A FUZZY BASED CROSS LAYER PROTOCOL FOR TRUST ERECTION IN WIRELESS SENSOR NETWORKS

K. Anusha[1], *A. Naveena*[2]

1. Student, Branch of WMC, G.Narayanamma institute of technology and science,JNTUH,Hyderabad,India.

2. Assistant Professor,Dept.of ETM, G.Narayanamma institute of technology and science, JNTUH, Hyderabad, India.

ABSTRACT:- The cross layer model is used to admit synchronization, exchange by overlapping multiple layers and joint improvement of procedures holds the key purpose of primary layers. It enables elasticity, reliability and efficiency in communication method. The fuzzy logic system(FLS) is employed to implement node selection mechanism to offer an effective transmission. Amongst these assistances, this model outsides a problem with security attacks in a network. To diminish these threats in a network, The Trust based fuzzy implicit cross layer protocol (TruFiX) which is a Trust based cross layer module(T-XLM)based protocol is used to allow and grip inter layer data exchange to adapt traffic attentiveness and develop system form. The enhancement of TruFiX is proposed protocol to overcome the problem of malicious node during transmission by choosing an substitute route. By taking into account with simulation results, proposed protocol was compared with FUGEF and TruFiX which shows an increment in the packet delivery ratio(PDR) and throughput of the system.

KEYWORDS:- Cross layer approach, Fuzzy logic system, wireless sensor networks, malicious node, forced fairness approach

I. INTRODUCTION

Wireless sensor network(WSN) consists of interconnected sensing element that communicate wirelessly to gather information regarding the encircling atmosphere. As sensor node has fixed energy assets, so smaller amount of energy must be expended to increase the efficiency of the scheme. An enhancement in energy and quality of service(QOS) is attained by cross layer protocols[1] than conventional layered protocols. In cross layer approach most of the methods are unsuccessful in considering the notion of complete security phenomenon to disapproval its value in existing system and communication procedures. To offer security in this protocols they failed in transporting security at less than three layers, which consume constraints to establish security mechanisms which tend to exploit significantly on resources. These conditions in a network tend to face the difficulty of raised delay, minimum lifetime and null delivery due to drain nodes. The trust worthy systems are implemented to overcome these problems to afford secure data delivery.

Trust is definiteness of honesty among two entities which are convoluted in communication and is attained by accepting created evidence from prior events and renovated to give a statement to handle future nodes dealings. The superimposed layout of node is not able to create a code which is capable of mitigating all threats in a network. The TruFiX protocol which is employed based on two frameworks and the enhancement of this protocol is proposed protocol embraces a modified IEEE 802.11 Distributed Coordinate Function(DCF) Media access Control and utilizes FLS to plan a report mechanism to distribute tranquil transmission mechanism. Among the simulation interpretations held, the guaranteed performance of suggested protocol among TRUFIX and FUGEF was related in the existence of malicious node and attained better performance.

II. LITERATURE SURVEY

DWSIGF[2] transmitting protocol improves enactment on selection mechanism of SIGF[1] protocol by selecting malicious nodes using collection window duration which rises its window period vigorously to built time shift in protocol versions. This protocol uses data link layer and routing layer functionalities. FUGEF [3] is employed to choose a sending candidate node that abolishes significant packet failures in network and afford improved security in system. It has low PDR and spatio-temporal calculations are not conceivable. The FUGEF exceeds DWSIGF in terms QOS performance, energy depletion and complete presentation of security facility, when exposed to black hole occurrences. When endangered to Sybil attacks no outcomes were shown as DWSIGF and FUGEF are modified only to black hole attacks.

The TruFiX[4] protocol embraces an altered IEEE 802.11 DCF MAC and two FLS to improve a response method to certify protected directing process. This is executed centered on XLM Framework and T-XLM Framework. The FLS are implemented in both the channel arrangement phase for reformed initiative determination and packet replacement phase for the reputation build-up. This protocol outsides problem if it identifies malicious node in the broadcast, as it halts the transmission of data which reduce the PDR and throughput of the network.

III. PROPOSED METHOD

The proposed protocol an enhanced trust based fuzzy implicit cross layer protocol is applied based on two frameworks:

1. XLM Framework

2. T-XLM Framework.

3.1 THE XLM FRAMEWORK

In this Framework[4] the parameters are plotted to the sensor protocol store to gain its amalgamation. In this manner it gives whole info to a node about taking part in the transmission mechanism. The communication method begins with a initialization phase which comprises a variable initiative(I_d) is allotted to 1 if the adjacent node fulfils all the 4 conditions and 0 if elsewise as shown in equation(1). The following conditions are recognized by constraints which show the intrinsic abilities of the protocol stack and which consists: relay packet rate λ_{relay} , remaining buffer capacity β, residual energy of node $E_{rem}$and signal to noise ratio ξ_{rts}.

$$I_d = \begin{cases} 1 & \text{If } \begin{cases} \xi_{RTS} \geq \xi_{RTS}^{Th} \\ \lambda_{relay} \leq \lambda_{Th} \\ \beta \leq \beta^{max} \\ E_{rem} \geq E_{rem}^{min} \end{cases} \\ 0, & \text{otherwise} \end{cases} \quad \textbf{(1)}$$

3.1.1 TRUST ESTIMATION PROCESSES

Trust is denoted as a recognition which is produced from control theory advised in the field of E-commerce to select reliable skill entities. Exploration evolved by applying the concept into different realms using skilled actions to efficiently evaluate trust through the performing objects in figure1.

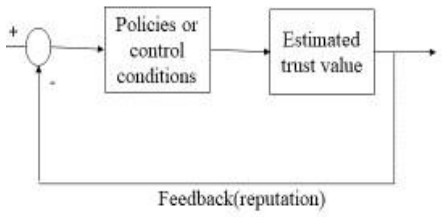

FIGURE 1:-A Typical Trust Model

The trust is estimated from previously invented evidences joined with reputation transmitted from contributing objects with in a network.

3.2 THE T-XLM FRAMEWORK

This scheme[4] is a sustained version of XLM Framework. It deeds trust in taking a packet transporting node to accelerate packet towards destination. The T-XLM theory TI is clarified in equation2, a association between the initiative resolution (I) and reputation(R).

$$TI = I \otimes R \qquad (2)$$

The modified I is shown in equation3

$$I = \begin{cases} Good, & \text{If } \begin{cases} \xi_{RTS} \geq \xi_{RTS}^{Th} \\ \omega_{relay} \leq \omega_{relay}^{Th} \\ \beta_{op} \leq \beta_{op}^{Th} \\ T \geq T^{Th} \\ E_{rem} \geq E_{rem}^{Th} \end{cases} \\ Fair, & \begin{cases} \xi_{RTS}^{min} \leq \xi_{RTS} < \xi_{RTS}^{Th} \\ \omega_{relay}^{min} \leq \omega_{relay} < \omega_{relay}^{Th} \\ \beta_{op}^{Th} < \beta_{op} \leq \beta_{op}^{max} \\ T^{min} \leq T < T^{Th} \\ E_{rem}^{min} \leq E_{rem} < E_{rem}^{Th} \end{cases} \\ \text{Unsuited, if Otherwise} \end{cases} \quad \textbf{(3)}$$

I is stated in a inherited language that is simply derived. The factors are outlined as ε_{RTS} is the received SNR value of the Request To Send(RTS) transmission resolute from resultant SNR ,ω_{relay} is defined as relay packet rate of a node deducted by the holding interval of packets gathering the RTS telecast and β_{op} is the barrier residency interval,E_{rem} is known as remaining energy of node.

$$R = \begin{cases} Trusted\ (T \geq T^{Th}) & \text{if } \begin{cases} Sr \geq Sr^{Th} \\ fr \leq fr^{Th} \\ \tau \leq \tau^{Th} \end{cases} \\ \text{Uncertain}(T^{min} \leq T < T^{Th}), & \text{if } \begin{cases} Sr^{min} \leq Sr < Sr^{Th} \\ fr^{Th} \leq fr < fr^{max} \\ \tau^{Th} \leq \tau < \tau^{max} \end{cases} \\ \text{Distrusted,} & \text{if } Otherwise \end{cases} \quad \textbf{(4)}$$

R define value of the node reputation that is the improved trust T value. Furthermore, *sr* states success ratio to show a nodes ability in broadcast of packet, *fr* is fairness ratio to guarantee path adjustment and τ is the interval of data transmission.

3.3 THE PROPOSED PROTOCOL

The TruFiX protocol omitted conversions that embrace trust and distrust as inconsistent balances of scale. The proposed protocol which is an enhancement of TruFiX protocol outfits routing procedure in two stages:-

1. CHANNEL ALLOCATION PHASE
2. PACKET REPLACEMENT PHASE

The FLS is implemented in both phases to direct packet to end point.

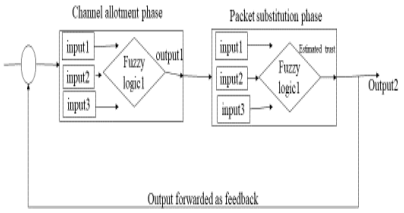

FIGURE 2:-Proposed Fuzzy Logic Design

3.3.1 THE CHANNEL ALLOCATION PHASE

The congregated response parameters comprises of progressive distance value (d)demonstrating the distance amongst the transmitting node and the sender node S, CTS response interval (ω), that is a purpose of link quality established on node dissemination in relation to distance as well as extra waiting period due to inter-frame spacing and the original trust(T) rate that is fix to 0.5. This is in

agreement with the trust formation values in abundant explores such as [20], [21], [33] just to remark a few. Each and every nodes reply is operated by the first fuzzy logic system to select the successive communicating candidate node and rated them as good, fair or unsuited.

3.3.2 THE PACKET REPLACEMENT PHASE.

In this method, info is transferred out of S to selected delivering contestant. After the completion of packet substitution, the candidate node is examined built on 3 Parameters which involves Sr, τ ,*fr* send to second FLS and rated as (trusted, distrusted, uncertain) and reverted as feedback to modernize the trust value by reputation R.

The whole transmission procedure is outlined in figure4.The transmission of data from sender to destination takes place as determined in figure4 below. Initially the sender broadcasts the ORTS messages to all the candidate nodes ,on receiving it the nodes calculate the parameters such as Forward distance value(d),CTS reply time(ω),Trust value(T) to include in the CTS reply. The response is 30 collected and transmitted as inputs to the first FLS and then the best candidate node is chosen and the data exchange is initiated, by calculating nodes parameters and selection frequency.

By implementing forced fairness method which allows every node to keep a list of nodes participated earlier, therefore if the node didn't took part previously in the transmission method, then its success ratio(Sr),fairness ratio(fr) and transfer period (τ) are given as inputs to the second FLS. Otherwise node is penalized by decreasing its fr and τ values, that it should not be selected in future interactions. If the node is a malicious node then it is penalized by the method and chooses an alternate neighbor route or else the nodes parameters are calculated to determine R .On completion of the processing of the parameters the trust value(T=R) and node list is also updated. The acknowledgement is send after the completion of forwarding of the data and it is continued until forwarding candidate is final destination.

In this protocol, if a malicious node is noticed in the routing process it takes an alternate route which results in minimum packet loss as it delivers the packets towards destination.

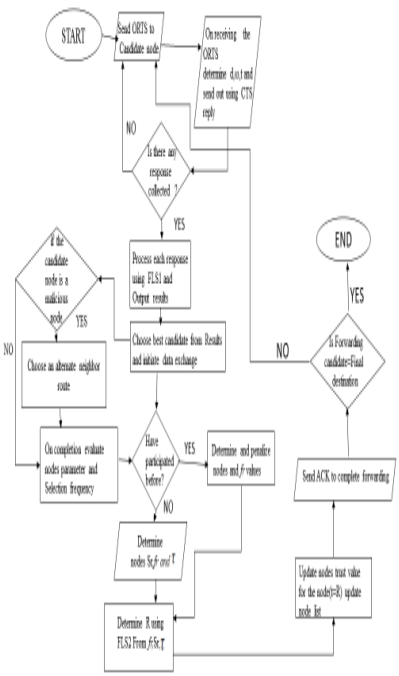

FIGURE 3:- FLOW CHART FOR ROUTING PROCESS

3.3.3 THE FUZZY LOGIC SYSTEM(FLS)

The FLS is an computationally intellectual system which is utilized to execute human like results that is simple and easy to recognize. From Figure3 FLS manages three variables using 27 rules. In the first FLS the (d, ω ,T) and rated as(good, fair and unsuited). The FLS2 process the variable (*sr*, *fr* and τ) and graded as trusted, distrusted and uncertain. The outcome produced is restored back as trust input to the first FLS which is generated from the second FLS, thus upgrading the previous misprision value 0.5 original trust value for that candidate node. The highest chance value is nominated as the finest transmitting candidate from figure5.

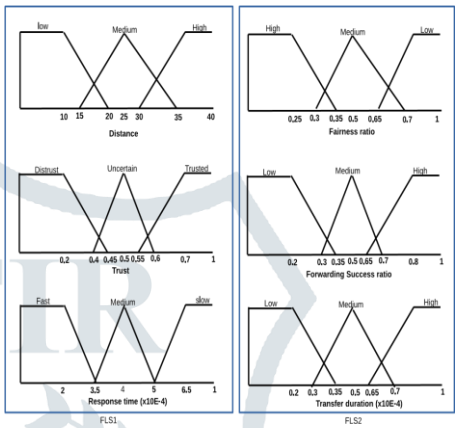

FIGURE 4:- Input Membership Functions for TruFiX

IV. RESULTS AND DISCUSSION

The performance of the Existing protocols (FUGEF), TruFiX and Extension of TruFiX are implemented using NS2 simulation. The parameters which are evaluated in these protocols are PDR, end to end delay, throughput and energy consumption of the network .

From figure9 among FUGEF, Existing and Extension the proposed protocol has achieved high PDR and less possibility of attacker selection. Thus, our proposed protocol outperforms all the other three protocols by mitigating the security threats in a network.

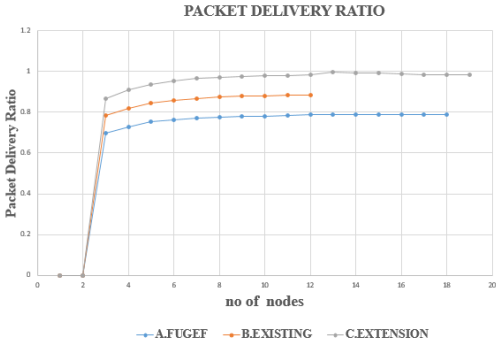

FIGURE 5: Packet Delivery Ratio.

From the above figure 14, the extension protocol achieved high PDR due to the node selection criteria by using forced fairness approach and FLS.

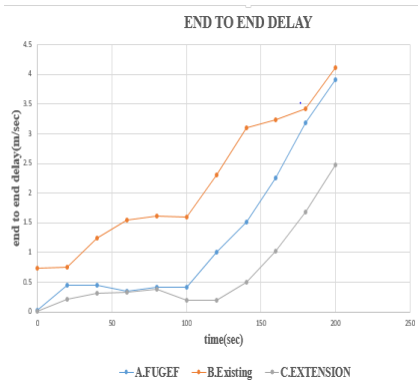

FIGURE 6: End to End Delay

From above figure 7 the enhancement protocol has high delay due to the processing in fuzzy logic system and to choose a alternate neighbor route which decreases delay than other protocols TRUFIX and FUGEF.

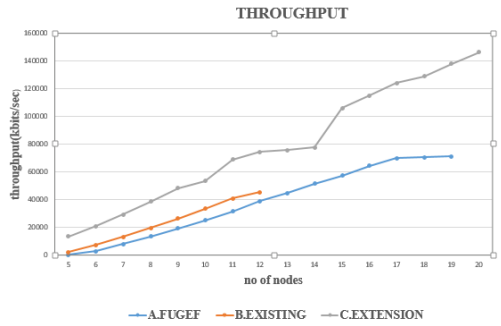

FIGURE 7:THROUGHPUT

From the above figure 8 the suggested one has maximum throughput as it has high success rate of reception at the destination due to the process done in the fuzzy logic system and also routing in an alternate route resulted in high throughput compared to other protocols.

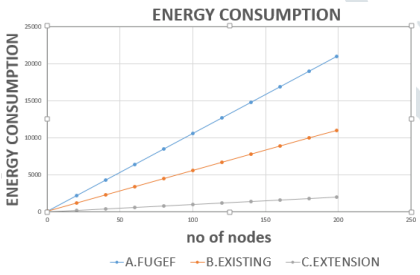

FIGURE 8:ENERGY CONSUMPTION

From the above figure 9,our projected protocol E-TRUFIX has less energy consumption in the whole transmission process as it finds an alternate route when it notice a malicious a node which in turn reduces the energy consumption than other protocols.

V CONCLUSION AND FUTURE SCOPE

The existing protocol TruFiX implements a forced fairness approach and penalize the nodes that participated and malicious node ,if it detects in the routing process and halts the transmission. To overcome the problem the proposed protocol is implemented which provides an alternate path after detecting a malicious node and securely transmits the packet to the destination by employing FLS. The results outlined show that the proposed protocol outperforms than other protocols such as TruFiX and FUGEF. This protocol acquired high PDR and throughput and reduced delay and energy consumption. Future experiments will include different threats and evaluation of other variables like β_{op} and E_{rem} to the FLS to specify the part that these variables act in blocking various forms of threats.

REFERENCES

[1] M. C. Vuran and I. F. Akyildiz, ``XLP: A cross-layer protocol for efficient communication in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 11, pp. 1578_1591, Nov. 2010.

[2] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, ``SIGF: A family of configurable, secure routing protocols for wireless sensor networks,"in *Proc. 4th ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2006, pp. 35_48.

[3] Z. M. Hanapi, M. Ismail, K. Jumari, and M. Mahdavi, ``Dynamic window secured implicit geographic forwarding routing for wireless sensor network," in *Proc. Int. Conf. Wireless Commun. Sensor Netw. World Acad. Sci., Eng. Technol.*, 2009, pp. 173_179.

.[4] I. A. Umar, Z. M. Hanapi, A. Sali, and Z. A. Zulkarnain, ``FuGeF: A resource bound secure forwarding protocol for wireless sensor networks," *Sensors*, vol. 16, no. 6, p. 943, 2016.

[5] idris abubakar umar1, zurina mohd hanapi1, (member, ieee),a. sali2, (member, ieee), zuriati a. zulkarnain1, (member, ieee)
``Trufix: A Configurable Trust-Based Cross-Layer Protocol For Wireless Sensor Networks``.

[6] Z.Wei, H. Tang, F. R.Yu, M.Wang, and P. Mason, ``Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning,"*IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4647_4658, Nov. 2014.

[7] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, ``E-hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks,"*Ad Hoc Netw.*, vol. 7, no. 6, pp. 1156_1168, 2009.

[8] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, ``A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw.*,
2005, pp. 1_10.

BIBILIOGRAPHY

K.Anusha Pursuing M.Tech in the department of WMC,G.Narayanamma Institute Of Technology and Sciences,under JNTUH, Hyderabad, Telangana, India.

Ambidi Naveena at present working as Assistant Professor in ETM Department ,G.Narayanamma Institute of Technology and Sciences, Hyderabad, She completed B.Tech from G. Narayanamma Institute of Technology and Sciences, Hyderabad.
M.E from Osmania University ,Hyderabad. At present pursuing Ph.D from JNTUH. She has 12 years of teaching experience.