless network this parameter do not have only one value but a set of values from which a decision has to take place. e.g. number of packets send by a node can be low , medium or high where each of this range will have a series of values i.e. low can be 1 to 100 packet .Medium can be 100 to 10000 packets .High can be 1 lakh to 10 lakh packet But this paper consider only a simple set of value for each of the parameter . The main drawback of these approaches is that the trust value will be Calculated in an inaccurate manner there the overall security of the by sending data between nodes which might not be trustworthy and reducing system.

III. PROPOSED SYSTEM

In this paper by using a fuzzy rule base secure and reliable routing protocol we can calculate the accurate trust value of node and its practically possible. The time required for sending packets from source to destination will not be delay and the sensor nodes also energized every time. By using fuzzy ruled based secure and reliable routing protocol even if the congestion occurs in the heterogeneous network then also packet easily transfer from source to destination without any delay. Fuzzy Logic (FL) is a method for computing the results based on "degrees of truthiness". It differs from the conventional binary logic. In the Boolean logic, we used two values, "true or false" or "0 or 1". This logic also widely used in designing the modern computers. But for some application, the results cannot be represented into the absolute terms of 0 and 1. For solving such problems, Fuzzy Logic can be used to give the reasoning that is approximate instead of fixed or exact. in this theory, the truth values range occur between totally true and totally false.

The main advantages of Fuzzy Logic are its dependency on heuristics, simplicity, flexibility of combining conventional control techniques, ability to imprecise information model nonlinear functions and model nonlinear functions, use of empirical knowledge .Due to the basic characteristics of adhoc networks like uncertainty due to dynamic topology and mobility of nodes, unstable links and limited resources; a precise and accurate model is not possible to implement



A. *Fuzzification*

In fuzzification routing, the constraints first undergo fuzzification and are mapped into sets by using membership functions. after fuzzification phase the inference engine with the help of the rule base computes the fuzzy output. This fuzzy output is sent back after defuzzification. In fuzzification step all the input parameter i.e. trusted value get from ESTAR routing are converted from actual value to fuzzy range. e.g. packet will be 100 to 200 will be considered as low.

B. Application of rule engine

The fuzzy inference engine s the second phase in fuzzy routing .in this phase we takes the value of fuzzy inputs at each node and scans through the fuzzy rule base and find the appropriate entry corresponding to the fuzzy inputs for calculating the fuzzy output cost for each node. In this step all the fuzzy inputs are applied proper rules and the fuzzy value of output is find out e.g. if packet are medium and packet lost was low than the trust value is high.

C. Defuzzification

Defuzzifier produces a significant result in fuzzy logic. Therefore, defuzzifier produces a real-world output from the fuzzy outputs which are between the range [0, 1] by using defuzzification techniques. the main objective of fuzzy routing protocol is to select the paths with the better fuzzy cost, it doesn't require the fuzzy outputs to be defuzzified and results can be computed by comparing between fuzzy costs itself. As an example, consider two route P1 and P2.The better route can be detect as follows without further defuzzifying the fuzzy outputs:

If Fuzzy (P1) < Fuzzy (P2)
Better route= P1
else
Better route= P2.

In this step the output fuzzified values is defuzzified and converted to an actual numerical value e.g. actual trust value is 1 if the fuzzified trust value was high.This approach wills not only improved the accuracy of the system but also reduces the time require for finding out the trust value of the node.

IV. MODULE

i) Development of heterogeneous wireless network

Here we can create heterogeneous wireless network. The Heterogeneous wireless network (HWN) is a network where network consist of devices or computer with different capabilities in terms of hardware, operating system, protocols.Wireless sensor network id used in different types of application like Area monitoring,health care monitoring,Environmental and earth sensing application like air pollution monitoring,landslide detection,forest fire detection,water quality monitoring,natural disaster prevention,and Industrial monitoring application like machine health logging,data logging,water/waste water monitoring,and structural health monitoring. The WSN is constructed by using sensor nodes and sink nodes.sensor node in a wsn is capable of performing some processing and collecting sensory information and communication with other nodes connected in a network . WSN consists of a few to several hundreds or thousands nodes and each node is connected to one (or sometimes several) sensors.

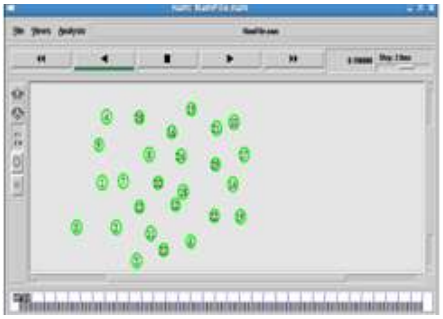


Fig 1. Generation of WSN and node scattered in the WSN

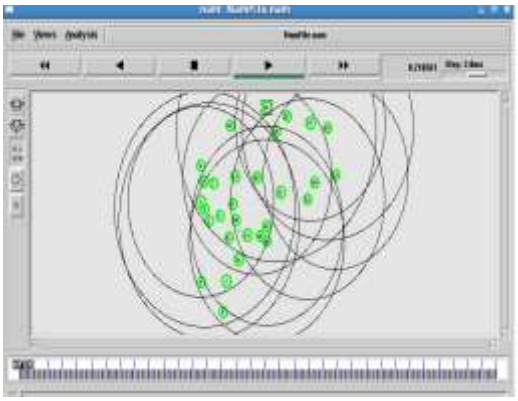


Fig 2.Path searching for Communication

Each sensor network node has part like a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit that used for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The data collected by all the sensor nodes are forwarded to a sink node. sometimes sink node is also known as base station.Therefore, the placement of the sink node has a major impact on the energy consumption and lifetime of WSNs.

ii) Development of ESTAR protocol for finding out trusted node.

ESTAR protocol for finding the trusted based and energy aware nodes. ESTAR not only evaluates the node competency as well as reliability in relaying the packet with multidimensional trust values. we used this highly trusted nodes which have sufficient energy to reduce probability of breaking the routs due to the ESTAR routing protocol. It uses the parameter like the parameter of number of packets, percent of sessions and the nodes ability to keep a route connected.

for calculating the trust factor of a node we consider two parameter like distance and the energy of the source node.if a node has a highest trust factor value then it is consider as a reliable node or trusted node and we transfer the packet by using that trusted node.in the future if congestion occure in network then also network not disturb and packet delivery will be done form source to destination without any delay.

the Euclidean distance is the distance between two nodes in the network. we used eculidean distance formula for calculating the node to node distance in wsn.The Euclidean distance between node p and q is the length of the line segment connecting them. the Euclidean distance is the distance between two nodes in the network. we used eculidean distance formula for calculating the node to node distance.The Euclidean distance between node p and q is the length of the line segment connecting them.Here we consider a two dimensional network for communication.therefore for calculating the euclidean distance we consider the parameter like transmitter location and receiving location of a node.if the distance is more but the energy required for transferring the packet is less then node considered as more trusted or reliable node.

For calculatinf the trusted factor of a node we used the formula

$$\text{Trusted factor of a node} = \frac{\text{Euclidean distance}}{\text{Energy of a source node}}$$

Euclidean distance = $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$

Where x_1 , y_1 is the transmitter location in a network
And x_2 , y_2 is the receiver location in a network
Here we consider the two dimensional network for data communication.

iii) Development of fuzzy ruled base ESTAR protocol for routing Module

a fuzzy rule base secure and reliable routing protocol we can calculate the accurate trust value of node and its practically possible. The time required for sending packets from source to destination will not be delay and the sensor nodes also energized every time. By using fuzzy ruled based secure and reliable routing protocol even if the congestion occurs in the heterogeneous network then also packet easily transfer from source to destination without any delay.

Fuzzy Logic (FL) is an method for computing the results based on "degrees of truthiness". It differs from the conventional binary logic. In the Boolean logic, we used two values, "true or false" or "0 or 1". This logic also widely used in designing the modern computers. But for some application, the results cannot be represented into the absolute terms of 0 and 1. For solving such problems, Fuzzy Logic can be used to give the reasoning that is approximate instead of fixed or exact. in this theory, the truth values range occur between totally true and totally false.

In fuzzification routing, the constraints first undergo fuzzification and are mapped into sets by using membership functions. After fuzzification phase the inference engine with the help of the rule base computes the fuzzy output.This fuzzy output is sent back after defuzzification.

In fuzzification step all the input parameter i.e. trusted value get from ESTAR routing are converted from actual value to fuzzy range. The fuzzy inference engine s the second phase in fuzzy routing .in this phase we takes the value of fuzzy inputs at each node and scans through the fuzzy rule base and find the appropriate entry corresponding to the fuzzy inputs for calculating the fuzzy output cost for each node.

Defuzzifier produces a significant result in fuzzy logic. Therefore, defuzzifier produces a real-world output from the fuzzy outputs which are between the range [0, 1] by using defuzzification techniques. The main objective of fuzzy routing protocol is to select the paths with the better fuzzy cost, it doesn't require the fuzzy outputs to be defuzzified and results can be computed by comparing between fuzzy costs itself.

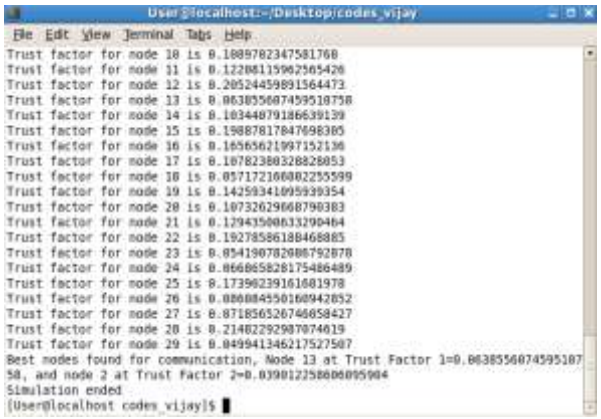


Fig 3 trusted factor of a node

iv) Performance evaluation of fuzzy ESTAR system and optimization of rule

In performance evaluation we analyze the performance that we get from ESTAR and fuzzy and also apply the optimization rules. In this module we Select nodes for communication, after selecting nodes find the best possible nodes for routing using the trust value . On the basis of trust value Select routing solutions from these nodes and Use the best possible route from the given solutions for evaluating the result.

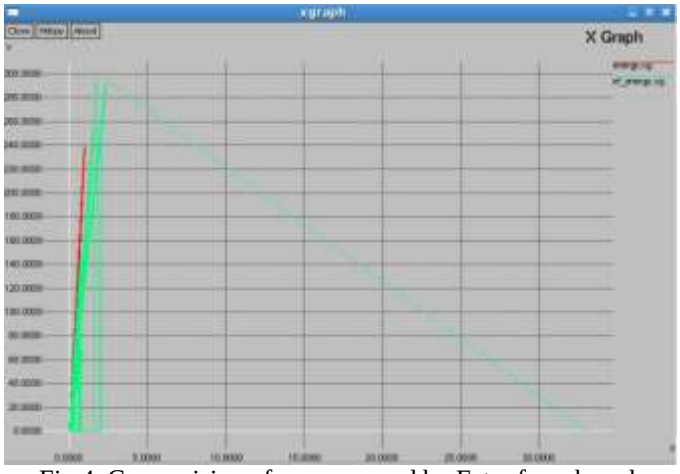


Fig 4. Comparision of energy saved by Estar fuzzybased routing and normal routing

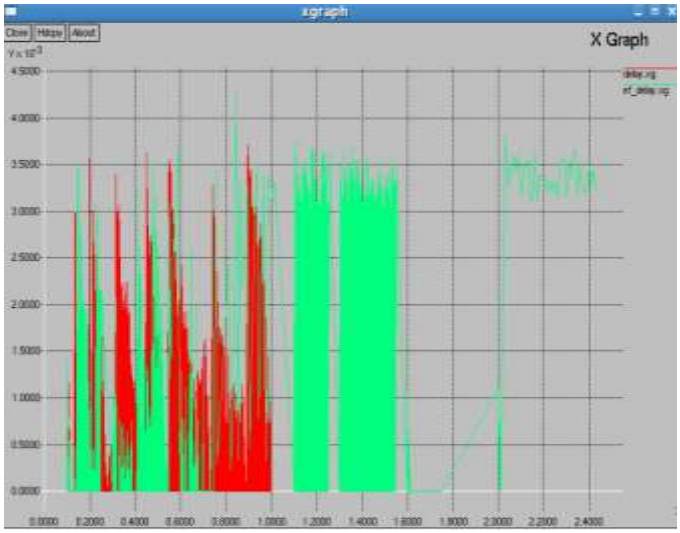


Fig 4. Comparision of delay produced by Estar fuzzybased routing and normal routing

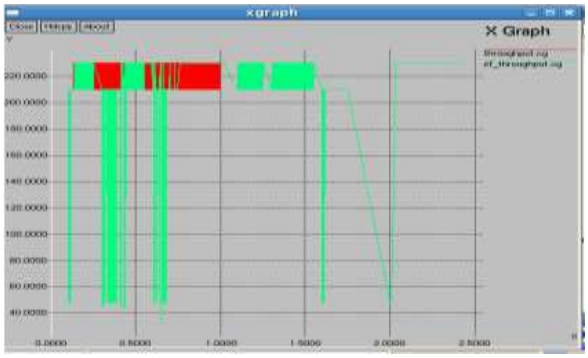


Fig 5. Comparision of throughput produced by Estar fuzzybased routing and normal routing

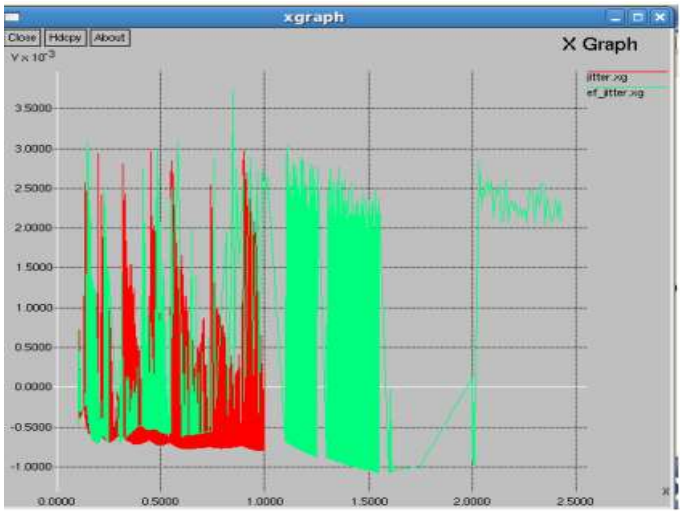


Fig 6. Comparision of jitter produced by Estar fuzzybased routing and normal routing

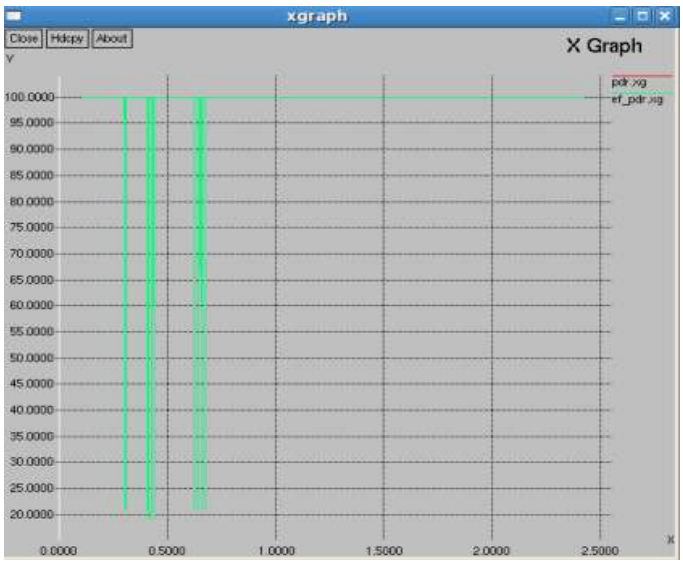


Fig 7. Comparision of pdr ratio produced by Estar fuzzybased routing and normal routing

V .CONCLUSION AND FUTURE SCOPE

By using the routing protocol based on fuzzy logic we not only determine the trusted node in a wireless sensor network but also the value of the trusted node is accurate as compare to reputation scheme ,ESTAR etc. The time required for sending packets from source to destination will not be delay and the sensor nodes also energized every time. even if the congestion occurs in the heterogeneous network then also packet easily transfer from source to destination without any delay. The node behavior is highly predictable in militarily and disaster recovery system because the network uses closed topology (like ring and mesh) and the nodes are controlled by one authority but in non-combatant, application the node can't predictable but by using fuzzy protocol in a routing the node bahaviour was easily predictable in a militarily and disaster recovery system.The fuzzy logic has a potential to solve the complex situation and imprecision in the data by using heuristic human reasoning and there is no need to used the complex mathematical model for calculating the data. It has a application in the field of signal processing,speech recognition,aerospace,embeddedsystem,robotics etc.

V. REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks", Bell Labs Technical , vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks", IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Mis- behavior in Mobile Ad Hoc Networks", Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.

[4] X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks", Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242, 2012.

[5] G. Indirania and K. Selvakumara, "A Swarm-Based Efficient Dis- tributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)", Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014.

[6] H. Li and M. Singhal, "Trust Management in Distributed Sys- tems", Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.

[7] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks", Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

[8] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System For Multi-Hop Wireless Networks", IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[9] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks", IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.

[10] M. Mahmoud and X. Shen, "An Integrated Stimulation and Pun- ishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks", IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

[11] G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks", IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[12] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scal- able Maturity-Based Model", IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

[13] S. Lindsay, Y. Wei, H. Zhu, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305- 317, Feb. 2006.

[14] M. Yu and K. Leung, "A Trustworthiness-Based QoS Routing Pro- tocol for Wireless Ad Hoc Networks", IEEE Trans. Wireless Comm., vol. 8, no. 4, pp. 1888-1898, Apr. 2009.

[15] Di Tang Tongtong Li Jian Ren and Jie Wu "Cost - Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks",IEEE Transactions on Parallel and Distributed Systems., 2014

[16] Mohmad M.E.A. Mahumad,Xiaodong Lin,Xue "Secure and Reliable routing protocol for Heterogeneous Multihop Wireless Network", IEEE transactions on parallel and distributed systems, vol. 26, no. 4, april 2015