ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Wireless Sensor Networks: Routing Protocols on Challenging and Security Issues

P Chitralingappa[1], Dr. V Raghunatha Reddy[2]

Research Scholar, Dept. of CST, SKU, Ananthapuramu, India[1]

Asst. Professor, Dept. of CST, SKU, Ananthapuramu, India[2]

ABSTRACT: Wireless Sensor Network [1] represents to a group of spatially scattered and dedicated sensors for recording and monitoring the physical conditions of the particular environment and configuring the collective data at a central location. In WSN, nodes are generally battery powered devices. These nodes have limited amount of initial energy that are consumed at different rates depending on the power level. The Routing Protocols of Wireless Sensor Networks depends on Design and Challenging issues are elaborated. Protocol operation based protocols, Network Structure based and Route Discovery based protocols are presented under the criteria of Classification of Routing Protocols in WSN. The lifespan of the network is defined as the time until the first node fails. In this paper we talk about three kinds of routing protocols those are TORA, HEED, INSENS and its energy efficiency, scalability, security and vice versa and its pros and cons.

KEYWORDS: WSN, Design and Challenging Issues; Classification of Routing Protocols; Proposed Routing Protocols: TORA; HEED; INSENS.

I. INTRODUCTION

Wireless sensor network is a network which consists of spatially independent dynamic and distributed devices those using sensors can monitor physical and environmental aspects and vice versa. WSN's can build on several nodes, which would have thousands of nodes being interconnected among them to scatter a huge network to collect the big data regarding, such environment. A sensor node typically consists of several parts i.e. radio transceiver with an internal antenna, a microcontroller used to interface with the sensors and an energy source usually a battery.

The sensor node could be either smaller one or larger one in terms of size. WSN must have base station (gateways/sink) which communicates its neighbour nodes according to the application (topology/algorithms) based. These large number of nodes wirelessly communicate with each other and to the base station directly or indirectly, and have capabilities to sense the data from their surroundings, store the data , pass their sensed data to their neighbor sensor nodes or to the base station and perform some computations on the sensed data. There are wide applications of WSN include: physical security, air traffic control, environment monitoring, healthcare monitoring, military and so on. Sensor networks may be quite different from various applications.

Due to recent technological progress and availability of low cost sensors created wireless sensor networks. Sensors are little devices that sense physical quantities and convert them in to electrical signals. A WSN consists of many sensor nodes that can sense data and communicate among them or to the sink (external base station). It mainly consists of 4 components:

A. Sensor Unit

B. Transceiver

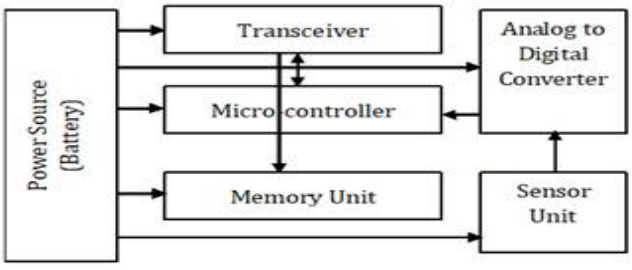


Fig. 1: Sensor node architecture

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

C. Power source (Battery)

D. Micro-controller

E. Memory Unit

F. ADC (Analog-to-Digital Converter)

One of the most important drawbacks of WSN is that sensor nodes battery powered and deployed in tough environment so it is not easy to recharge or replace the batteries all the times the node fails or dead.

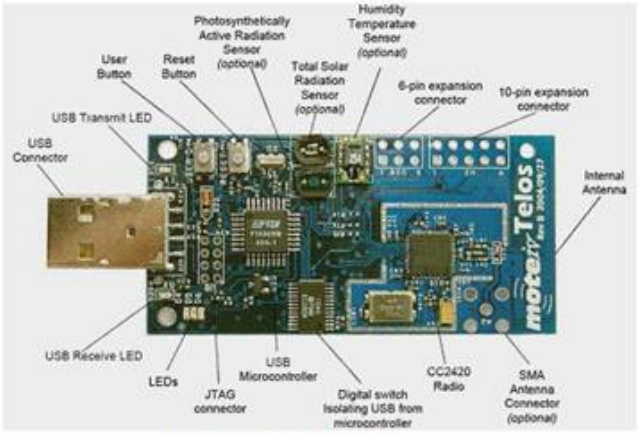


Fig. 2: Sensor mote

Fig. 3: Sensor mote

II. DESIGN ISSUES OF ROUTING PROTOCOLS

Initially WSNs are mainly motivated by military applications. Later on the civilian application domain of wireless sensor networks have been considered, such as environmental and species monitoring, production and healthcare, smart home etc. These WSNs may consist of heterogeneous and mobile sensor nodes, the network topology may be as simple as a star topology; the scale and density of a network varies depending on the application. To meet this general trend towards diversification, the following important design issues of the sensor network have to be considered [4], [5].

Fault Tolerance

Due to lack of power, some sensor nodes may fail or be blocked; it leads to physical damage or environmental interference. The failure of sensor nodes should not affect the entire sensor network. Fault tolerance is the ability to prolong sensor network functionalities without any interruption due to sensor node failures.

Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds, thousands or more and according to routing plans routing schemes must be scalable enough to respond to events.

Production Costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node depends on the overall cost of the networks and so try to make sensor cost to diminish against application.

Operating Environment

We can use sensor network at large machinery, bottom of an ocean, biologically or chemically field, battle field, attached to fast moving things, in forest area for habitat monitoring etc.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Power Consumption

Actually the wireless radio's transmission power is quite proportional to distance squared due to the presence of obstacles because multi-hop routing consumes less energy as compared to the direct communication. The multi-hop routing offers significant overhead for the MAC and topology management thereby. In some cases direct routing works enough if all the nodes very nearer by the base station, depends on application that too. But any way nodes span fairly depends on its battery power.

Data Delivery Models

Data delivery models represent how to deliver collected data from every node, depending on the application of the sensor network to the sink. It can be categorised as Continuous, Event driven, Query-driven and Hybrid. In the continuous data delivery model, each sensor periodically sends data. In event-driven data delivery models, the data sends when an event occurs. In query driven models, the data sends when query is generated by the sink. Rest of the sensor networks apply a hybrid model using a combination of continuous, event-driven and query driven data delivery.

Data Aggregation/Fusion

Since sensor nodes might generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the combination of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average. As computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation. This technique has been used to achieve energy efficiency and traffic optimization in a number of routing protocols.

Quality of Service (QoS)

The quality of service means the quality service required by the application, it could be the length of life time, the data reliable, energy efficiency, and location-awareness, collaborative-processing. These factors will affect the selection of routing protocols for a particular application. In some applications (e.g. some military applications) the data should be delivered within a certain period of time from the moment it is sensed.

Data Latency and Overhead

These are considered as the important factors that influence routing protocol design. Data latency, which represents a stipulated data to be transferred from one point to another point in time. Overhead is it's the mingle of excess memory, computation time, bandwidth and rest of the sources which requires to accomplish a particular task.

Node Deployment

Node deployment can purely dependent on its application basis. It rules the performance of the routing protocol. The node deployment can be determined in two ways which are either deterministic or self-organizing. In case of deterministic situations, the sensors are manually take placed and data can be routed through pre-determined paths. In other terms of self organizing systems, the sensor nodes would be spread randomly creating an infrastructure in an Ad-hoc manner. In Ad-hoc systems, the position of the sink node plays crucial role in terms of energy efficiency and performance.

III.CHALLENGING ISSUES OF ROUTING PROTOCOLS IN WSN

Routing in WSN consist various challenging issues [6], [7] such as power supply, Network lifetime, scalability, energy efficient, fault tolerance, processing capability, robust, transmission bandwidth, global address, load balancing, frequent topology changes, data processing, data aggregation, data redundancy, etc. Clustering routing protocols try to overcome a few of these challenges some of them are listed below:

Network Lifetime:

Clustering routing protocol helps in energy-efficient routing thus the overall network lifetime is increased.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Energy Efficient:

Data aggregation at CH reduces data transmission and thus saves energy. Whereas inter-cluster communication helps in less energy consumption.

Fault Tolerance:

In WSN nodes are deployed in harsh environment and thus nodes are usually exposed to risk of malfunction and damage. Tolerating the failure of nodes or CH is necessary in such conditions. Rotating the role of CH among the nodes in the cluster is also a solution for CH failure.

Robust:

WSN like wired network doesn't have any fixed topology thus addition of new node, node mobility, node failure, etc. has to be maintained by the individual cluster not by the entire network. CHs rotate among the entire sensors node to avoid single point of failure.

Load Balancing:

The distribution of nodes in the cluster makes load balancing and the data fusion happens at the cluster head before inter-cluster transmission. CH will take the responsibility for maintaining load balance within the cluster.

Data Processing:

Data redundancy can be reduced by aggregating the packets send by various nodes in the cluster to the CH. Thus various redundant data can be removed during this process.

IV. CLASSIFICATION OF ROUTING PROTOCOLS IN WSN

Routing protocols in wireless sensor network might differ depending on the application (Protocol Operation-based), network architecture (Network-Structure-based) and route discovery based. These routing protocols [8], [9], [10], [11] as shown in Fig. 4.

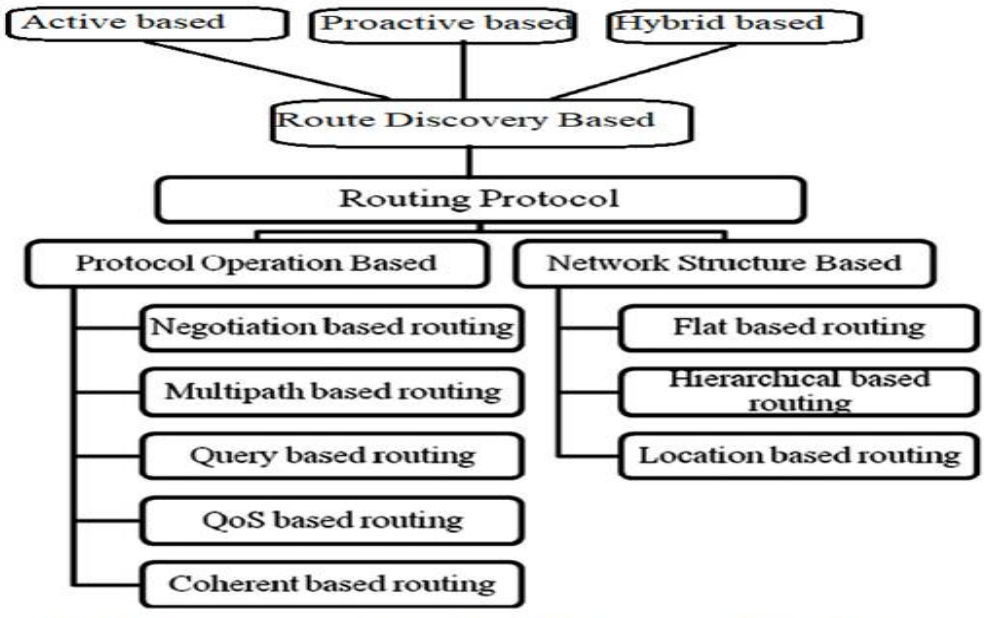


Fig. 4 : Classification of Routing Protocols in WSN

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Protocol operation based protocols:

Negotiation Based Routing:

Negotiation based routing protocols are used to eliminate redundant data transmissions. Negotiation based routing protocols are, Sensor Protocols for Information via Negotiation (SPIN), SPAN, Virtual Grid Architecture routing (VGA) and Sequential Assignment Routing (SAR) protocol.

Multipath Based Routing:

Multi-paths are used rather than single path in order to enhance the network performance. These protocols offer fault tolerance by having at least one alternate path from source to sink. Then always some of the paths are kept alive to sending periodic messages. Directed Diffusion is a good for robust multipath routing and delivery.

Query Based Routing:

In these protocols, the destination nodes propagate a query for data (sensing task or interest) from a node through the network. The node containing this data sends it back to the node that has initiated the query. Examples are: Directed Diffusion, Sensor Protocols for Information via Negotiation (SPIN), Rumor Routing, Gradient-Based Routing (GBR).

QoS Based Routing:

In these protocols, the network has to balance between energy consumption and data quality. The network has to satisfy certain QoS metrics (delay, energy, bandwidth, etc.) when delivering data to the BS. Examples are: Sequential Assignment Routing (SAR) and SPEED are QoS based routing protocols.

Coherent Based Routing:

In these protocols, the entity of local data processing on the nodes distinguish between coherent (minimum processing) and non-coherent (full processing) routing protocols.

Network structure based protocol:

Flat Based Routing:

In these protocols, each node plays the same role and sensor nodes collaborate to perform the sensing task. Examples are: Sensor Protocols for Information via Negotiation (SPIN), Directed Diffusion, Rumor Routing, Gradient-Based Routing (GBR), Minimum Cost Forwarding Algorithm (MCFA), Constrained Anisotropic Diffusion Routing (CADR), ACtive Query forwarding In sensoR nEtworks (ACQUIRE).

Hierarchical (Cluster-based) Routing:

In hierarchical routing protocols, higher-energy based nodes are being functionalized towards its process and send the data, where as low-energy based nodes being sensed the assigned target. And making of formation of clusters and allocates a prominent tasks to cluster heads to enhance the entire system's energy efficiency, life span and scalability. Hierarchical routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink node. Some of the hierarchical routing protocols are: Low Energy Adaptive Clustering Hierarchy (LEACH), Threshold sensitive Energy Efficient sensor Network (TEEN), AdaPtive Threshold sensitive Energy Efficient sensor Network Protocol (APTEEN), Power Efficient Gathering in Sensor Information Systems (PEGASIS), Hybrid Energy Efficient Distributed Protocol (HEED), Stable Election Protocol (SEP).

Location Based Routing:

In location based routing protocols, sensor nodes will be addressed in terms of their locations. The distance among neighbouring nodes can be speculated on the basis of incoming signal strengths. The neighbour's nodes relative coordinates can be attained by exchanging theirs information among them or by coordinating with a satellite using GPS. Suppose To save the energy of nodes on the location-based schemes better they would go to sleep if there is no sensing

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

event. Examples are: Geographic Adaptive Fidelity (GAF), Geographic and Energy Aware Routing (GEAR), SPAN, Greedy Other Adaptive Face Routing (GOAFR).

Route Discovery based protocols:

Active based

These protocols are also called as On-Demand routing protocols as in these kind of routing protocols node searches for route on-demand i.e., whenever a node wants to send data it searches route for destination node and establishes the connection. Examples are AODV, LMR, TORA, DSR, and LQSR.

Proactive based

These protocols are also called as table driven routing protocols since they maintain the routing information even before requiring of this information. Each and every node maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. The protocols under this category maintain different number of tables. Furthermore, they are not suitable for large networks, as they need to maintain entries for each node in the routing table. Examples are DSDV, OLSR, CGSR, WRP, TBRPF and QDRP.

Hybrid based

The Combination of both reactive and proactive is called hybrid routing protocol. Examples are ZPR, BGP and EIGPR.

TEMPORALLY ORDERED ROUTING ALGORITHM (TORA)

Temporally-Ordered Routing Algorithm was invented by Vincent Park and Scott Corson from the University of Maryland. The TORA is an adaptive, distributed, loop-free, on-demand routing protocol [12], [13],[14] for multi-hop networks which has minimum overhead against topological changes. The main intention of the TORA is to limit control message propagation in the highly dynamic mobile computing environment. Each node has to explicitly initiate a Query when it needs to send the data to a particular destination. TORA algorithm is based on the link reversal concept. It makes use of Direct Acyclic Graph (DAG) for defining upstream and downstream routes. With more number of nodes in network, the TORA protocol provides better route aid. It is relatively complicated protocol but supports control messages in case of link failures. In contrast to other protocols TORA will be able to recover point of failure directly. It exhibits high overhead for small networks. TORA minimizes the communication overhead and consists of 'link reversal' of the Directed Acyclic Graph (DAG). TORA attempts to build what is known as a Directed Acyclic Graph (DAG) which routed at the destination. TORA assigns directions [15] ("upstream" or "downstream") to the links between nodes to forward datagram's to the destination based on the relative values of a metric associated with each router. The importance of these heights in TORA routing protocol are that a node in network may only forward data packets downstream instead of upstream. TORA essentially performs three tasks. It has 3 basic route functions: establishment, maintenance, and erasing. In TORA routing protocol, each node will have a capability, contains a structure of network that describing node height and status of all connected links. The node/router can specifically define its metrics towards its height. The significance of the "height" field is that the node will only forward datagram's downstream. Temporarily ordered routing algorithm is designed to reduce communication overhead against to local topological changes in ad hoc network. Another smart function of TORA routing protocol is the localization of control packets to a small region (set of nodes) near the occurrence of a topological changes due to route break. Each and every node in the sensor network should maintain local information and topology about adjacent (one hop) nodes. TORA works based on link reversal algorithm. Node links with an unknown or undefined height are considered un-directed and cannot be used for forwarding.

- ✓ Creation of a route from a source to destination (Route Creation).
- ✓ Maintenance of the route (Route Maintenance).
- ✓ Erasure of the route when the route is no longer valid (Route Erasure).

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

TORA Attributes:

- ✓ On-Demand source initiated routing.
- ✓ Nodes only maintenance the information about the adjacent nodes.
- ✓ Provides multiple routes.
- ✓ Creates loop-free routes.
- ✓ Handles partitions by erasing route.

Node height in TORA:

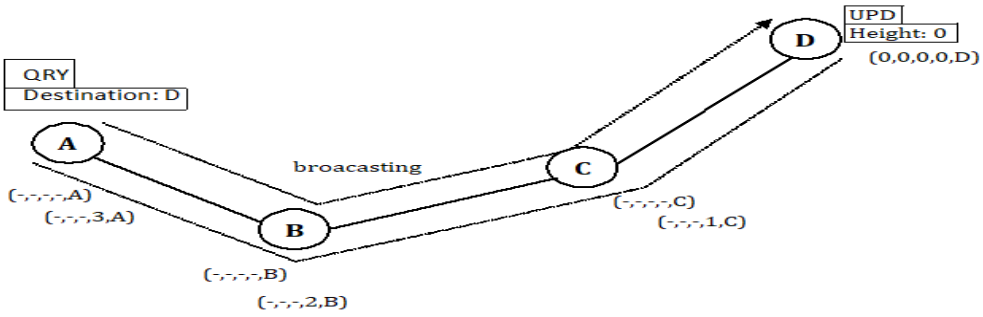
In TORA the height assigned to every node is represented by Quintuple.

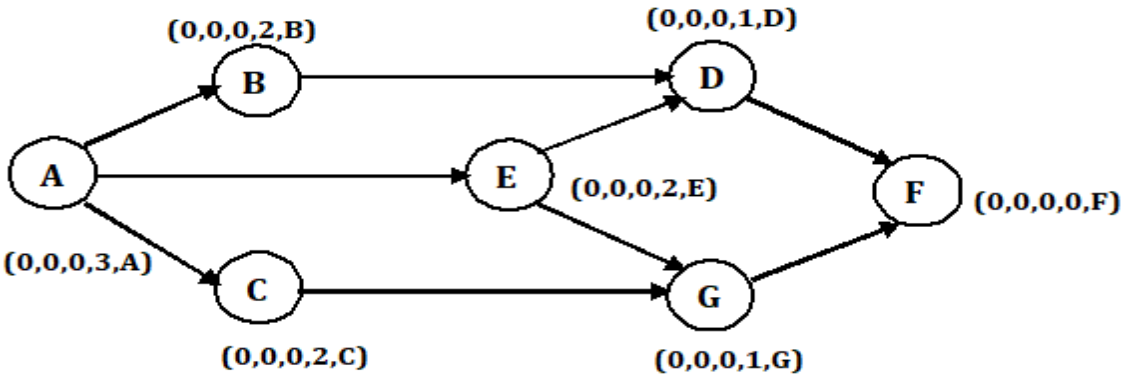
$$Hi = (\tau, Oid, r, \delta, i)$$

The first three fields represent the reference level. Where,
τ= a time tag indicating the time of link failure.
Oid= Originator id (unique id of the node that defined the new reference level).
r= reflection list
δ= integer used to order nodes with respect to unique reference level.
i= unique identification of the nodes.

Each node other than the destination maintains its height with respect to the destination. Initially the height of each node is set to null i.e., Hi = (-,-,-,-,i) and the height of the destination is always 0 i.e., Hi = (0,0,0,0,dest)

How TORA works:





ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

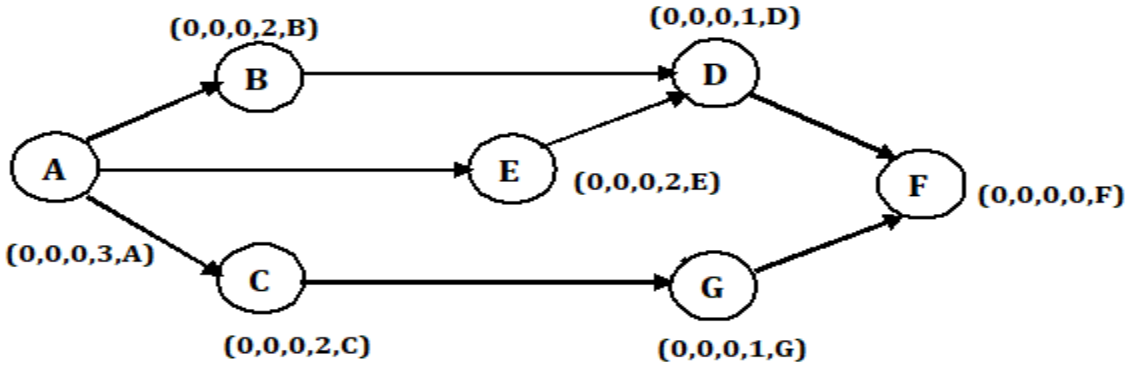
Vol. 7, Issue 9, September 2018

Node can send data to only neighbours having less height i.e. A to F and every node will have a downstream link.

TORA Route maintenance:

Case 1:

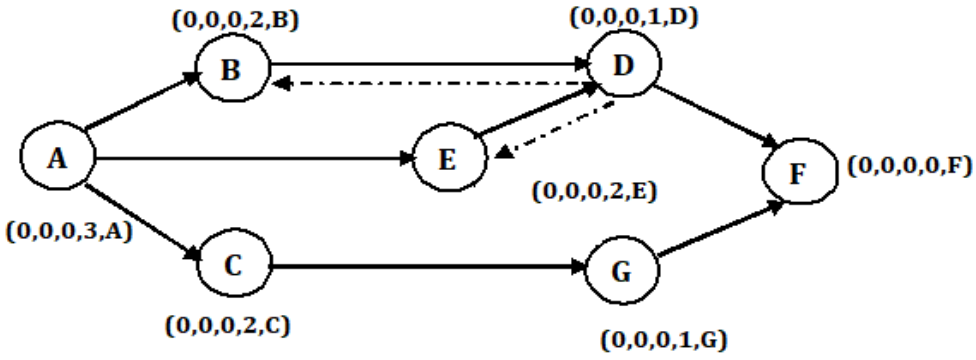
Link is broken and every node in network has a downstream link, no action is required. If nodes are having neighbours with less height no need to update route. Here link between E and G is failed.



Case 2: Generate

Link is broken and node in network doesn't have any downstream link, create a new reference level and send it to neighbours with the help of (Old-ref+1, node-id, 0, 0, node-id). Here, link between D and F is failed.

--



According to above tuple reference,
Old-ref+1=0+1=1
Node-id =D
=0
=0
Node-id =D

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

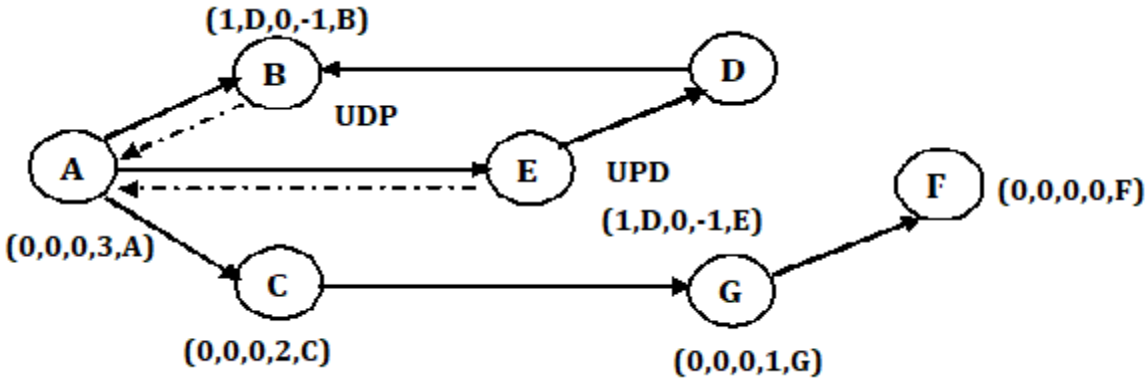
Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

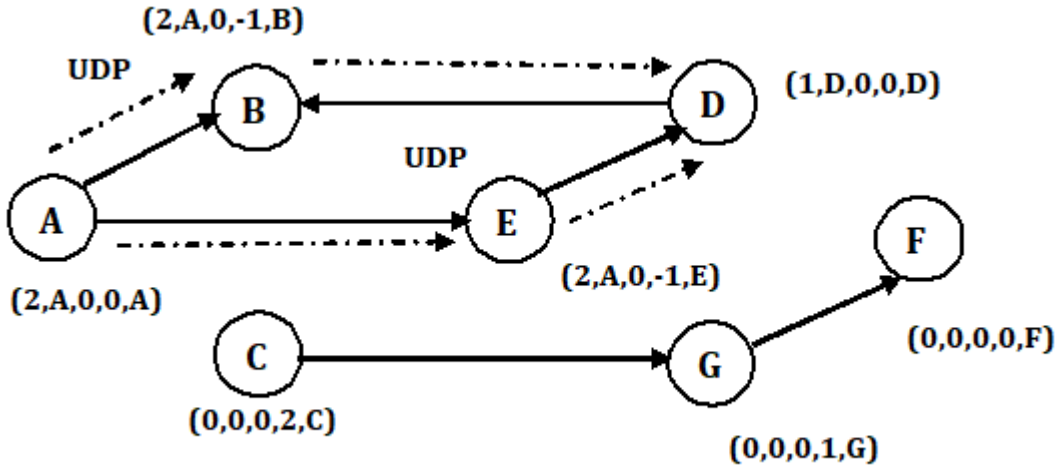
Node B and E receive UPD packet with height information. Height of D is greater than their current height so link direction will be changed.

Case 3: Propagate

Node in network doesn't have any downstream link because of route-maintenance process. Compare neighbours reference level, if it's not same then take highest reference level.
(<reference of highest node>, that node order-1, <node-id>)



Assume link between A and C is failed.



ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

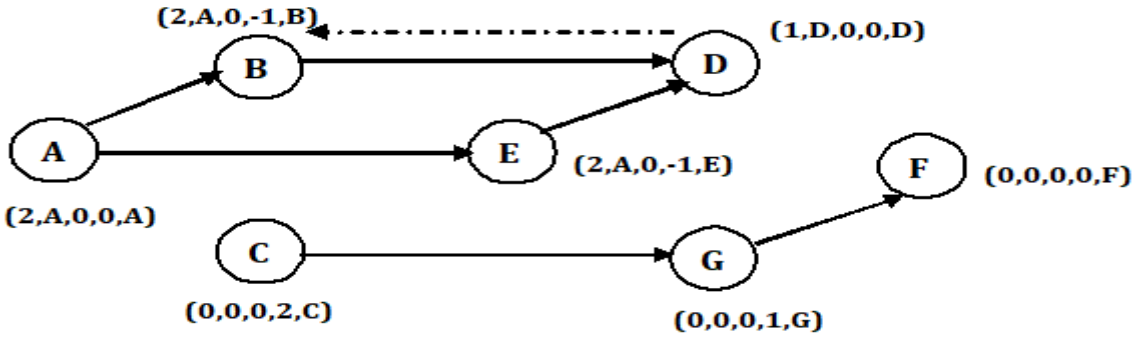
Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Direction will be pointed to neighbours because they are having less reference level.

Case 4: Reflect

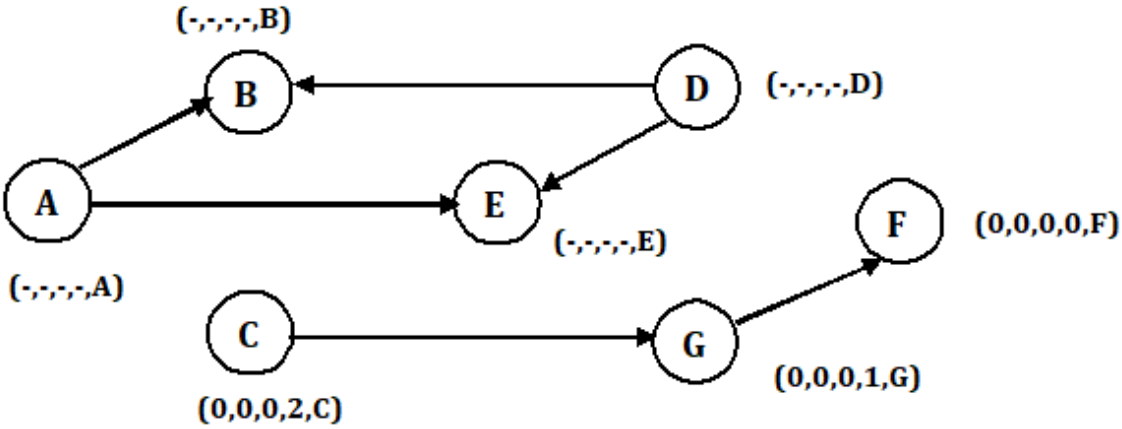
Node in network doesn't have any downstream link because of route-maintenance process. Compare neighbours reference level, if it's same and r=0 then taken reference level as it is and change reflection bit to 1. (, , 1, node-id)



All neighbours of D having same reference with r=0 so D will reflect it back.

Case 5: Detect

Node in network doesn't have any downstream link because of route-maintenance process. Compare neighbours reference level, if its same and r=1 set height to null and broadcast clear packet to neighbours.



Node A is having two neighbours with same reference and with r=1 so A will clear the heights.

Advantages of TORA:

- ✓ It provides loop free routes to the destination
- ✓ It emphasis on multipath routing

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

- ✓ It performs best for dense networks
- ✓ The possibility of congestion is reduced
- ✓ It is designed in such a way that is reduces routing overhead in the network.
- ✓ It maintains multiple routes to the destination
- ✓ It has the capability of removing invalid routes

Disadvantages of TORA:

- ✓ TORA is dependent on synchronised clocks for communication in the network.
- ✓ It sometimes creates invalid temporary routes
- ✓ It is dependent on lower layers for some of the functionalities
- ✓ With increase in mobility of nodes, the performance of TORA degrades eventually.
- ✓ When the amount of traffic increases in the network the protocol may not work efficiently

Hybrid Energy Efficient Distributed clustering Protocol (HEED)

Hybrid Energy Efficient Distributed clustering Protocol was proposed by O. Younis and S. Fahmy in 2004. Hybrid Energy Efficient Distributed protocol was designed to select different cluster heads. It is a multi-hop WSN clustering algorithm which brings an energy-efficient clustering routing with explicit consideration of energy. It is a distributed clustering algorithm, developed to over some of the drawbacks in LEACH.

In HEED [16], each cluster one node selected as a cluster head, its responsibility is coordinating with other cluster heads. To increase energy efficiency and prolong network lifetime intra cluster communication is used and it communicates with other cluster heads. In Hybrid Energy Efficient Distributed clustering algorithm, each node is mapped to exactly one cluster. The node can directly communicate with its cluster head (via a single hop). Based on its local information each node independently makes its decisions. Clustering terminates within a fixed number of iterations. Each and every cluster consists of exactly one cluster head and ordinary node.

In HEED, on the basis of residual energy the node will be elected as a cluster head which is the main factor and supposed to enhance the energy efficiency and still prolongs network lifespan, we must consider intra-cluster communication / coordination cost as a secondary clustering factor. If any node would have high residual energy and low cost, it would be elected as a cluster head at consecutive clustering intervals. Hence the lifespan of the network would be more as compared to energy efficient protocols for wireless sensor networks [17].

Basically in the HEED the distribution of energy consumption [18] makes the extension of the life span of all the nodes embedded in the network and tries to balance the stability of its neighbor set as well. Neighbours will update the information about their neighbor sets in the construction of multi-hop networks by sending and receiving messages periodically. Because it uses communication cost as a secondary factor to make improved the lifespan of wireless sensor network, HEED built-form well as compared to other protocols in the network. Actually it is fairly variant from the LEACH, in the matter of CH election, HEED will not elect nodes as CHs by randomly. The cluster construction is based on the hybrid mixture of two factors. One factor holds the node's residual energy, and the other one is intra-cluster communication cost. In HEED, elected CHs would have high average residual energy as compared to other protocols.

- ✓ To overcome the disadvantages of LEACH, PEGASIS, TEEN. HEED is introduced.
- ✓ Some research papers shows that HEED consumes low battery in wireless sensor networks

The enhancement is done in the CH selection method. HEED, selects CH on the basis of energy as well as communication cost. In HEED, each node is mapped to exactly one cluster. It is divided into three phases:

- ✓ Initialization Phase: Each sensor node sets the probability Cprob of

$$CH_{prob} = C_{prob} \cdot \frac{E_{residual}}{E_{max}}$$

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

becoming CH follows:

Where Cprob is the initial percentage of CH required in the network, Eresidual is the current energy of the node and Emax is the maximum energy of the fully charged battery.

- ✓ Repetition Phase: This is an iterative phase in which each node repeats the same process until it find a CH to which it can transmit with least cost. If any node finds no such CH, the elects itself to be a CH and sends the announcement message to its neighbours. Initially sensor node become tentative CH, it changes its status later if it finds a lower cost CH. The sensor node becomes permanent CH if its CHprob has reached.
- ✓ Finalization Phase: In this phase nodes either picks the least cost CH or itself becomes a CH. Though it is an improvement over LEACH still it has some disadvantages like more CH are generated than expected and it is not aware of heterogeneity.

Features of HEED

- ✓ To increase energy efficiency and prolong network lifetime we can consider intra cluster communication cost as a secondary clustering parameter.
- ✓ Intra clustering communication involves communicating with other cluster heads
- ✓ Cost is a function of cluster properties and whether power levels are permissible for transmission within a cluster.

Advantages of HEED

- ✓ HEED distribution of energy extends the lifetime of the nodes within the network thus stabilizing the neighbouring node.
- ✓ Does not require special node capabilities, such as location-awareness
- ✓ Does not make assumptions about node distribution
- ✓ Operates correctly even when nodes are not synchronized.
- ✓ Creates well distributed clusters Requires only local communication
- ✓ Reduces energy load
- ✓ Extends network lifetime
- ✓ The advantages of HEED are that nodes only require local (neighbourhood) information to form the clusters
- ✓ the algorithm terminates in O(1) iterations
- ✓ The algorithm guarantees that every sensor is part of just one cluster, and the cluster heads are well distributed.

Disadvantages of HEED

The random selection of the cluster heads may cause higher communication overhead for:

- ✓ the ordinary member nodes in communicating with their corresponding cluster head
- ✓ cluster heads in establishing the communication among them, or
- ✓ Between a cluster head and a base station.
  - The periodic cluster head rotation or election needs extra energy to rebuild clusters.
  - Communication
- ✓ Bandwidth is limited and must be shared among all the nodes in the sensor network
- ✓ Spatial reuse essential
- ✓ Efficient local use of bandwidth needed

INSENS (INtrusion-tolerant routing protocol for wireless SEnsor NetworkS):

When we talking about secure routing protocol for WSN, We suggest the INSENS [19], [20] routing protocol. WSN are drastically moving and emerging section in the mobile computing area. And more exactly our goal is to

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

design of an intrusion-tolerant secure WSN's that have a strengthen property that a single compromised node can only disrupt a localized portion of the network, but it would not fetch the whole network.

The design of objective for the intrusion-tolerant for secure WSN's that provide the protection against two classes of attacks that can bring up the whole network of sensors. The first one is DoS (Denial of Service) type attacks that makes flow the data packets to the whole network and second one is Routing attacks that makes an error based control packets which contained false routing data across the network.

Basically an individual node would not allow broadcasting to the whole network. Only the gateway node (sink) would get such ability to broadcast, so that individual nodes will not spoof the gateway node and flood the network thereby. But for unicast packets, nodes firstly communicate through the base station, allowing the gateway node to act as packet filter to retain DOS through a single node.

Actually INSENS is similarly resilient to distributed DOS as multiple nodes won't broadcast to the whole network. Secondly to prevent the advertised of false routing data, the control of routing information must be authenticated. And a key effect of this approach is that the gateway node always receives the correct and partial knowledge of topology. If this base station may not receive all of the topology based discovery data due to localized intrusions, the picture of the network that the gateway node is able to constructs is nevertheless connect. The third addressing resourcing constraints, INSENS follow two design decisions: symmetric key cryptography which is based for confidentiality and authentication network base station and resource based constrainable sensor nodes and dissemination of routing tables. Fourth to address the notion of compromised nodes redundant multipath routing is built into INSENS to achieve secure routing.

An INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS), builds forwarding tables at each node to make facilitated communication / coordination among sensor nodes and a sink. It makes lessen the computation, communication, storage, and bandwidth due to same kind of functionalities would be held at base station. INSENS won't rely on to detect intrusions, but rather bears intrusions by diverting the culpable nodes. The paramount factor at INSENS, actually the culprit node can handle some of the nodes in its vicinity, but it can't able to manage the entire network towards being bugged and it's not easy for it.

The design and implementation of secure WSNs must simultaneously address several difficult research challenges. First, wireless communication among the sensor nodes increases the vulnerability of the network to eavesdropping, unauthorized access, spoofing, replay and denial-of-service (DOS) attacks. Second, the sensor nodes themselves are highly resource-constrained in terms of limited memory, CPU, communication bandwidth, and especially battery life. These resource constraints limit the degree of encryption, decryption, and authentication that can be implemented on individual sensor nodes, and call into question the suitability of traditional security mechanisms such as compute-intensive public-key cryptography for such resource constrained sensor nodes. Third, WSN facing the risk of physical security due to individual sensor nodes will be black eyed by the intruders can devastate the devices by hacking since Sensor nodes will be deployed manually / physically at the field. As mainly the intruder can try to hack /attack on a node, suppose it compromises to surrender, through it the intruder can inject false / flaw messages / routing information can be sent to its neighbour nodes which are at its proximity and try to make the services break down.

Intrusion-tolerant routing protocol for wireless Sensor NetworkS (INSENS) is proposed for the prevention of these network layer attacks [21] in the sensor network. INSENS blocks the network layer attacks from Sybil or wormhole. INSENS constructs secure and efficient tree-structured routing for WSNs, and is tailored for the asymmetric architecture and resource constraints of WSNs. A key objective of INSENS is to localize the damage caused by an intruder who has compromised deployed sensor nodes. Such an intruder could inject, modify, or block data packets, and in the worst case could bring down the entire sensor network, e.g. by flooding malicious packets. INSENS is hence portrayed to defend and sustain intrusions and makes intruder be in its limitations without in doing of knave activities.

The key principles in the design of INSENS are as follows:

- Intrusion tolerance

1. Limited broadcast using one way hash chains (OHCs): INSENS permits only base stations to initiate flooding of the network, e.g. to set up routing information. Each base station stamps each of its broadcast packets with a one way hash chain number, which we term a one way sequence number. Intruders will be unable to guess the

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

next number in the OHC and will thus be restricted in their ability to flood the network, thereby enhancing intrusion tolerance.

2. Multipath routing: INSENS employs redundant multipath routing to enhance intrusion tolerance. To the extent possible, multiple disjoint paths are set up from each sensor node, so that even if an intruder compromises a node or a path, alternate forwarding paths exist. The desire for intrusion tolerance must be balanced against the energy cost of multipath routing. INSENS can be configured to fall back to a secure single-path routing mechanism.
3. Limited routing updates: Only the base station is allowed to update a node's data routing table. This is accomplished by assuming a secret pairwise key shared only between the base station and a sensor node. This inhibits many attacks directed towards routing information updates in sensor networks, e.g. the sinkhole attack.

❖ Adaptation to resource constraints

1. Symmetric key cryptography is chosen to implement confidentiality and authentication between the base station and each resource-constrained sensor node.
2. Complexity is pushed away from resource-poor sensor nodes and into the resource-rich base station, which is chosen as the central point for computation and dissemination of the routing tables.

❖ Novel mechanisms are introduced to address several specific attacks against sensor network routing. For example, lightweight bidirectional verification is applied to defend against the rushing attack. The nested message authentication code (MAC) is used as a countermeasure against the wormhole attack.

❖ To accommodate different sizes of sensor networks, a basic three-phase version of INSENS is presented for moderately-sized sensor networks with a single base station, while an enhanced single-phase version of INSENS is presented for large-sized sensor networks with many base stations. Multipath routing to multiple base stations also improves tolerance against base station failures or isolation of a single base station.

INSENS will protect against various attacks which are possible on non-secure routing protocols in sensor networks, e.g., the spoofed routing information attack, sinkhole attacks, selective forwarding, wormhole attack and Sybil attack. The prominent factor of an INSENS can even be endured in getting damaged by making injected, modified, spoofed, eradicated, or blocking packets.

Basic INSENS protocol

The basic INSENS protocol is divided into two parts: route discovery and data forwarding. Route discovery ascertains the topology of the sensor network and sets up appropriate forwarding tables at each node by exchanging control messages. It is performed in three phases.

✓ In the first phase (Route Request), the sink starts a limited flooding requiring for information about all the reachable nodes in the network. This mechanism makes nodes to meet their neighbours, as shown in Fig. 5(a).

✓ In the second phase (Route feedback), all the nodes send their local information / topology to the sink as a response to the previous request, message will be sent through the inverse path of the received message as shown in Fig. 5(b).

✓ In the third phase(Routing table propagation), the gate way will be main substance in the network can check its topology information, calculates the multipath forwarding tables for every sensor node, and forwards those tables to concern / respective nodes in a breadth-first manner using a routing update message. Those results in a multi-hop multipath data forwarding tree. Fig. 5(c) illustrates only the multipath routes constructed for one node, not for all nodes. The complete multipath tree will be a union of all multipath routes for single nodes. After this point, multi-hop data forwarding can commence.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

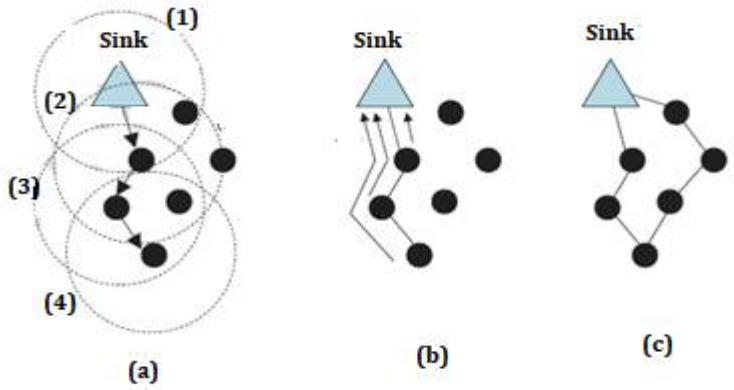


Fig. 5: Three Phases of Basic INSENS: (a) ROUTE REQUEST is flooded from sink. (b) ROUTE FEEDBACKS are unicast back to the sink from each sensor node, containing neighbourhood local / topology information. (c) ROUTING TABLE PROPAGATION is securely unicast to each node, in a breadth-first manner, establishing multi-path routing.

Enhanced INSENS protocol

The enhanced INSENS protocol incorporates several unique features and countermeasures to address the limitations of the basic INSENS protocol:

- ✓ bidirectional verification is used to defend against the rushing attack;
- ✓ multiple paths to multiple base stations is used to make INSENS more scalable for larger sensor networks
- ✓ A set of secure maintenance mechanisms are introduced to manage node joining and leaving in a network.

INSENS challenges:

Wireless communication is broadcast in nature, adversary can:

- ✓ Eavesdrop on packets as they cross the network
- ✓ Tamper with transmitted packet
- ✓ Inject packets to initiates DOS
- ✓ Sensor nodes over highly constrained in;
  1. Limited power / lifetime
  2. Low power micro sensors & actuators
  3. Slow embedded processors
  4. Limited memory
  5. Low bandwidth communications
- ✓ Distributed in the fields in-sites, lacking physical security.

V. CONCLUSION

In this paper, we have proposed and explored three protocols of WSN to assess its properties against its functionalities. The main intention of the TORA, is to limit control message propagation in the highly dynamic mobile computing environment. Each node has to explicitly initiate a query when it needs to send the data to a particular destination. In HEED, in each cluster one node may be selected as a cluster head, based on residual energy and to increase energy efficiency and prolong network lifespan. The third protocol INSENS will protect against various attacks which are possible on non-secure routing protocols in sensor networks, e.g., the spoofed routing information attack, sinkhole attacks, wormhole attack and Sybil attack. Presented that the Challenges of these three protocols meets

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

the efficiency of Wireless Sensor Netowrks. In future, analysation will takes place by implmenting the parameters of these 3 proposed protocols towards the best outcome of efficiency of WSN. The implementation of these proposed protocols is effected with the help of simulators.

REFERENCES

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankaraubramaniam, and Erdal Cayirci: A Survey on sensor networks, IEEE Communications Magazine (2002).
[2] Ajay Jangra et al. Wireless Sensor Network (WSN): Architectural Design issues and Challenges (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 3089-3094
[3] M.A. Matin and M.M. Islam, Overview of Wireless Sensor Network, September 6th 2012.
[4] Kay Romer, Friedemann Mattern: The Design Space of Wireless Sensor Networks, IEEE Wireless Communications, pp. 54-61 (December 2004).
[5] Rajashree.V.Biradar , V.C .Patil , Dr. S. R. Sawant , Dr. R. R. Mudholkar: CLASSIFICATION AND COMPARISON OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS on Special Issue on Ubiquitous Computing Security Systems, January 2010.
[6] S. Karthik, Dr. A. Ashok Kumar, Challenges of Wireless Sensor Networks and Issues associated with Time Synchronization, Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015.
[7] Sharma, S., Bansal, R. K., & Bansal, S. (2013). Issues and Challenges in Wireless Sensor Networks, International Conference on Machine Intelligence and Research Advancement, 2013.
[8] Ali Modirkhazeni, Norafida Ithnin, Othman Ibrahim, Empirical Study on Secure Routing Protocols in Wireless Sensor Networks, International Journal of Advancements in Computing Technology Volume 2, Number 5, December 2010.
[9] Hassan Echoukairi, Khalid Bourgba and Mohammed Ouzzif, A Survey on Flat Routing Protocols in Wireless Sensor Networks, September 2015.
[10] Reem Abu Taleb, A Study of Secure Routing Protocols for Wireless Sensor Networks, Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, Vol. 6, No. 3 March 2015.
[11] Zhe Yang and Abbas Mohammed Blekinge Institute of Technology Sweden: A Survey of Routing Protocols of Wireless Sensor Networks , December 14th 2010.
[12] V. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks, Proc. IEEE INFOCOM '97, Kobe, Japan (1997).
[13] Park V. and S. Corson, 2001. Temporary-ordered Routing Algorithm (TORA), Internet Draft, draft-ietf-manettora-spec-04.txt.
[14] V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification IETF Internet draft (1998), http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec- 01.txt.
[15] Anand Pandey, Dinesh Kumar, Shailendra Kumar Singh: Performance Evaluation of TORA Protocol with Reference to Varying Number of Mobile Nodes: IJAIEM, ISSN 2319 – 4847, Volume 2, Issue 12, December 2013.
[16] Ossama Younis, Student Member, IEEE, and Sonia Fahmy, Member, IEEE HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks: IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 3, NO. 4, OCTOBER-DECEMBER 2004.
[17] Rathna.r and Sivasubramanian.a," Improving energy efficiency in wireless sensor networks through scheduling and routing", 2012.
[18] Harneet Kour, Ajay K. Sharma: Hybrid Energy Efficient Distributed Protocol for Heterogeneous Wireless Sensor Network, International Journal of Computer Applications (0975 – 8887) Volume 4 – No.6, July 2010.
[19] Jing Deng, Richard Han, Shivakant Mishra, INSENS: Intrusion-Tolerant Routing in Wireless SensorNetworks, University of Colorado, Department of Computer Science Technical Report CU-CS-939-02.
[20] J. Deng, R. Han, and S. Mishra, (2006) "INSENS: Intrusion-tolerant routing for wireless sensor networks," Computer Communications, vol. 29(2), pp. 216-230.
[21] Mohamed-Lamine Messai, Classification of Attacks in Wireless Sensor Networks, International Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014.
[22] AlyMohamed El-Semary andMohamed Mostafa Abdel-Azim, New Trends in Secure Routing Protocols for Wireless Sensor Networks, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.