# A Review On Cross Layer Routing Protocols In Wireless Sensor Networks

K.Anusha[1], A.Naveena[2]
[1]*Student, Branch of WMC,G.Narayanamma institute of technology and science,Hyderabad,India.*
[2]*Assistant Professor,Dept.of ETM,G.Narayanamma instituteof technology and science,Hyderabad,India.*

**Abstract- Wireless Sensor Network consists of enormous amount of sensor nodes that sense the physical parameter changes from the sensing range and gathers this information and forward it to the sink.As the sensor nodes have limited battery so the energy efficiency is the crucial factor .To reduce the energy consumption selection of forwarding candidate to route towards the destination is the main criteria in wireless sensor networks. This process of selecting the relay node is accomplished using cross layer approach as it is not possible by traditional layer approach. The cross layer approach is used to provide reliability,adaptability,flexibility and efficiency in communication process.This paper proposes the survey on protocols using cross layer mechanism and its limitations.The three main categories for comparison are explored in this paper are a type of method for node selection, prevention of attacks, energy consumption.**

**Keywords - Wireless sensor networks, cross layer,security,energy efficiency,Fuzzy logic system,blackhole,Sybil,replay DOS.**

## I. INTRODUCTION

Wireless sensor network consists of small embedded devices called sensor nodes which are used to sense the changes in environmental and physical conditions and collect the information and relay the data to the base station or sink.In wsn time synchronization and also location information of source,candidate nodes and destination plays a major role in routing the data to the destination.As the sensor nodes are small in size they can be deployed in huge numbers on large scale which in turn increases the coverage and enhances the performance of the network.

Cross layer approach is used to exchange different information among different layers and enhances the performance of the entire network,where as traditional layered approach doesn't share information among layers and it is only suitable to wired networks.Cross layer can be used to increase the performance,data rate,energy efficiency and quality of service by utilization of techniques.The cross layer integrates the functionalities from physical to application layer in order to adapt to changes in environment.As the sensor nodes have limited energy resources so by using the cross layer approach the resource bound security routing protocols have been implemented to improve the energy efficiency in network. The node selection place a major role in transmission of the data to destination by consideration of parameters such as distance,remaining energy,cost etc. This survey paper proposes the different routing protocols using different methods in selection of relay node by using cross layer approach.

## II. LITERATURE SURVEY

*2.1 Energy efficient beaconless geographic routing (ebgr)*

EBGR provides a guaranteed loop free delivery from source to sink as long as the network is connected.It utilizes the physical,MAC and routing layer functionalities. It minimises energy consumption by choosing the neighbour with optimal relay position as next hop.EBGR is further extended to lossy sensor networks to deal with dynamic topology.

EBGR works in two modes:-

*2.1.1 Beaconless greedy forwarding mode:-*

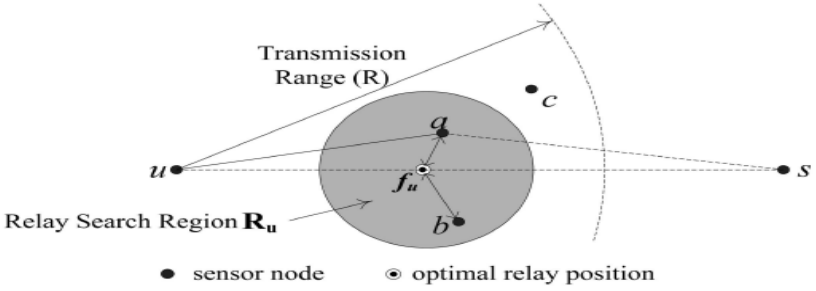


Figure:-Forwarding Area

A node which has a packet to transmit,first calculates its distance as it knows its current position and sink's position,if sink is nearby it directly transmits data.Otherwise it broadcasts RTS message in relay region as shown in above figure. On receiving RTS the nodes send CTS messages in response and the one which is received with minimum delay is selected as next hop neighbour and on overhearing it, the nodes in relay region cancel their responses. If no node is in the relay region then the forwarder enters into the beaconless recovery mode

*2.1.2 Beaconless recovery mode:-*

In this mode it uses angular relaying algorithm to recover from local minimum.The angular relaying algorithm uses two phases:-

Selection Phase:-In this phase a forwarder broadcasts RTS message and nodes reply with CTS messages in counter clockwise order based on angular delay function.Then the protest phase begin after the first candidate valid CTS response.

Protest Phase:-Let the w node is the first candidate to send CTS then only the nodes in $N_{GG}$(u,w) (Gabriel circle having uw as diameter) are allowed to protest.Finally the forwarder sends the packet to the selected candidate.

The Advantages of this protocol are:-

EBGR has the characteristics of both geographic and power aware routing.

It provides loop free,stateless and energy efficient communication in dynamically changing topology and lossy sensor networks.

It consumes less energy than other protocols.

The Disadvantages of this protocol are:

It is accessible only to attack free environment.

It suffers from energy insufficiency problem as residual energy is not considered.

*2.2 A mac/routing cross layer approach to geographic forwarding in wireless sensor network(macro)*

In Geographic forwarding there is no need to know the information regarding location, as the node should know only its coordinates and of destination.In order to support this geographic forwarding,MACRO integrates MAC and Routing layer functionalities in order to deliver packet to destination.MACRO selects the next best relay node based on the energy efficient choice taken by the current relay node at each hop. MACRO exploits the information regarding the capability of nodes in order to use different transmission power levels to increase the efficiency towards destination per unit transmission power.

The current relay node triggers a competition to choose best next relay node among all relay nodes by increasing transmission power levels.This process repeats until better node is selected if there is no use in increasing power and the information passed to it.

MACRO protocol is composed of two algorithms:-

Selection of next relay node

Wake up

*2.2.1 Selection of next relay node:-*

The current relay node runs a procedure in which the next best relay node is selected .let us consider $R'$ is the current relay node and $R''$ is the candidate relay node and P is the transmission power used to transmit data to candidate relay node and d(A,B) is the distance between node A and B, $G_{R',R''}$ is the weighted progress towards destination obtained per unit transmitted power as shown in below equation.

$$G_{R',R''} = \frac{d(R',D) - d(R'',D)}{P} \qquad (1)$$

At each hop the weighted progress factor must be maximised for the selection of next relay node.let i be the variable used to represent the set of neighbours in which relay node is selected and it is initially set to $1 S_i(R') = S_1(R')$ and increased by 1 every time until it is estimated that increase in transmission power will maximize the progressive factor.This process will continue until further increase in power will not increase in weighted progress factor.

*2.2.2 Wake up of neighbour nodes:-*

In order to decrease the energy consumption MACRO cyclically switch OFF the wireless interface and $T_{cycle}$ is the duration of cycle and $T_{ON}$ is the duration of each interval and is switched ON during each cycle.Acurrent relay node sends WAKEUP messages to wake up the neighbour nodes for a particular time interval $T_{cycle}$ and a control message GO AHEAD to trigger up the competition between nodes.The nodes on receiving the WAKEUP messages be awake and waits for the GO AHEAD control message.The current relay node should wakeup all neighbours in a particular time period.The node waits for a time interval after receiving GOAHEAD message and sends its weighted progress factor, now the current relay node will select the best relay node based on the progress factor.If a collision occurs it uses backoff procedure using CSMA/CA mechanism and if it doesnot receive any message in particular time period the wireless interface is SWITCHED OFF.

The Advantages of this protocol are:-

To increase lifetime of network, the capability of nodes to exploit different transmissionpower levels are considered.

To reduce energy consumption the wireless interface is switched OFF and ON.

The weighted progress factor is maximised in order to select next relay node at each hop.

The disadvantages of this protocol are:-

End to End delay is increased due to number of hops travelled by the packets.

*2.3.Sigf:-a family of configurable secure routing protocols for wireless sensor networks*

Due to the severe resource constraints in wireless sensor networks it give rise to resource bound security solutions SIGF is based on IGF Non Deterministic/MAC routing protocol which is stateless allows to handle dynamic topologies.

SIGF comprises three protocols:-

*2.3.1 SIGF-0:-*

It keeps no state and routing information but it achieve high Packet delivery ratios probabilistically.SIGF-0 selects next hop relay by dynamically increasing the collection window based on responses this will prevent attack possibility to some extent.A source S sends ORTS messages which doesn't contain information regarding location of source and destination in order to avoid attacks to one hop neighbours and on receiving it the nodes turn ON their CTS timers and on expiry they respond CTS response to S. It collects the responses until collection window closes and selects the candidate node based on priority and remaining energy that makes best progress toward destination and the data is forwarded to node.

*2.3.2 SIGF-1:-*

It keeps local state, no shared keys between nodes in network and gathers information from neighbours about its current state and statistics of neighbours and it is able to defend against Sybil attacks.SIGF-1 is classified in three categories:- data of local node,statistics about neighbour nodes,derived values from both. Each local node maintains the number of messages sent by node to all neighbours and calculate derived values at each node, it also contain buffer B which contains recently stored messages.At each neighbour we keep the following:- $N_{sent}, N_{location}, N_{delay}, N_{forward}$.On the transmission of message the copy of message is stored in buffer B with timestamp.The message is flushed from buffer if t it is overheard by its relay to the downstream node.The $N_{forward}, N_{delay}$ are updated if the buffer fills $N_{sent}$with message loss and failures.A reputation above threshold is selected and it is based upon options:earliest responder,random responder,responder with highest routing priority.The threshold calculations are used to reduce wastage of energy in sending message to neighbour with known poor performance and claims to be the best route.If no nodes are above threshold then a suboptimal route is selected with high reputation.Hence SIGF-1 performs well with black hole and Sybil attacks.

*2.3.3 SIGF-2:-*

To provide strong security guarantees it uses neighbourhood shared state at a greater cost. It uses pairwise shared keys in neighbourhood.SIGF-0 and SIGF-1 protect against attacks by adding nondeterminism to dynamic forward candidate selection.But it shows poor performance against some attacks,to overcome that limitation SIGF-2 uses shared keys using cryptographic operations which provideauthenticity,freshness, integrity and confidentiality.

The state and protocol configuration options required for use of SIGF-2 are:-

MESSAGE AUTHENTICATIONϵ{ all MESSAGES, only DATA, NONE}:-Authentication may be provided to the protocol messages(ORTS,ACK,DATA,CTS) or only to DATA portion which further decreases communication overhead and computation but does not prevent replay attacks.
MESSAGE SEQUENCINGϵ{yes,no}:- In this process the protocol messages have increasing sequence number s.A receiver accepts the message from neighbour N when s is greater than sequence number of N in order to obtain freshness and the sequence number of the neighbour should be updated upon every reception.
PAYLOAD ENCRYPTIONϵ{yes,no}:-It uses a shared key between ORTS sender and the relay to hide the contents of data message from attackers.

| Protocol | General approach | Corruption | Wormhole | HELLO flood | Black hole | Sybil | Replay DOS |
|---|---|---|---|---|---|---|---|
| IGF | Dynamic binding | yes | yes | Yes | no | no | No |
| SIGF-0 | Non Determinism | yes | yes | Yes | yes | no | No |
| SIGF-1 | Local Reputation | yes | yes | Yes | yes | yes | No |
| SIGF-2 | Cryptography | yes | yes | Yes | yes | yes | Yes |

Attacks Resisted By IGF and SIGF protocols
The Advantages of this Protocol are:-
Next hop is chosen deterministically and dynamically.
Robustness to mobility andfailures.
It provides data freshness by message sequencing.
Fixed window period is used to select non malicious nodes.
The Disadvantages of this protocol are:-
Greater Cost in order to implement cryptographic mechanisms.
Minimal security is only provided at greater cost.

*2.4.Dynamic window secured implicit geographic forwarding routing protocol(dwsigf)*
DWSIGF routing protocol improves on sampling process in SIGF in order toselectmalicious nodes by dynamic collection window period to create time shift in protocol semantics.This protocol uses MAC and network layer for routing and provides handshake mechanism for node to node transmission in 60 degrees sextant centered on direct line with destination as shown in below figure.

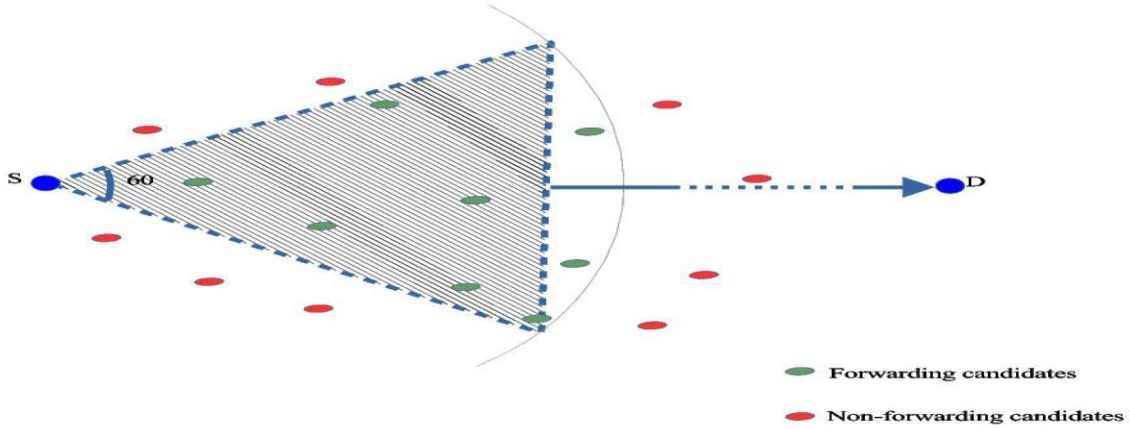


Figure:-Forwarding Area

The forwarding area which consists of forwarding and non-forwarding candidates as explained in above figure receives ORTS message from intended sender when sender's NAV timer is zero and an idle channel is sensed for a DIFS timeperiod. On receiving it the non forwarding candidates suppress their timers and the forwarding candidates set their CTS response timer ON andon expiry of it sends CTS response to the sender.The sender collects CTS responses using dynamic collection window and chooses the candidate node based on DWSIGF-R and DWSIGF-P forwarding strategy.
1.DWSIGF-R:-This strategy selects the node randomly which has positive IDTD(Increasing distance towards destination)value which shows the nodes progress towards destination.
2.DWSIGF-P:-It selects the node with highest IDTD value and uses greedy forwarding approach.

The sender send the data to the node after selection using DCF 802.11 semantics 802.11(ORTS=>CTS=>DATS=>ACK).The use of IDTD parameter has resulted in simplification of spatio-temporal predictions.
The Advantages of this protocol are:-
Minimal selection of malicious nodes by using dynamic collection period.
Utilization of IDTD parameter which has resulted in simplification of spatio temporal predictions.
The Disadvantages of this protocol are:-
It suffers from substantial packet losses by malicious nodes by considering distance parameter only.

*2.5. Fuzzy based geographic forwarding protocol(fugef)*
FUGEF is implemented to select a forwarding candidate node which eliminates substantial packet losses in network and provide better securityin network. It selects the node based on three parameters:-Remaining energy,connectivity cost and progressive distance and FLS.

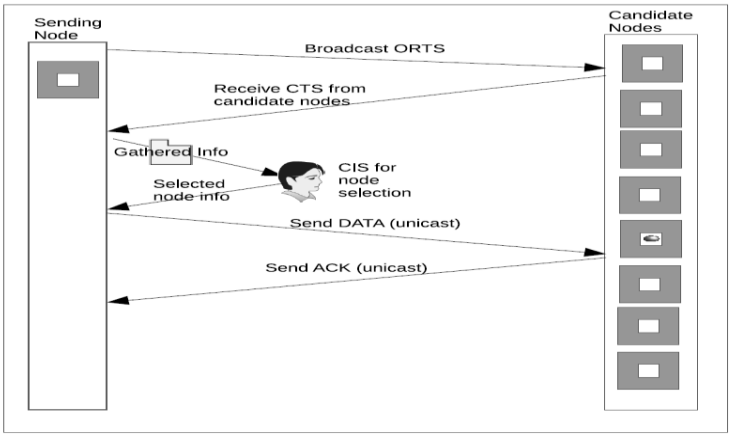

Figure 5.1:-FORWARDING PROCESS

As shown in above figure the sender collects the individual CTS response which contain location and remaining energy by using pseudorandom collection window period which has 2 intervals and is used to collect at one CTS response after receiving the ORTS message by the candidate nodes. The sender then using the location information calculates progressive distance and connectivity cost.The computed values along with remaining energy are send as inputs to FLS which computes on CIS(computational intelligence system) that is capable of enabling intelligent behaviour in complex and unstable environments.
The FLS is used to select a node which has a highest chance value. The FLS system consists of four main components:-

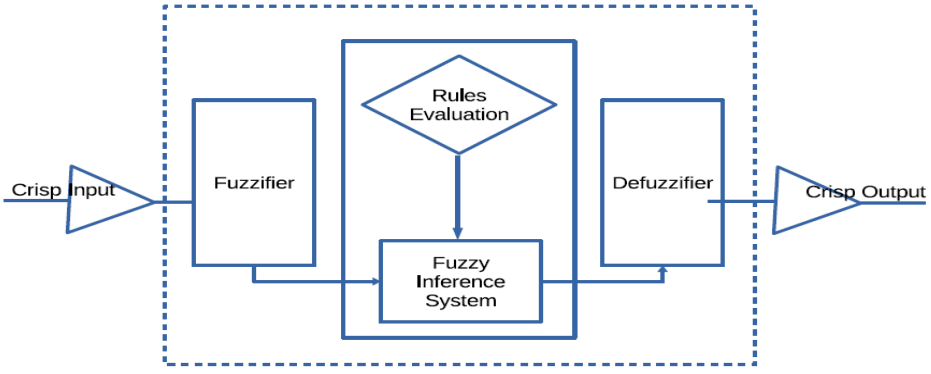

Figure 5.2:-FUZZY LOGIC SYSTEM

Fuzzifier:-It converts the input values into suitable linguistic values by Mapping each value to a universal set.
Fuzzy inference system(FIS) and rule evaluation:-FIS and rules evaluation work together to obtain a Fuzzy output set by applying IF-THEN rules to membership values

Defuzzifier:-It is the process of conversion of fuzzy output sets back to crisp outputs.

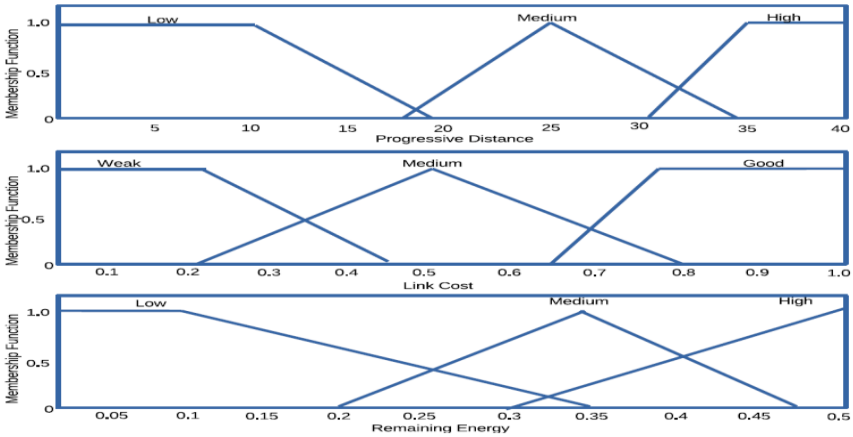


Figure 5.3:-FUZZY INPUT MEMBERSHIP MAPPING

The node with highest chance value is selected as appropriate candidate node as mentioned in figure 5.3 and the data is forwarded and the acknowledgement of reception of data is send from the forwarding candidate node.
The Advantages of this protocol are:-
The FUGEF utilizes a new form of dynamism and introduces three selection parameters: remaining energy, connectivity cost, and progressive distance, as well as a Fuzzy Logic System (FLS) for node selection.
Low energy consumption.
Less end-to-end delay.
The Disadvantages of this protocol are:-
Low packet delivery ratio.
Spatio temporal predictions are not possible.

Comparision Of Different Cross Layer Routing Protocols

| ROUTING PROTOCOL | METHOD | LIMITATION |
|---|---|---|
| Energy-Efficient Beaconless Geographic Routing in Wireless Sensor Networks | It uses the functionalities of both MAC and Physical layer and guaranteed loop free delivery using Greedy Forwarding strategy | It suffers from energy insufficiency problem |
| A MAC/routingcross-layer approach to geographic forwarding in wireless sensor networks | It utilises the functionalities of both MAC and Routing layer and forwards the data by increasing transmission power levels | End to End delay is increased due to number of hops travelled by the packets. |
| A family of configurable,secure routing protocols for wireless sensor networks. | It gives rise to resource bound security solutions which chooses next hop dynamically in fixed window period.It comprises of three protocols :-SIGF-0,SIGF-1,SIGF-2 | Greater cost in order to implement cryptographic mechanisms. |
| Dynamic windowsecured implicit geographic forwarding routing for wireless sensornetwork | It utilises the functionalities of MAC and network layer and implements handshake mechanism for node to node transmission. | It suffers substantial packet loses due to consideration of only one distance parameter |
| FuzzyBased Geographic Forwarding routing protocol | It utilises the functionalities of physical, MAC and Routing layer and for node selection it considers remaining energy, distance, cost as parameters. | Low packet delivery ratio and spatio temporal predictions are not possible. |

## III. CONCLUSION

Cross layer routing protocols enhances the security and the performance of the system has been explained in this paper.The energy efficiency is achieved by node selection by considering some parameters and accomplished using methods.This paper shows the merits and demerits of different routing protocols discussed.In future works, routing protocols are implemented to overcome this limitations such as lifetime,packet delivery ratio,better efficiency during attacks which will increase the performance of the system.

## IV. REFERENCES


[1] F. Akyildiz, M. C. Vuran, and O. B. Akan, ``A cross-layer protocol forwireless sensor networks," in Proc. IEEE 40th Annu. Conf. Inf. Sci. Syst.,Mar. 2006, pp. 1102_1107.

[2] H. Zhang and H. Shen, ``Energy-efficient beaconless geographic routingin wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 21,no. 6, pp. 881_896, Jun. 2010.

[3] L. Galluccio, A. Leonardi, G. Morabito, and S. Palazzo, ``A MAC/routingcross-layer approach to geographic forwarding in wireless sensor networks,"Ad Hoc Netw., vol. 5, no. 6, pp. 872_884, 2007.

[4] 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.

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

[6] Z. M. Hanapi and M. Ismail, ``Impact of blackhole and Sybil attacks ondynamic windows secured implicit geographic forwarding routing protocol,"IET Inf. Secur., vol. 8, no. 2, pp. 80_87, Mar. 2014.

[7] 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.


## V. BIBILIOGRAPHY


K.Anusha Pursuing M.Tech in the department of WMC,G.Narayanamma Institute Of Technology and Sciences,under JNTU H,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.