Research Journal of Applied Sciences, Engineering and Technology 12(11): 1095-1111, 2016
DOI:10.19026/rjaset.12.2851
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: October 9, 2015 Accepted: January 16, 2016 Published: June 05, 2016

Research Article

Diversity in Wireless Sensor Networks

Priya Verma and Gurjot Singh Gaba
Discipline of Electronics and Communication, Lovely Professional University, Phagwara, Punjab, 144411, India

Abstract: Due to the potential applications of Wireless Sensor Network in numerous areas, it has gained lot of importance but its functionality is subjected to lifetime of network, energy efficiency of node/network, security of data, coverage of whole network etc. The main aim of this study is to investigate the various domains of Wireless Sensor Networks. These following domains are routing, MAC layer, clustering, deployment, attacks and cryptography. Study of these techniques is concluded through comparison of different protocols on the performance measuring parameters like power consumption, scalability, quality of service, data aggregation and query based approach. It is found from the simulation that MCFA protocol works better than LEACH, SPIN, SMAC, Rumor Routing etc. in terms of power usage, quality of service, scalability and data aggregation.

Keywords: Clustering, cryptography, deployment, MAC, routing, Wireless sensor network

INTRODUCTION

If we connect two or more computers then Network is formed. Different computers are allowed by network to exchange data. There are many types of Networks like Local Area Network (LAN), Wide Area Network (WAN) and Metropolitan Area Network (MAN). Topology plays an important role in formation of network. Various tasks can be accomplished in the network like file sharing, hardware sharing and program sharing and user communication. Sending of data from one source to another is called transmission of data and the medium through which data are sent is called as transmission media. There are two types of media's for the data transmission which are 'guided medium' and 'unguided medium'. Wireless medium leads to a very much neater environment because they use less cabling and they do not need cables across our office and houses. In a network, points where two or more devices can be connected and two or more links can terminate are called nodes. The same fundamental theory exists in Wireless Sensor Network. In Wireless Sensor Network, instead of computers, small and powerful processing nodes are used which are called as sensor nodes (Bokare and Ralegaonkar, 2012).

Wireless Sensor Network consists of many sensing element nodes i.e., hundreds and thousands of nodes that senses the events and collects information from the environment and routes it to the base station. WSN design comprises of layered design and clustered architecture. In layered design, one powerful base station exists with several layers of sensing element nodes around sink. In clustered design, every cluster has one Cluster Head (CH) and all the sensor nodes are well ordered into different clusters in the network. Node architecture in Wireless Sensor Network consists of sensor, power supply, memory, transceiver and microcontroller (Sharma and Mittal, 2013). Wireless Sensor Network is initialized in practice through optimal routing, appropriate clustering and deployment, prevention from attacks, necessary MAC protocol and use of cryptography as highlighted in Fig. 1. In the routing field of WSN, for any transmission of data over the network; use of various routing protocols are necessary which can route the information through multipath transmission instead of direct transmission (Kumar and Katiyar, 2015). In clustering, heterogeneous node elements are placed in different clusters where each cluster has one head of the cluster (CH) who collects information from the sensor nodes exists in cluster and then route the information to the Base Station (BS) (Sasikumar and Anitha, 2014). In deployment, node elements are deployed in any particular zone which requires to sense, when any event occur, one of the node detect it and originate the report of that event and transmit it to the sink node or BS through multipath transmission (Seema, 2013). In Wireless Sensor Networks, various types of attacks are being done by attackers to degrade the performance of the network. These are sinkhole attack, black hole attack, wormhole

Corresponding Author: Gurjot Singh Gaba, Discipline of Electronics and Communication, Lovely Professional University, Phagwara, Punjab, 144411, India

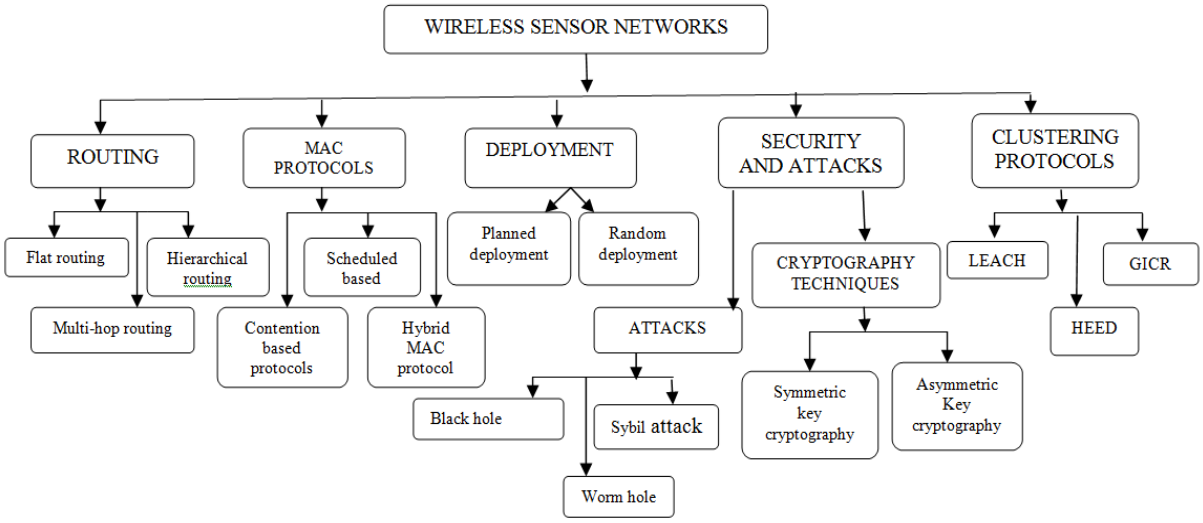

Fig. 1: Tree structure highlighting key elements of WSN set-up

attack, jamming attack etc. (Alam and De, 2014). Media Access Control (MAC) is also one of the important fields in Wireless Sensor Network because only MAC specifies that at what time nodes need to communicate with each other in the network and when they have to send their data to the base station. If there is no existence of MAC protocol, then collision will occur in the network because multiple nodes may start interacting within same time; which in turn, creates much trouble in the network (Patil *et al*., 2013b). For any type of transmission over the network, authentications, integrity and security is required. It can be achieved using Cryptography. It is most important field where a transmitted message is encrypted with some encryption algorithm and then encrypted message is sent to the destination node. This ensures that no unintended user can access the transmitted message (Jirwan *et al*., 2013). Various encryption techniques are built for the safe communication over the network which includes Caesar ciphers, block ciphers, one time pad ciphers and many more. So security is the major concern in the network domain (Shakti, 2013). Various applications of Wireless Sensor Networks includes detection and reporting of an event, tracking based applications, sink initiated querying, data gathering and periodic reporting etc.

LITERATURE REVIEW

The study and research of Wireless Sensor Network is categorized into five domains. These domains are Routing, MAC protocol, Deployment, Security and Attacks, Clustering. These domains are well described and classified in this study to provide better understanding.

Few insights of these domains are as described below:-

Routing: General classification:

- Flat routing
- Multi-hop routing
- Hierarchical routing

Flat routing: Flat routing assigns an equivalent task to each node and the results are passed to base station on the idea based on some question. This method of causation processed information consistent with question is data centric approach. Several protocols belong to this category. Some of these are: SPIN, Direct diffusion, Rumor routing, MCFA, COUGAR and ISDQ and CADR.

Sensor Protocol for Information via Negotiation (SPIN): In this protocol, information is passed to all or few nodes within the network with assumption that every node has equal potential and communication methodology. It gathers Meta-data (Set of information that identifies the data regarding alternatively data) from completely different nodes and additionally appends a singular ID to the current Meta data to avoid redundancy/duplication. SPIN Protocol uses data negotiation. It may be a periodic protocol that works on the basis of time intervals or on-demand. It works in 3 steps which are ADV, REQ and DATA as shown in Fig. 2. In ADV (Advertisement), nodes that have some data to share, advertise their data to its neighbor with the employment of ADV messages. REQ (Request) is employed to indicate interest towards the Meta-Data. REQ message is directed to the source who promoted the meta-data. Source node starts transmitting the data to the node which have a Unique ID when it receives REQ (Kumar and Katiyar, 2015).

Directed diffusion: In WSN, directed diffusion is called as data aggregation. Energy of communicating

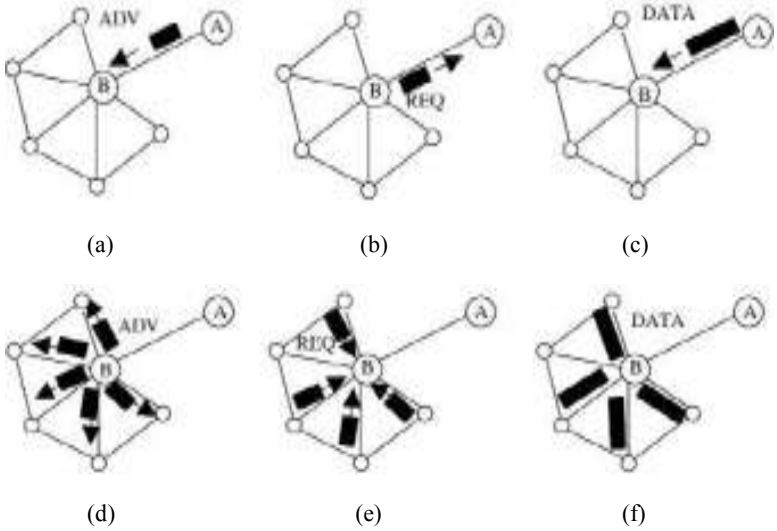

Fig. 2: SPIN PROTOCOL; (a): node A advertising its data to node B; (b): node B responds by sending a request to node A; (c): node A send data to node B; (d), (e), (f) process continues

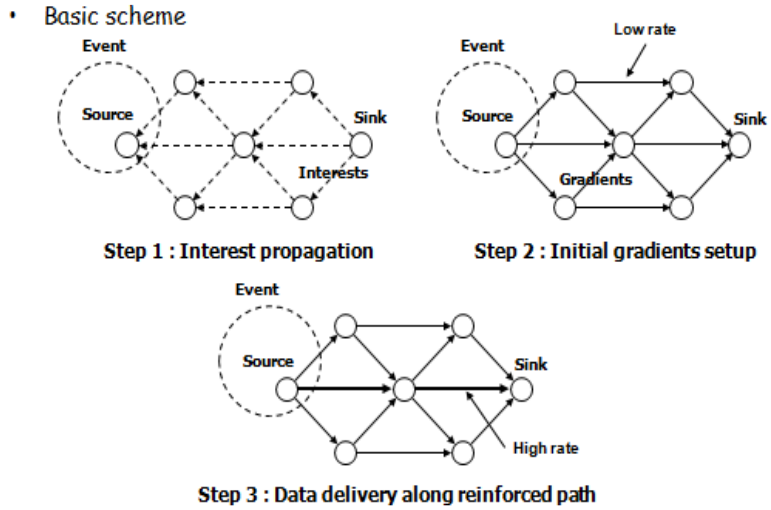

Fig. 3: Directed diffusion protocol phases

nodes is preserved with help of aggregation mechanism. It receives data from detector nodes spread across the area until data from all nodes are not received, removes the redundant data and finally send the aggregated data to destination node. Due to aggregation, lots of overhead is reduced thus increasing the lifetime of the node. Directed diffusion could also be a multiple offer, single sink protocol that defines the path from multiple nodes to single destination. Directed diffusion is meant for strength, scaling and energy efficiency. It is Knowledge Centrical communication protocol based totally on application directed protocol. Throughout this protocol, sink node shows interest for a particular data. Sources satisfying the interest could also be found and intermediate nodes can transfer data directly towards sink as shown in Fig. 3. Main choices in direct diffusion area are Unit Interest (It could also be a matter that specifies what user wants), Gradient (In every detector node there is a creation of direction state that receives the interest) and data dissemination (Through which path the information will be to relayed the sink node) (Kumar and Katiyar, 2015).

Rumour routing: It is another approach similar to directed diffusion. The algorithmic formula works on agents and events. In Rumor routing represented in Fig. 4, base station yields question for information to those particular nodes who knows the data rather than flooding queries overall within the network. Event tables are generated by every node. Once a node observe any change in the surroundings, it start checking its event table, if observed change is already listed, no changes takes place and if it's not, then node start updating its event table. Node start yielding information from packet denoted as 'agent' and forwards this 'agent' to all its neighbors on the event

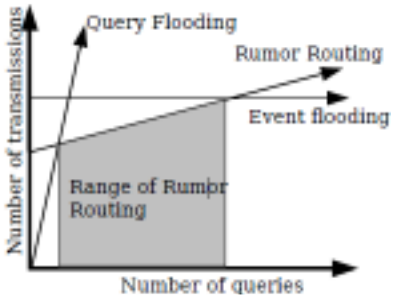

Fig. 4: Rumor routing

basis. Neighbor nodes start adding the agent information in the table along with ID. Base station questions solely to that node that generates agents of the generated question. Rumor routing is not like directed diffusion where multiple methods have shaped from supply to destination. Routing is the consumption of energy in generating and maintaining the events table. There's only 1 path from sender to receiver. The most noticeable weakness of Rumor.

Minimum Cost Forwarding Algorithm (MCFA): It is a Minimum Cost Forwarding Algorithm and it's principle of operation is somewhat similar to Distance Vector Routing (DVR) algorithm of ad-hoc networks. MCFA relies on belief that supply and destination nodes of the networks are perpetually mounted at their locations and solely the route from supply to destination must be found, rather than holding events table. The routing table is maintained that carries the smallest amount path from supply to destination. MCFA operation starts with the formation of a cost table, where cost of every node is stored into the sink memory. Sink node spread an Advertisement (ADV) message. Every node sends the message to its neighboring node on receiving the message after adding its own cost in ADV message. The cost field computation gets over once the ADV message propagates within the whole network. At last, the supply node sends information to the sink node through the trail with minimum cost. Disadvantage of MCFA is the variety of updates that takes place when two routes have identical cost and then it'll be tough to decide the most effective path. To overcome this drawback, a backtrack formula was designed that ensures that the update can happen solely once a particular quantity of time is $c \times L_{oc}$ wherever c is constant and L_{oc} is that the cost related to the link from wherever last update are received.

Information Driven Sensor Querying (ISDQ): The main principle in ISDQ is to route data in such a way to achieve additional information and less delay. Base station initially decides the event for question so as to explore the node concerning with the precise event space. Afterwards, the nodes near the information participate in the process.

Constrained Anisotropic Diffusion Routing (CADR): CADR permits each node to estimate value per information and conjointly the data that cost less and ample to be used is then forwarded to sink node.

COUGAR: Its basic operation is to hide the question process from network layer operation. However the limitation here is that the execution of further layer i.e., query layer that consumes additional energy.

Multi-hop routing: In this approach, every node re-directs the perceived knowledge to alternative node towards sink and performs better than direct transmission mechanism through short distance knowledge mechanism. However during this multi-hop routing, there's additional load on the nodes that are close to concerning base station and they run out of their energy at any time which may degrades the performance of the network. Examples are DSDV, AODV.

Hierarchical routing: It is additionally known as cluster based routing. In this routing, high energy node are used for communication and low energy nodes are used for sensing purpose. It's economical than flat routing. Information is aggregated at cluster level that reduces the quantity of packets being directed from supply to destination that successively reduce the consumption of energy. The employment of cluster head may be an important part in hierarchical routing. Since cluster heads needs additional energy for communication purpose, cluster head rotation is additionally a very important step in hierarchical routing.

MAC PROTOCOLS

Wireless Sensor Network exhibits wide space for researchers because of the acute scope of applications in several domains, for e.g. to notice any specific event; observance of specific areas etc. MAC protocol is required to find the way nodes in network can communicate? At what time they have to communicate? Incorrect slot timings could lead to simultaneous communication between nodes at same time that result in collision and plenty of issues within the network. Some reasons of energy wastage are collision, packet overhead, idle listening and latency. MAC protocol for WSN is classified into 3 basic classes that are contention based protocol, scheduled based protocol and hybrid MAC protocol (Patil *et al*., 2013b).

Scheduled based protocols: In scheduled based protocol, a schedule is prepared which allocates the timings to nodes as per the TDMA plan to use the resources (like Bandwidth) of the network. Scheduled based protocol helps to avoid collision and ideal

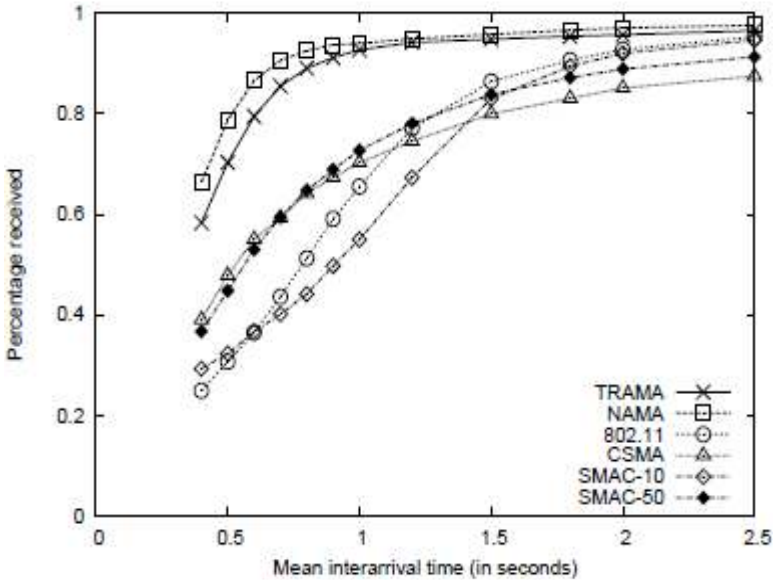

Fig. 5: Unicast traffic

listening. On demand, scheduled may be mounted or computed. In different words, slots are pre-allocated to the user or individual nodes. Owing to this, each node can send information supported their interval and so it avoids collision. Scheduled based protocols are TDMA, FDMA and CDMA.

In Time Division Multiple Access (TDMA), the time is divided into range of frames and every frame is further partitioned into range of time slots. Nodes are allotted with these different time slots and each node has several slots through which it sends signals to the other nodes. To overcome the problem of overlapping, there ought to be time synchronization between totally different nodes.

In Frequency Division Multiple Access (FDMA), there's a waveband that is assigned into sub channels. These sub channels are appointed to numerous nodes for the transmission of knowledge signal. Nodes ought to transmit data in their allotted channels solely.

In Code Division Multiple Access (CDMA), it uses spread spectrum techniques. There are no time slots and frequency channels for transmission. In CDMA, full frequency spectrum is available for the nodes; however is transmitted with totally different codes thus preventing collisions and overlapping (Patil *et al*., 2013b).

Traffic Adaptive Medium Access protocol (TRAMA): Mostly TDMA based protocol is used for the implementation of collision free and energy efficient channel in WSN. In TRAMA, nodes are placed to low power idle state once they aren't transmitting packet and conjointly not receiving any packet to preserve the valuable resources. TRAMA includes of neighbor protocol, scheduled exchange protocol and adaptive election protocol. In Neighbor protocol, there's a group of data of all the neighboring nodes within the network. In scheduled exchange protocol, there's associate degree interchange of the neighbor's scheduled and 2 hop neighbor data. Adaptive election algorithmic program decides the nodes which will send and receive the information. In uncast traffic shown in Fig. 5 and broadcast traffic shown in Fig. 6, TRAMA is compared with 802.11, CSMA, S-MAC-10 and S-MAC-50.

Contention based protocols: In contention based protocols, the slots are pre allotted to the quantity of users and that they ought to send information solely at intervals their allocated slots. There's an extreme risk of collision in these protocols. Contention based protocols don't needs synchronization as in TDMA. The disadvantage of competition based protocols is that here all nodes ought to send request to the central node for resource allocation, thereafter central nodes forever stay in on-state that degrades the energy potency of the network. Contention based protocols are ALOHA, CSMA, S-MAC and T-MAC.

ALOHA: It refers to a straightforward communication theme during which every supply node in the network send information whenever it has frame to send. If the frame reaches destination successfully, consequent frame is transmitted.

Pure aloha: When the sender has information to send, it only accesses the channel for the transmission of information shown in Fig. 7. The prominent limitation

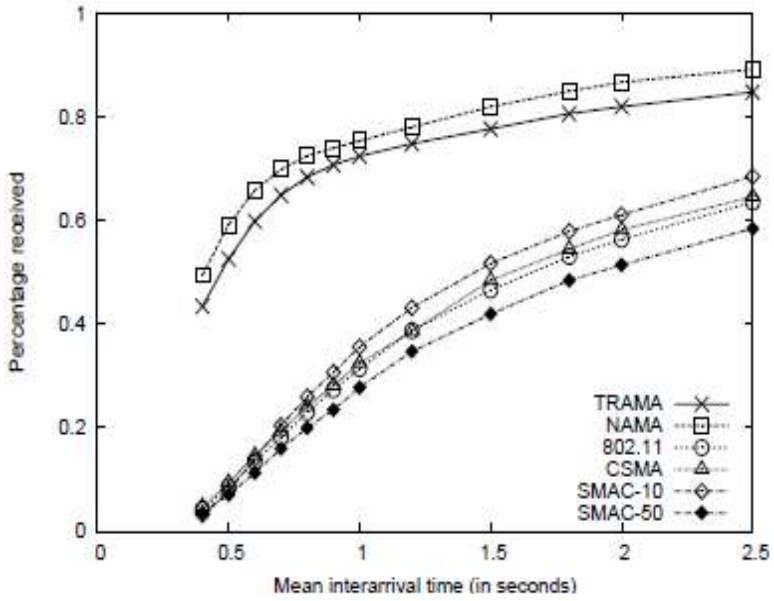

Fig. 6: Broadcast traffic

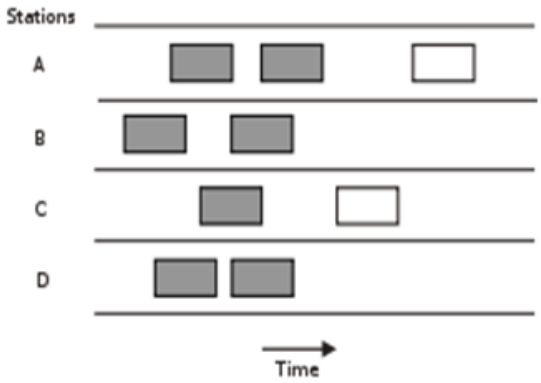

Fig. 7: Pure ALOHA

here is the availability of one channel to share among all the nodes which may lead to latency, overhead and collision.

Slotted aloha: In slotted ALOHA, there's a division of time into various slots and nodes usually senses the channel at the beginning of each slot and occupy it if channel is idle, if node didn't occupy the channel at the beginning of the slot, then it has to wait till next consequent slot as shown in Fig. 8. In slotted ALOHA, there's conjointly a likelihood of collision once clocks of nodes within network are asynchronous.

Carrier sense multiple access: When a node has information to send, it transmits spontaneously in Pure ALOHA and Slotted ALOHA that result in totally different issues within the network like collision, latency etc. To mitigate these issues we've got Carrier Sense Multiple Access. In CSMA, if node has information to send, it initially senses channel, if channel found unoccupied, then solely it transmits information which can scale back matter of collision

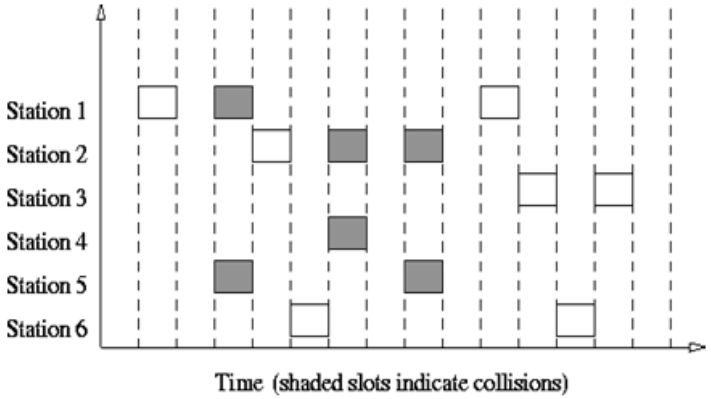

Fig. 8: Slotted ALOHA

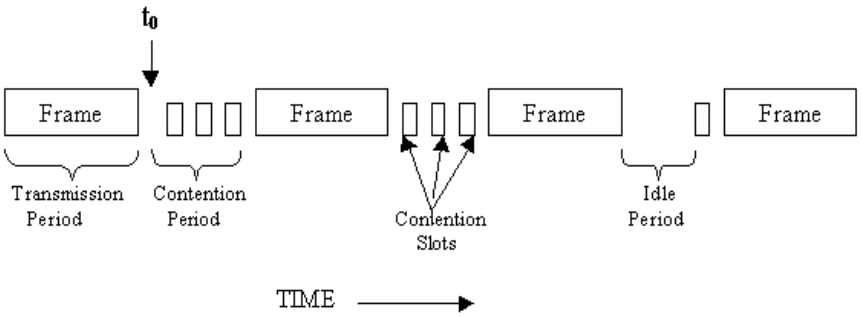

Fig. 9: Carrier sense multiple access

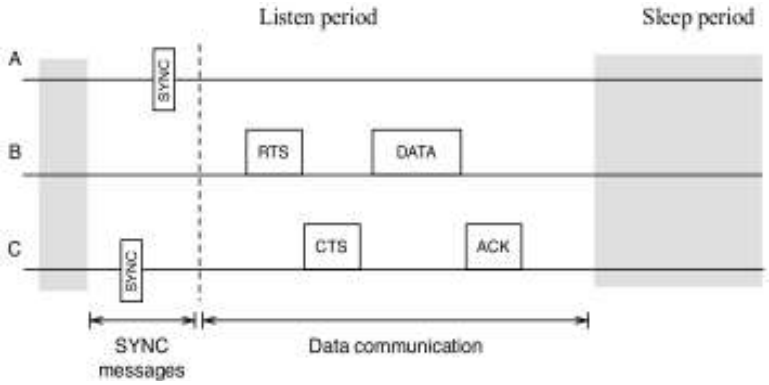

Fig. 10: Working principle of S-MAC

within the network. In CSMA/CA, once medium is unoccupied, station doesn't transmits instantly. It holds its transmission for a moment of time referred to as Inter-Frame Space (IFS) (Patil *et al*., 2013b). Upon waiting, if channel is idle, it sends the packet shown in Fig. 9. In CSMA/CD, acknowledgement mechanism is employed to watch whether or not the transmission is successful. In CSMA/CD, a node monitors the channel ceaselessly even after the transmission of the packet.

S-MAC (SENSOR MAC): This protocol reduces the energy consumption attributable to overhead, idle listening and collision. Throughout this, every node has a pair of states: Active state and Sleep state. A node can transmit and receive information solely in its listening time. Sensor-MAC acquires a periodic wake up strategy. S-MAC tries to synchronize the schedule of neighboring nodes soon to make them listen simultaneously. It's of three phases: SYNC, RTS and CTS as shown in Fig. 10. Packet contains SENDER-ID and sender sleep schedule. Receiver alters their timings accordingly. In RTS, all the nodes interested in transmission show their interest to a specific node. In response to RTS, the secondary node generates CTS frame that stands for Clear to send and forwards it to the node from whom RTS was issued. In S-MAC, all the nodes from virtual cluster synchronize their sleep and listen periods and communicate throughout listen

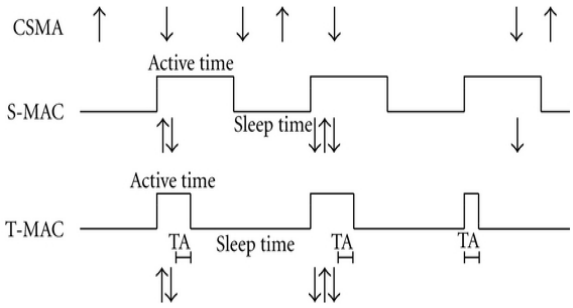

Fig. 11: T-MAC operation

periods and do rest in the remaining time. The prominent advantage is that it avoids idle listening and conjointly the disadvantage is length of listen quantity and sleep amount is uniform in S-MAC, it will be tough to manage in variable traffic load that degrades the effectiveness of the protocol (Patil *et al*., 2013b).

T-MAC (TIME-OUT MAC): Time-out MAC is designed to improve the standards of S-MAC protocol under dynamic traffic load conditions. It's similar to S-MAC, however it adaptively reduces the listen period resulting in energy conservation (refer Fig. 11).

Moreover listening period ends immediately once no node desires to transmit the information whereas in S-MAC, the listen amount encompasses a stable length.

Table 1: Extensions of WLAN standards

IEEE 802.11	Year introduced	Frequency band (GHz)	Transmit schemes	Modulation types
a	1999	5	DSSS/OFDM	BPSK, QPSK, 16-QAM, 64-QAM
b	1999	2.4	DSSS	CCK
g	2003	2.4, 5	DSSS/OFDM	CCK, BPSK,QPSK, 16-QAM, 64-QAM
n	2009 (est.)	5	MIMO-OFDM	BPSK, QPSK, 16-QAM, 64-QAM
ac	2013	5	MIMO-OFDM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

LAN (IEEE 802.11 Wireless WLAN) standard: WLAN in the year 1997 was customary brought forward. It is based on Carrier Sense Multiple Access/Collision Avoidance. Once a sender desires to send a packet, it hears the channel foremost. So, once the channel is free for specific time, node begins transmission.

On listening to request, receiver send acknowledgement. If sender does not capture the acknowledgement, it again re-transmits the request packet (Patil *et al*., 2013a). Thus as per authority, maximum seven times it has potential to re-transmits the request packet. To beat the possibilities of collision, method of RTS is employed. When receiver is idle, it sends CTS back to sender and then starts communication. The disadvantages are: Every station needs to anticipate an amount of time which can cause a lot of delay. Because of this, effectiveness of the whole system has been affected. Table 1 shows the extensions of IEEE 802.11 i.e., 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac along with their invention dates, frequency band, transmit schemes and modulation types.

Hybrid MAC protocol: Hybrid based protocols are the combination of TDMA and CSMA.

ZEBRA-MAC (Z-MAC): Hybrid protocols merge the power of TDMA and CSMA. This protocol behaves like CSMA, when number of users wanted to acquire the Bandwidth is less. However, in high competition, it behaves like TDMA. During deployment, time slots to the users or nodes are provided. Each node has one or plenty of slots available for transmission. Throughout this protocol, nodes ought to perform carrier sensing, that is sensing the channel before transmit to see whether or not or not the channel is idle or not. If the channel is found unoccupied, then it begins the transmission of data. Some limitations of this protocol are:

Hidden terminal drawback in Z-MAC: Consider a three-node chain in HCL mode: A--B--C, assigned slots one, two and three severally as shown in Fig. 12. If the slot is two and also the owner (B) doesn't transmit its information, then each A and C may contend for identical slot and transmit, since they're each within the one-hop neighborhood of B. this might cause a hidden terminal drawback. Thus, the sole method of avoiding

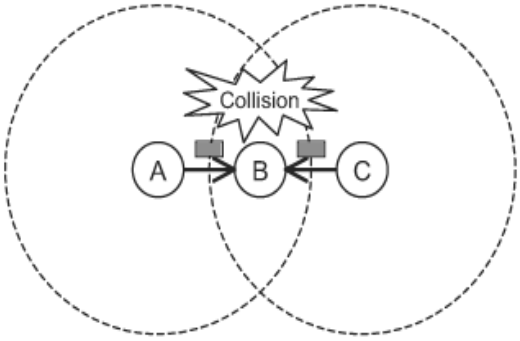

Fig. 12: Hidden terminal problem in Zebra-MAC

hidden terminals is truly to limit slot rivalry to the slot owner (s).

- Slot assignment and clock synchronization that utilize a lot of energy than a straightforward CSMA- only scheme.

Deployment: Deployment may be a serious issue to be resolved in WSN. Node deployment carried in a correct manner will scale back several advanced issues of WSN like routing, communication etc. In WSN, deployment majorly falls in two classes i.e. planned deployment and random deployment. Once the deployment of sensing nodes is completed, its task is to stay monitoring that event ceaselessly. Once an event happens or once any changes takes place, one amongst the nodes detects it and generates the report of that event and transmit the report back to base station through multi hop wireless links. It may extend the period of the network (Deif and Gadallah, 2014).

Planned deployment: In planned deployment, location of sensors deployment is chosen before its deployment. In alternative words, deciding the location of sensors first and deploying them.

Random deployment: In random deployment, sensing element nodes are deployed in explicit space by aircraft etc. One issue in random deployment is the communication hole that arises due to random deployment which doesn't cover the whole space. Therefore it's tough to urge for the report of that place where hole is present. Such types of holes are called as communication/coverage hole, routing holes and jamming holes (Seema, 2013).

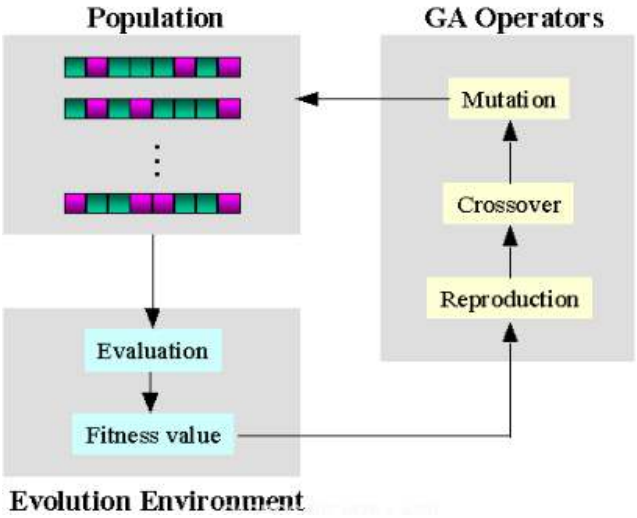

Fig. 13: Genetic algorithm

Approaches in wireless sensor network deployment algorithms: Four mathematical approaches used in such algorithms are Genetic Algorithm, Computational Geometry, Artificial Potential field and Particle Swarm Optimization.

Genetic Algorithm (GA): GA works on optimized rule base algorithm. This rule is employed for finding improvement issues in numerous fields like networking, engineering etc. It estimates best answer through generating totally different individuals. Some implementation steps of this algorithm are shown in Fig. 13.

Selection rules: There is a selection of individuals which is known as parents that contributes to the next generation population.

Cross over rules: In this two parents are combined to form the children's for next generation.

Mutation rules: Random changes are applied to parents to form children.

Fitness evaluation: To evaluate weakest individual from the population.

This algorithm will terminate after finding an individual with a fitness corresponding to satisfactory solution to the problem.

Computational geometry: It is the study of algorithms which may be expressed in terms of pure mathematics. In WSN, most of the studies were supported by these two notable processes based on pure mathematics structures that are renowned as Voronoi diagram and Delaunay triangulation.

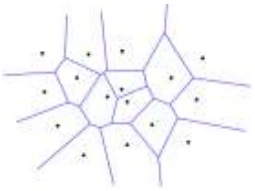

Fig. 14: Voronoi diagram

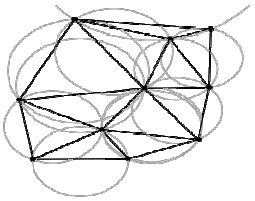

Fig. 15: Delaunay triangulation

In Voronoi diagram (Fig. 14), based on distance the plane is split into divisions to administer points in an exceedingly specific set. A group of points known as sites induce Voronoi diagram. Face coincides to the regions where one site is closest; there's a portioning of the plane.

Delaunay triangulation: Delaunay triangulation for a set S of points in a plane is a triangulation DT(S) such that no point in S is inside the circumcircle of any triangle in DT(S).Triangulation of a set S is defined as the planar subdivision whose bounded faces are triangles and whose vertices are the points of the set S as shown in Fig. 15. DT (S) has a very interesting property that it does not contain a point of S in its interior or inside the circumcircle of any triangle. This property is called empty circle. Delaunay triangulation method can help in estimate the point of weakest coverage in a deployed WSN and hence provides very useful guidance in case of deploying new sensors to improve coverage area.

Artificial potential field: This concept is earlier introduced in the field of robotics. In this approach, a mobile robot is assumed to be moving in a field of artificial, i.e. virtual forces. The goal can be represented by an attractive pole, which exerts virtual attractive forces on the mobile robot. The obstacles are represented by repulsive forces on the mobile robot (Seema, 2013).

Mathematically, this approach can be represented in the following equation:

$$U_{art}(x, y) = U_{att}(q) + U_{rsp}(q) \quad (1)$$

Particle swarm optimization: Birds move within the area and search for their food. One amongst the bird/insect smells the food and so found the goal that is termed expertise. Then this expertise is communicated to any or all of the swarm, direct its movement towards the search region to seek out the optimum resolution. S is outlined as N particles. Particles are assumed to maneuver at intervals in a delimited region, iteratively so as to go to all regions completely (Seema, 2013). It's achieved by shaping the rate of every particle that is employed to regulate the particle position in each iteration. This algorithm conjointly maintains a memory set wherever every particle store the simplest position it's ever reached throughout its search in delimited region.

Clustering: Clustering is an important technique In Wireless Sensor Network to provide better scalability, reliability, reducing the consumption of energy and increase overall network performance. In WSN nodes consists of three parts i.e., sensing, process and communication. Therefore, to supply higher scalability and improve the other parameters of the network, device nodes are sorted into clusters. Grouping of device nodes is termed as cluster. Hierarchical clustering is a competent way to minimize the overall energy consumption in cluster through aggregation. There are different clustering algorithms which are cluster head selection, heterogeneity and clustering process. Clustering is employed in Wireless device Networks which results in higher scalability, economical supply distribution and flexibility to handle a growing quantity of work in an exceedingly capable manner (Sasikumar and Anitha, 2014).

Drawbacks of clustering:

Range of clustering: The analysis says that cluster heads are indicated on the premise of their unique-id or residual energy. But unique-id and residual energy as a selection parameter does not guarantee that chosen cluster head will be always remain an optimized one. If the cluster head is present at extreme end of cluster or elsewhere in cluster then it desires RF enhancement to send the information to a longer distance. This turns to be a disadvantage of clustering.

Hot spot in clustering: All the nodes that are associated directly with base station have a lot of masses to cover. As a result, they need to forward the information coming from all the nodes to the Base Station. If these device nodes lose their energy then it's out of the question to send the packet to the destination station. In this case, network communication dies out as way nodes won't be able to transmit the information to the bottom or base Station (Kumar *et al*., 2014).

Ripple effect in clustering: In some cluster schemes, once any event happens within the network which disrupts the functioning of the cluster, then there's formation of cluster head again in the network. As an example, death of some nodes ends up in re-elections of cluster head once more. Therefore it's called ripple result of re-clustering. Re-election of cluster head might have an effect on the structure of the many clusters. So, this disadvantage additionally degrades the general performance of cluster within the network.

Flooding in clustering: Lot of energy of device nodes is wasted due to discovery of the new routes through flooding of packets within the entire network.

METHODOLOGY

The work is extensively carried out by the researchers on MATLAB (Gilbert *et al*., 2012). Various protocols are implemented and tested on a sample network. This network is created in MATLAB and kept same for testing of all protocols to measure their performance and to reveal the suitability of protocols in various applications.

Different algorithms of clustering:

Low energy adaptive clustering hierarchy protocol: LEACH is Low Energy Adaptive Cluster Hierarchy protocol. Leach may be a cluster primarily based routing protocol. During this, CH collects information from all of its cluster members within the cluster and sends that collected data to destination node or base station as shown in Fig. 16. Therefore cluster head decreases the transmission distance by aggregation the information from all nodes and save additional quantity of energy at every node. The communication method in LEACH is completed in 2 ways that i.e., setup section and steady section.

Figure 17 shows about the cluster head formation process in LEACH protocol.

Setup phase: In setup section, cluster head is selected through elections where each node generates a number whose range is between zero and one and compares that number with a threshold value. Those nodes can become the cluster heads whose range is larger than threshold.

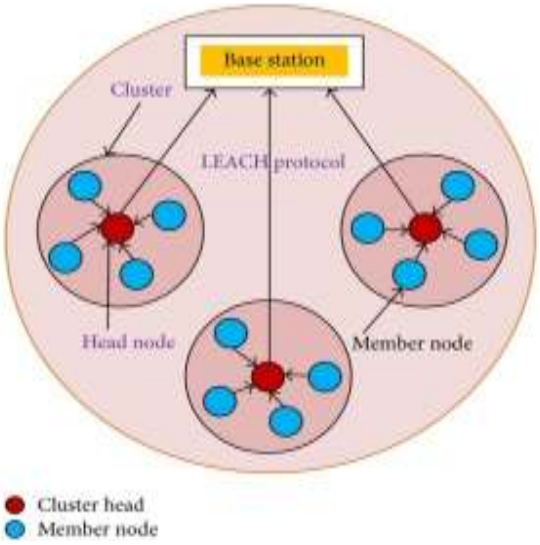

Fig. 16: Process of clustering in LEACH protocol

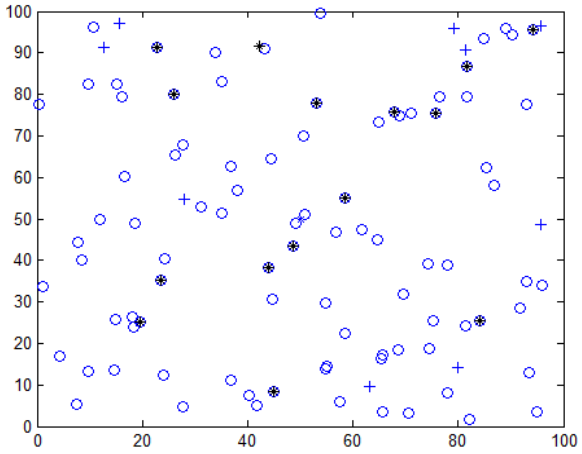

Fig. 17: Cluster head formation process in LEACH

The elected node later broadcast message to all alternative nodes within the network concerning its election as Cluster Head. One or additional message can also be received by nodes through completely different cluster heads. Stronger the signal, node is nearer to cluster and therefore node will verify its distance from cluster head. Subsequently node sends a message to cluster head that contains its ID. Once the CH receives data from the node it records the node ID and adds that node as its member node. After sharing data, every CH becomes aware about its cluster members. Subsequently cluster head prepares a TDMA schedule and broadcast it to all the cluster members for the collision free transmission. Through this manner all the member nodes get their time slots for the transmission of information, afterwards steady section starts:

$$T(n) = \frac{p}{1-p*\left(r \bmod \frac{1}{p}\right)} \; if \; n \in G \qquad (2)$$

where,

p : The desired percentage of cluster heads
r : The current round
G : The set of nodes that have not been cluster heads in the last $1/p$ rounds.

Steady phase: Within the steady section, once the clusters are created and TDMA schedule is fixed, information transmission takes place. Nodes prefer to send the data in the allocated slot only. The cluster head perpetually activates the transceiver within the steady state section (Kumar *et al*., 2014).

Drawbacks of LEACH:

- In LEACH, low energy nodes may also become the cluster head. Cluster head communicates with base station in single hop; therefore LEACH cannot be utilized in massive scale WSNs.
- To receive information from nodes, cluster heads never goes on sleep mode that leads to consumption of heap of energy. This degrades the general performance of the network since Cluster Head during this state would die out soon and restructuring of the network will continue to happen.

Hybrid, energy-efficient and distributed clustering approach: HEED is Hybrid, Energy-Efficient and Distributed cluster approach. In HEED, one hop communication is carried out by nodes leading to preservation of energy.

It uses an iterative clustering process for the choice of Cluster Head. HEED periodically selects cluster heads according to the node's residual energy and a secondary parameter, like node proximity to its neighbors or node degree (Kumar *et al*., 2014). In HEED, after variety of iterations it terminates the clustering process. It usually leads to increase in the network time period by distributing energy consumption. This approach added some options to the LEACH protocol i.e. during this protocol, sensor nodes are supposed to communicate regarding their residual energy throughout the network which may help to pick a stronger Cluster Head as compared to the initial LEACH protocol. Sensor node chooses a cluster head in its cluster range that converts LEACH into multi hop network.

H-HEED is updated protocol of HEED which provides the higher results than original HEED. In H-HEED there are two types of sensing element nodes that are: advanced nodes and normal nodes. In this heterogeneous approach, all the two level nodes are having completely different energy levels. So the protocol H-HEED will increase the performance, network lifespan, energy efficiency of the network as compared to HEED protocol (Sasikumar and Anitha,

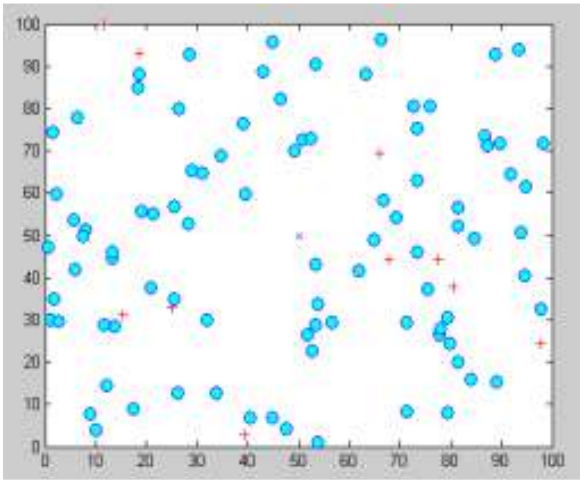

Fig. 18: Random deployment of sensor nodes

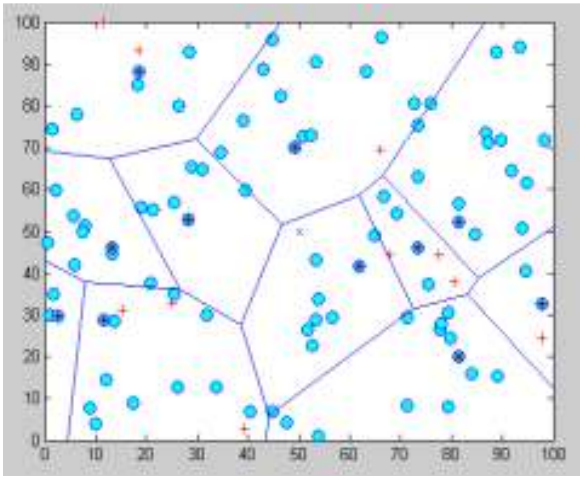

Fig. 19: Cluster formation

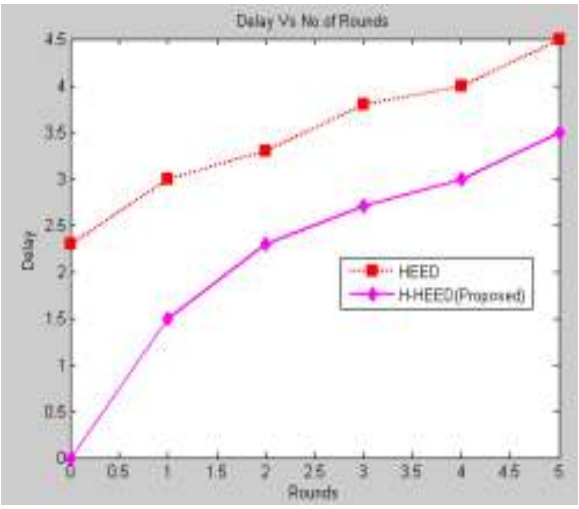

Fig. 20: Delay Vs number of rounds

2014). Figure 18 depicts that there are two styles of nodes that is advanced nodes and normal nodes.

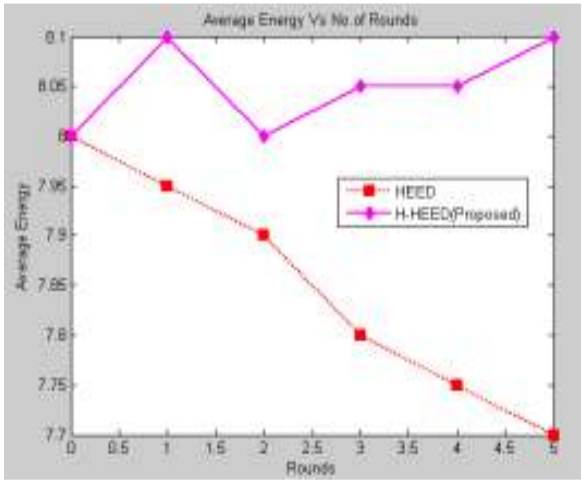

Fig. 21: Average energy Vs No. of rounds

Advanced nodes are symbolized with plus symbol and normal nodes are symbolized in circular form.

Figure 19 shows the formation of clusters. Firstly, cluster heads are elected and then the nodes which are nearest to that cluster heads will form the groups.

Figure 20, for every round the different delay values of HEED and H-HEED are plotted.

Figure 21, for every round, different energy values of HEED and H-HEED protocol are plotted.

Disadvantages of HEED:

- Higher communication overhead possible here due to the arbitrary selection of Cluster Heads.
- Frequent changing of Cluster Head and rebuilding clusters again and again consumes extra energy which can degrade the performance of the network.

Two step cluster head selection routing protocol:

- TSCHS is two step cluster head selection routing protocol. CHs in LEACH are randomly chosen based on threshold value thus resulting in decrease in lifetime of the network due to inappropriate selection method of Cluster Heads. Thus there's a replacement routing protocol referred to as TSCHS, which may resolve the cluster head selection problem of LEACH. In TSCHS, Cluster heads are selected in a temporary manner based on distance from cluster head to base station and residual energy.

There is various analysis problems on clustering that are still in coffin like there is an assumption that the base station and sensor nodes are stationary in nature; however in some applications, there is a requirement of mobile nodes for e.g., battle. In such cases, the updating of all the information tends to consume unnecessary energy. Therefore, new routing techniques are required. In cluster based routing protocols, each sensor node must send information to cluster head. Cluster Head

then forwards the information to the base station after aggregation. The research problems related to such protocols are how to form clusters such that the energy consumption and delay should be as minimum as attainable in WSN.

Attacks and security: Wireless Sensor Network, there is classification of attacks in three groups i.e., outside and inside attacks, passive and active attacks and mote class and laptop attacks.

Outside and inside attacks: Outside attacks in Wireless sensor Network comes from those nodes that don't belong to the network. Outside offender node does not have any information regarding layout of the network. Inside attacks are those attacks that have license to access the network and conducts attack while staying inside the network.

Passive and active attacks: Passive attacks are primarily eavesdropping. In passive attacks, the opponent node do not modifies the information. But in an active type of attack, the wrongdoer node tries to form changes within the information and even tries to send the information on wrong target.

Mote class and laptop attacks: During mote class attack, an opponent node will decide upon the varied nodes that have an equivalent ability within the network and by using these nodes it will attack over the network. However in laptop class, an intruder attacks the system by using solid devices like laptop so that powerful attack can be done to harm the network.

Threat attacks in WSN: Different possible attacks can be categorized as:

DOS attacks: In DOS attacks, the attacker attempts to prevent user from accessing the network.

Jamming: In jamming, wrongdoer creates a large number of radio frequencies within the network that ends up in eruption in communication within the network.

Data integrity attack: In this attack, wrongdoer introduces the false node within the network. Once information is shared over the network then that false node modifies the information of the packet or packet header which contains the destination information of packet. This might be a compromise to the integrity of the information.

Sybil attack: A Sybil attack occurs when the attacker creates multiple identities or when a node in the network

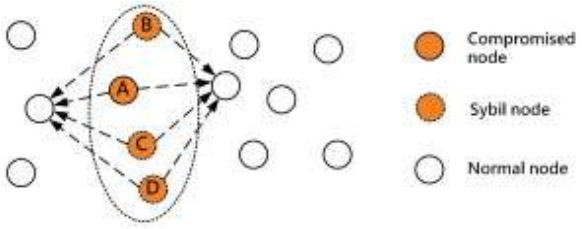

Fig. 22: Sybil attack

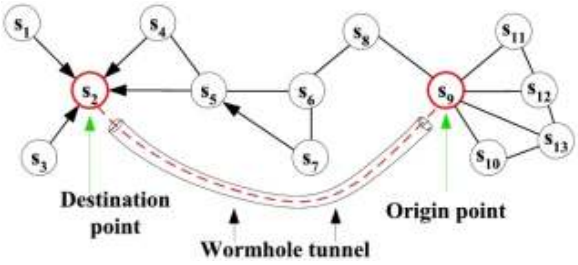

Fig. 23: Wormhole attack

claims multiple identities (Alam and De, 2014) as shown in Fig. 22.

Black hole attack: By publicizing itself as a shortest path, any false node will react as a part within the field of sink and tempts the whole traffic to be felt it. Then adversary collects all the packets coming back from that route that he publicized as a shortest route and once a route is created, malicious node then starts dropping packet or frame. It produce high rate of packet and integrity loss.

Wormhole attack: Most complicated attack and hardly detected. Adversary may produce a prime quality tunnel between two nodes i.e., one inside the network and one outside the network. All the entire traffic of malicious nodes moves through it as shown in Fig. 23. The adversary received messages from one section of the network and tunnels this message over a low latency link and sends this message to the opposite section of the network. Wormhole node creates fake path advertisement that points to shorter path than the initial one within the network. It has one or additional malicious nodes and a tunnel between them. The attacking node will capture the packet from one location and transmits them to alternative distant set node.

Sinkhole attack: As the name suggests, the adversary creates a sink close to the nodes. Sink hole attacks produce compromised node by spoofing all the information of routing protocol to make a false optimum path. Malicious nodes are extraordinarily engaging and manipulating the neighbor node to choose thereon false path that's reaching to the compromised nodes at the end. By creating the sink, the adversary may drop all

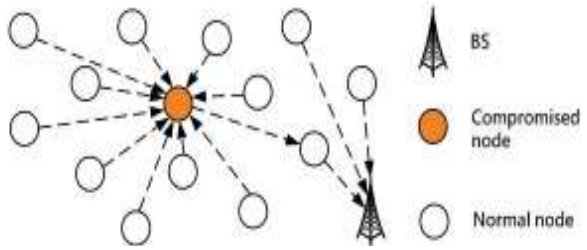

Fig. 24: Sinkhole attack

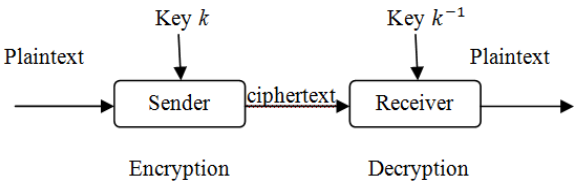

Fig. 25: Components of cryptography

packets travelling over network and do modification inside the network (Alam and De, 2014) as shown in Fig. 24. Since all node communicate with each other via base station, the adversary simply move all the traffic on the quality route to destination created by it.

CRYPTOGRAPHY (SECURITY)

CRYPTOGRAPHY comes from Greek work 'Secret writing'. Cryptography is invented for safely transmission of knowledge, within the existence of any malicious node or attacker. In cryptography, encryption is done at the transmitter end so that no attacker will be able to interpret it while data is on the way. It can provide Confidentiality, Integrity and Accuracy (Jirwan *et al*., 2013).

Few components required to perform the task of Cryptography is:

Plaintext and cipher text: The original information routed over the network is called plaintext as shown in Fig. 25. After applying encryption algorithm to the plaintext, a cipher text is obtained.

Cipher: Encryption and decryption algorithm used in cryptography to encrypt and decrypt the message information are called ciphers.

Key: A number that a cipher operates on is called a key. For encryption, three elements are needed i.e., coding key, rule and plaintext. Once these elements are used along, they forms cipher text. For decryption also, we needed, key, cipher text and algorithm.

Alice, Bob and Eve: There are three characters involved in explanation of encryption process i.e., Bob, Alice and Eve. Alice transmits the information message. Bob is at the receiver side, he receives the information transmitted by Alice. Eve is an attacker node that tries to disrupt the communication between Alice and Bob.

Techniques of cryptography:

Symmetric key cryptography: Secret key cryptography is also known as symmetric key cryptography. In this encryption technique, an identical key as shown in Fig. 26 is used by both the parties involved. The same key is used to decrypt the message which is used by the sender for encryption. Both source and destination end uses the same key or secret key. This technique was built in very past years, during wars, when message was to be exchanged between different parties, in order to get security into their work, so that no outsider can access their information.

Asymmetric key cryptography: Asymmetric key cryptography works on two dissimilar keys i.e., private key and public key. Receiver stores the private key secretly and discloses the public key to the general public as shown in Fig. 27. When Alice wants to send information to Bob she uses the general public key to

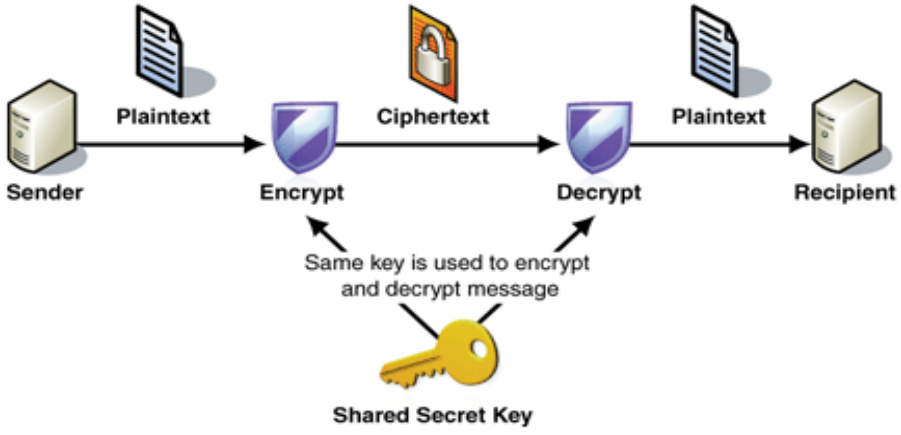

Fig. 26: Symmetric key cryptography

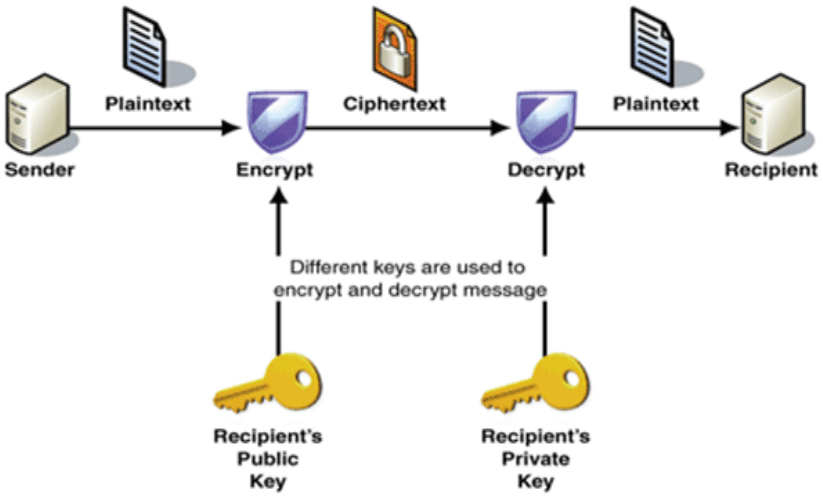

Fig. 27: Asymmetric key cryptography

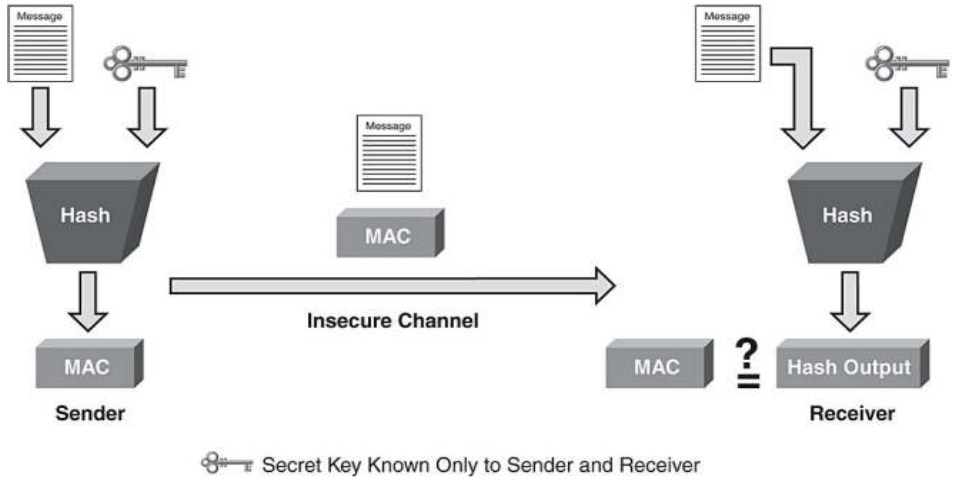

Fig. 28: Hash process

create cipher text of the message and as the Bob has private key, so message is decrypted by Bob at destination end. Two algorithms are common in Asymmetric key cryptography i.e., RSA and Diffie Hellman.

RSA: RSA is the most common public key cryptosystem that is employed by trendy PC's to cipher and decipher information data, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman. RSA operates on two numbers, e and d as shown in Fig. 27 because the public and personal keys. The general public key may be shared with everybody, whereas the non-public key should be kept secret. In RSA cryptography, the public key will be used to cipher a message; then alternative (secret) key is employed to decipher it. This attribute is one reason why RSA has become the foremost widely used cryptosystem. It provides a way of reassuring the confidentiality, integrity, believability and non-reputability of electronic communications and information storage (Jirwan *et al*., 2013).

Diffie hellman: Diffie Hellman was one amongst the primary inventors who addressed various issues of attacks and concluded its research with the invention of various security protocols. This was done before the invention of symmetric key cryptography. The purpose is to agree on a key that multiple parties will use for a even coding, in such a simplest way that attacker cannot acquire the key:

- For the interchanging of key, Diffie Hellman specially proposed a Key Exchange protocol (Diffie and Hellman, 1976).
- In this two parties can interchange the key over the net without storing the key for future use purpose.

Cramer-shoup: A public-key cryptosystem proposed by R. Cramer and V. Shop of IBM in 1998. They

Table 2: Attributes of various routing and MAC protocols

Routing protocols/ Figure of merit	Classification	Power usage	Scalability	QOS	Query based	Data aggregation
SPIN	Flat	Average	Average	No	Yes	Yes
DIRECT DIFFUSION	Flat	Average	Average	No	Yes	Yes
RUMOR ROUTING	Flat	Low	Good	No	Yes	Yes
MCFA	Flat	Low	Good	Yes	Yes	Yes
CADR	Flat	Average	Average	No	No	Yes
CSMA	Contention based	Low	Good	No	No	Yes
TRAMA	Scheduled based	Low	Good	No	No	Yes
SMAC	Contention based	Low	Average	No	No	No
TMAC	Contention based	Low	Limited	No	No	No
LEACH	Hierarchical	High	Good	No	No	Yes
ZMAC	Contention based	Low	Good	Yes	Yes	No
IEEE 802.11	Contention based	Average	Average	Yes	Yes	No

proposed an asymmetric key system which was proven very efficient against adaptive chosen cipher text attack.

Digital Signature Algorithm (DSA): DSA provides the digital potential for the authentication and security of messages from opponent party. It is defined in NIST's Digital signature standard which is also called as DSS.

Hash function: Algorithms that don't use any key are hash function. Based upon the plaintext, a fixed hash value is computed which helps to preserve the integrity of data and makes it impossible for any third party to alter the data. The principle of concept is shown in Fig. 28.
Some hash algorithms are:

- Message digests algorithms which include MD2, MD4 and MD5.
- Secure hash algorithms which include SHA-1, SHA-2, SHA-224, SHA-256, SHA-384 and SHA-512 can produce hash values 224, 256, 384 bits in length.

RESULTS AND DISCUSSION

Results shows that much potential work have been carried out in the past. There are abundant techniques but with different properties which have been observed from the findings which is cited under Table 2. Table 2 describes the various protocols that have been examined and simulated. It is found that Rumor routing, TRAMA, ZMAC, MCFA are more optimized techniques as compared to the LEACH because of good scalability and low power consumption. LEACH has the potential to withstand increase of load and area of communications but it suffers from high power consumption. There are few techniques which are working moderately with average power consumption and average scalability options; those are SPIN, Direct Diffusion, CADR and IEEE 802.11. Data aggregation is done to increase the network lifetime. It is revealed from the results that SPIN, Direct Diffusion, CADR, Rumor Routing, MCFA, CSMA, TRAMA and LEACH aggregates the data to save energy at nodes but this feature was found to be missing in SMAC, TMAC, ZMAC and IEEE 802.11.

CONCLUSION

WSN is a broad area of research. A lot of research has been carried out in the recent era to obtain QOS. The motivation behind new inventions is the tremendous applications and diversity of WSN. A lot of MAC, Routing protocols and techniques are developed but still there are lots of flaws on which researchers need to do work. During the study, it is found that routing is a challenging issue in WSN because lot of attacks is carried out during transmission. It means while making routing protocol, two main things must be kept in mind i.e., Optimized and secured path. Therefore, it is suggested to use protocols which have the capability to increase the network life, energy efficient and reliable.

REFERENCES

Alam, S. and D. De, 2014. Analysis of security threats in wireless sensor network. Int. J. Wireless Mob. Network., 6(2): 35-46.

Bokare, M. and A. Ralegaonkar, 2012. Wireless sensor network: A promising approach for distributed sensing tasks. Excel J. Eng. Technol. Manage. Sci., 1: 1-9.

Deif, D.S. and Y. Gadallah, 2014. Classification of wireless sensor networks deployment techniques. IEEE Commun. Surv. Tutorials, 16(2): 834-855.

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. IEEE T. Inform. Theory, 22(6): 644-654.

Gilbert, E.P.K., B. Kaliaperumal and E.B. Rajsingh, 2012. Research issues in wireless sensor networks applications: A survey. Int. J. Inform. Electron. Eng., 2(5): 702-706.

Jirwan, N., A. Singh and S. Vijay, 2013. Review and analysis of cryptography techniques. Int. J. Sci. Eng. Res., 4(3): 1-6.

Kumar, A. and V.K. Katiyar, 2015. Routing approaches for wireless sensor networks. Int. J. Comput. Appl., 109(6): 34-40.

Kumar, V., S.B. Dhok, R. Tripathi and S. Tiwari, 2014. A review study of hierarchical clustering algorithms for wireless sensor networks. Int. J. Comput. Sci. Issues, 11(3): 92-101.

Patil, U.A., S.V. Modi and B.J. Suma, 2013a. Analysis and implementation of IEEE 802.11 MAC protocol for wireless sensor networks. Int. J. Eng. Sci. Innov. Technol., 2(5): 278-284.

Patil, U.A., S.V. Modi and B.J. Suma, 2013b. A survey: MAC layer protocol for wireless sensor networks. Int. J. Emerg. Technol. Adv. Eng., 3(9): 203-211.

Sasikumar, M. and R. Anitha, 2014. Performance evaluation of heterogeneous-HEED protocol for Wireless Sensor Networks. Int. J. Adv. Res. Comput. Commun. Eng., 3(2): 5555-5558.

Seema, R.G., 2013. A survey on deployment methods in wireless sensor networks. Int. J. Adv. Res. Comput. Sci. Software Eng., 3(7): 540-543.

Shakti, S., 2013. Encryption using different techniques: A review. Int. J. Multidiscipl. Acad. Res., 2(1):1-9.

Sharma, S. and P. Mittal, 2013. Wireless sensor networks: Architecture, protocols. Int. J. Adv. Res. Comput. Sci. Software Eng., 3(1): 303-308.