International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

Design Challenges and Comparative Analysis of Hierarchical Based Routing

Akhil Vaid [1], Harneet Kour Khajuria[2], Loveneesh Talwar[3]
[1]Junior Engineer Power Grid Cooperation of India, India
[2]Department of Electronics & Communication Engineering, YCET, Jammu, India
[3]Department of Electrical Engineering, YCET, Jammu, India
Email address:[3] loveneeshtalwar@gmail.com

***Abstract*—**Wireless Sensor Networks (WSN) are receiving significant importance in the present scenario owing to their unlimited potential and world wide applications. Mostly the network is composed of a number of nodes that are deployed in an extensive area and all nodes are not necessarily connected directly. So in order to relay the data intermediate nodes communicate together there by selecting the suitable routing path in accordance to the routing protocol of the network and then relay the data towards base station. In short the routes in the network are determined by the most secured and energy efficient routing protocols. The most energy efficient routing protocols for WSNs are the Hierarchical or cluster base routing protocols. In this paper different hierarchical routing techniques have been studied and analyzed and further the secured protocols are compared on various criteria's.

***Keywords*—** Hierarchical (cluster based); routing security; wireless sensor networks (WSNs).

I. PAPER DESCRIPTION

Wireless Sensor networks are emerging as a new tool in various fields The Routing protocols in wireless sensor networks (WSNs) are mainly classified in two categories:-network structure and protocol operation. This paper imparts knowledge and better understanding of different hierarchical routing protocols along with their working principle, advantages and limitations. The readers will learn that, it is the special advantage of scalability and efficient communication which makes the hierarchical routing concept employed in wireless sensor networks for the perfect energy efficient routing. It also gives a detailed account of different security considerations while designing hierarchical cluster based and chain based routing protocol for a wireless sensor network.

II. INTRODUCTION

Wireless Sensor Networks (WSNs) are formed of a set of nodes that intend to gather information and forward it to sink. These networks are formed by small, inexpensive and resource limited devices that have ability to communicate with other devices in a wireless manner [1].Wireless Sensor networks are applicable in various fields such as habitat monitoring in nature preserves, surveillance of buildings as well enemy activities in battle field etc. At the darker side wireless sensor networks (WSNs) poses a problem in research as a challenge due to their high flexibility supporting several real world applications which further makes global technical solution difficult to define [2]. The WSN protocols are different from the traditional wireless protocols in view of their large network size, limited power supply and inaccessible remote deployment environment. The Routing protocols in wireless sensor networks (WSNs) are mainly classified in two categories:-network structure and protocol operation. Network structure is further classified into Flat, hierarchical and location based routing. On the other hand Protocol operations are further classified into negotiation, multi-path query; QOS and coherent based routing that are useful in computation of path routing and highly affect the performance of the wireless sensor networks. This further indicates that in order to balance the load among the sensor nodes and prolonging the lifetime of a network, the development of these routing protocols is necessary.

A. Basis of Hierarchical Routing Protocol

In a sensor network the nodes are severely constrained by energy, storage capacity and path computation power so the designing of energy efficient routing protocol is critical in order to prolong the lifetime of the sensor network nodes. A large number of protocols have been developed to make the wireless sensor networks practically applicable and efficient [4]. These Routing protocols intend to make the constituent network nodes to work in unison to achieve a specific task or multiple tasks in order to minimize energy expenditure and maximize the network lifetime. The routing protocol of sensor networks is typically partitioned into two sub routings:-Flat routing protocol and Hierarchical routing protocol. In order to avoid the duplicated data transfers, the sensor network nodes performs a process called Data aggregation process. The sequence of such processes forms the basis of hierarchical routing protocol based upon clusters since the efficient selection of cluster heads can reduce the power consumption and hence maximizing the lifetime of the sensor networks further [5]. Since most of the hierarchical routing protocols aim to be developed as energy efficient, the security issues are not given much importance most of the times. But in certain applications such as military the data is to be maintained secret while communicating between sensor nodes and basin so security issues are also required to be focused in developing routing protocols. Keeping in view the security issues, this paper tends to discuss and analyze the advantages and limitations of secure hierarchical protocols techniques developed till now.

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, "Design challenges and comparative analysis of hierarchical based routing", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

III. Background

Generally the routing protocols proposed for communication networks proposed are based mainly on network architecture and applications but when it comes to the wireless sensor networks the design objective for research is to obtain the design algorithm that results in the optimal tradeoff between the energy consumption, latency and the data rate. While studying various routing protocols and their applicability to communication networks, we came across the study of routing protocols applicability to the wireless sensor networks and figure out the difference between their applicability and routing when compared to conventional communication networks which further created interest in study of different routing protocols in wireless sensor networks which is classified further as chain based hierarchical routing protocols and cluster based hierarchical routing protocols. In this paper a summary of these hierarchical routing protocols along with their applicability, advantages and limitations as well as various security issues to be considered is made which throws light and help better to understand the various routing protocols applied to sensor networks and how they differ from simple routing protocols and contemporary communication networks.

IV. Wireless Sensor Network Vs Contemporary Communication Network

Sensor networks routing being differs from contemporary communication as well as wireless ad hoc networks in view of following challenging characteristics:-

- Global addressing for the deployment of sheer number of sensor nodes is not possible.
- In sensor networks, the flow of sensed data from multiple regions i.e. sources to a particular sink i.e. command center is required in almost all applications which is contrary to typical communication network.
- Significant redundancy is present in the generated data traffic since multiple sensors may generate same data within the vicinity of a phenomenon.
- Sensor nodes require careful resource management since they are constrained tightly in terms of transmission power, on board energy, processing capacity and storage [11], [3]

V. Hierarchical Routing

The aim of the hierarchical routing is to maintain the energy consumption of sensor nodes efficiently either by allowing multi hop communication within a cluster and then performing data aggregation and fusion thereby intending to decrease the number of transmitted messages to sink and further allowing the system to cope up with additional loads there by enabling it to cover a large area of interest without degrading the service.

A. Various Hierarchical Routing Protocols

The use of hierarchical cluster based routing algorithm (micro) extends the life time of the sensor networks and maintains the balance of power consumption by sensor nodes A first level clustering algorithm based on the heed algorithm is executed first by all the nodes in the sensor network and only the first level cluster heads participates in the second level election which uses a new approach for calculation of cluster head probability which are used to cluster the network into rounds only and as per the conventional approach the algorithm terminates in six rounds only thereby reducing the energy or power consumption. The cluster based routing employed in wireless networks are well known techniques with the special advantage of scalability and efficient communication which makes the hierarchical routing concept employed in wireless sensor networks for the perfect energy efficient routing. In this hierarchical routing architecture the higher energy nodes are used to process and send the information and the lower nodes are used to perform the sensing operation in the vicinity of the target. The advantages like overall system scalability, lifetime of the network and energy efficiency owes to the formation of clusters and further assigning special tasks to the cluster heads. In other words it can be inferred that hierarchical routing is an efficient way to reduce the energy consumption within the cluster formed and by performing the data aggregation and fusion there by reducing the number of transmitted messages to the base station. Hierarchical routing is the two layers routing where one layer is used to select the cluster heads and the other layer is used for routing [7], [12].

Leach (Low Energy Adaptive Clustering Hierarchy)

LEACH is a hierarchical cluster based routing protocol for sensor networks introduced by Heinemann et al [6] .It includes distributed cluster formation followed by random or stochastic selection of few network nodes as cluster heads (chs). In this cluster protocol the cluster head role is transferred periodically among the network nodes in such a way that the energy consumption or energy load is evenly distributed as well. Working Principle: In this clustering protocol, the data arriving from nodes inherent in a cluster is compressed by the respective cluster heads nodes and then transmitted to base station as aggregated packet thereby reducing the amount of information to be transmitted.

Advantage and limitation: The advantage associated with LEACH protocol when applied for routing in wireless sensor network is that it extends the network lifetime and assumes:
$T(n) = p / [1 - p \times (r \bmod p-1)]$
$T(n) = 0$
Where n is random no. between 0 and 1, P is the cluster head probability, G is the set of nodes that weren't cluster heads the previous round,
If $n < T(n)$, node becomes a cluster-head. The amount of energy depletion by data transfer is given as:
The energy being dissipated to run the transmitter: Eelec
The energy dissipated by the transmission amplifier: ξamp
Transmission cost: $ETx(K, d) = Eelec + \xi amp\ kd\lambda$
Receiving costs: $ERx = Eelec\ k$
Where k is the length of the message in bit, D is the distance between nodes, and λ represents the path loss exponents.

The performance of LEACH ROUTING PROTOCOL depends on rounds and for each round a cluster head is elected which uses both the number of nodes except those used as cluster heads and the percentage of cluster heads used in a

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, "Design challenges and comparative analysis of hierarchical based routing", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

network for its election. After the cluster head is defined in a set up phase, the cluster head further establishes a TDMA schedule for the transmission of data in its cluster there by allowing other nodes to switch off their interfaces when they are not employed in its cluster as specified by this scheduling. This cluster head acts as a router to its sink and is also responsible for the data aggregation process. The cluster head also reduces the redundancy as the sensors located in the close area are controlled by the cluster head. A modified version of this protocol is known as LEACH-C (or LEACH Centralized) which is also based on the time rounds which are further divided into set up phase and the steady phase. In the set up phase the sensors inform the base station about their positions and their energy levels. This version has a deterministic threshold algorithm, which takes into account the amount of energy in the node and/or whether or not the node was recently a cluster-head. This information is used by the base station to decide the structure of clusters and corresponding cluster heads in each cluster. The cluster structure obtained as a result of LEACH-C is considered as an optimization of results of LEACH protocol since the complete status of the network is acknowledged by the base station [2], [3].

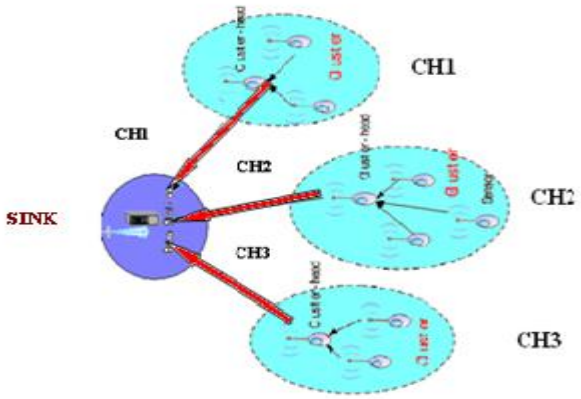

Fig. 1. Cluster architecture of leach.

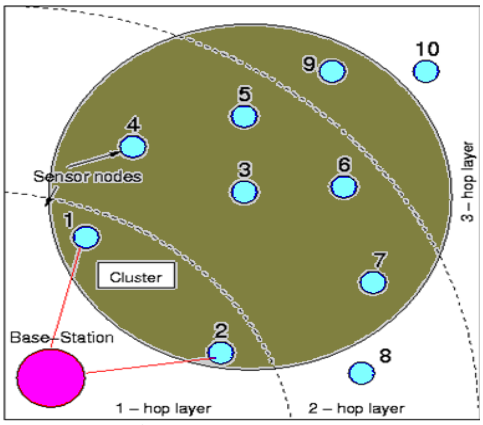

Fig. 2. Layer architecture of leach.

T (n) new = p E n_current / [1 - p × (r mod p-1)] E n_max
Where E n_current is the amount of current energy, E n_max is the initial amount of energy.

$$T(n)_{new} = \frac{P}{1 - P \times (r \bmod P^{-1})}\left[\frac{E_{n\_current}}{E_{n\_max}} + (r_s \operatorname{div} P^{-1})\left(1 - \frac{E_{n\_current}}{E_{n\_max}}\right)\right]$$

PEGASIS (Power-Efficient Gathering in Sensor Information Systems)

To overcome the limitations of LEACH, an enhancement over leach protocol gave birth to another hierarchical routing protocol called PEGASIS introduced by Lindsey and Raghavendra [7]. PEGASIS is a near optimal chain based protocol developed assuming that to increase the network life time, the nodes in the network need only to communicate with their closest neighboring nodes and then they take turns while communicating to the base station. Whenever the round of all nodes communicating with the base station ends, a new round will start and this continues. This help reducing the power consumption required to transmit data per round since the power draining is spread uniformly over all nodes. PEGASIS was developed with two prime objectives:

- Increasing network lifetime which is accomplished by increasing the lifetime of each node in the network using collaborative techniques.
- Reduction in bandwidth consumption while communicating by allowing only local coordination between the closer nodes in the network [1], [2].

Working principle: PEGASIS uses only one node in a chain instead of multiple nodes to transmit data to base station and avoids the cluster formation unlike LEACH. The data aggregation is performed by the node and is forwarded to the node in the chain that communicates with the sink. In each round one node in the chain is elected to communicate with the sink that is the chain is constructed with a greedy algorithm in two steps:

Chain construction: The chain is constructed using the greedy algorithm approach starting from the node that is farthest from the base station. Each node also adjusts its signal strength so that only node to which it communicates receives the message.

Gathering data: Chain is constructed then the leader of each round is selected stochastically as if number of nodes is N, then I MOD N is selected as the head node for I round. This random selection of head nodes provides the robust network since the nodes likely die at random locations and hence whenever a node dies the chain is reconstructed bypassing the dead node. Data gathering is initiated by token passing after selecting leader which requires small energy consumption due to small sized token. In a particular round the head node passes the token to the closest node which initiates transmitting data to next

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, "Design challenges and comparative analysis of hierarchical based routing", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

connected node in the chain where data is fused and then transmitted to succeeding node and so on until all the fused data is received at the head node. The head node then transmits the fused data to the base station. Each node in the network is selected at least once to function as a head node. Each node transmit and receives a single packet in each round and waits until it receives the data from the previous node before transmitting its own data, thus called data gathering.

Advantage and limitation: PEGASIS capable of extending network lifetime of the network twice the amount when compared to lifetime extended by LEACH protocol that is improves the performance gain by eliminating the dynamic cluster formation overhead as in LEACH and by data aggregation thereby reducing number of transmissions and receptions..PEGASIS requires dynamic topology adjustments to know about the energy status of its neighbor to know where the data is to be routed which in turn introduces significant overhead especially in highly utilized networks, which creates delay. In order to reduce the delay simultaneous transmissions are pursued which lead to HIERARCHICAL–PEGASIS, an extension to PEGASIS which tends to decrease the delay incurred during packet transmissions to the base station by using Energy-delay metric to solve data gathering problems [5], [7].

TEEN (Threshold sensitive Energy Efficient sensor Network protocol)

TEEN is considered as the hierarchical protocol specially formulated for reactive networks since it responds quickly to the changes in the relevant parameters. In TEEN protocol the cluster head sends two threshold values a hard value and a soft value. The nodes sense their environment continuously and when a parameter from the attribute set reaches its hard threshold value for the first time, the node switches on its transmitter and sends its data. The nodes then transmit this data in the current cluster period if following conditions are satisfied: 1) the current value of the sensed attributes is greater than the hard threshold value.2) Current value of sensed attribute differs from sensed value by an amount equal to or greater than the soft threshold value. Both of these strategies aims to reduce the energy consumption while transmitting messages. But it has limitation that the nodes will never communicate if the threshold values are not reached and the user will not get any data from the network and will not know even if the nodes die. In short this protocol is not suitable for the applications where the user needs to get data on a regular basis. [2], [5], [6].

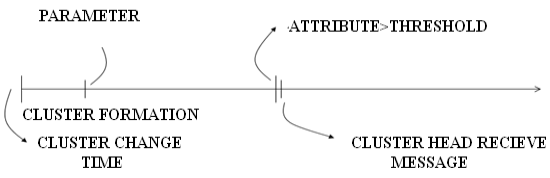

Fig. 4. Time line for teen.

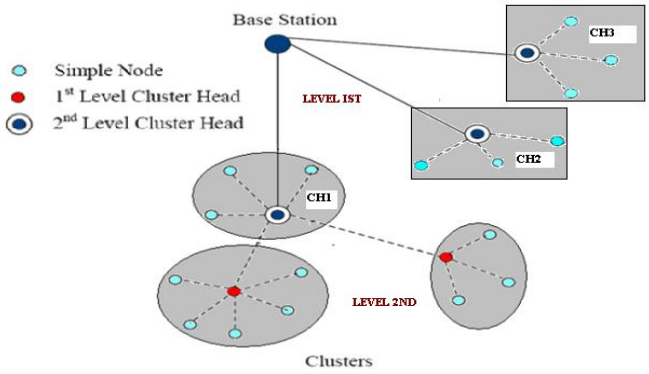

Fig. 5. Hierarchical clustering in teen and apteen.

Adaptive Threshold Sensitive Energy Efficient Sensor Network Protocol (APTEEN)

It is developed with a goal to capture periodic data collection as well as reacting to time critical events and supports three different query types historical, used to analyze the past values of data one time, used to make a snapshot view of network and then persistent , in order to monitor an event for a period of time.[8] Which enable to overcome the two limitations overhead and complexity in case of cluster formation at multiple levels by implementing threshold based functions and dealing with attribute based naming of queries. In APTEEN protocol, the following parameters are broadcasted by the cluster heads:

- *Attribute (A)*: it is set of the physical parameters used to obtain user interest data.
- *Thresholds (ST)*: includes hard threshold value (HT) and a soft threshold value (ST).
- *Schedule*: A slot is assigned to each node depending on TDMA scheduling parameter.
- *Count time (CT)*: Maximum time period between two successive reports sent by a node.

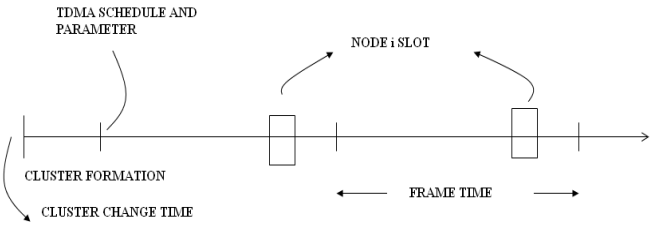

Fig. 6. Time line for apteen.

Working principle: Node keeps on sensing the environment continuously and only those nodes that sense data value at or beyond the hard threshold (HT) participate in the transmission. If the sensed data is beyond the threshold value the node transmits data only when that attributes changes by an amount greater than the soft threshold value (ST). The node is forced to sense and retransmit the data, if it does not send data for a time period equivalent to the count time. Each node in the cluster is assigned a transmission slot using TDMA schedule.

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, “Design challenges and comparative analysis of hierarchical based routing”, *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

Advantages and limitations: APTEEN algorithm considers combination of both proactive and reactive policies and allows the user to set the count time (CT) and the threshold values for the attributes thereby providing greater flexibility and control over energy consumption is obtained by changing the count time as well as the threshold values. But the limitation acquired in this routing protocol is its additional complexity which is required to implement the threshold functions and the count time. The main drawback of the scheme is the additional complexity required to implement the threshold functions and the count time [2], [5], [9].

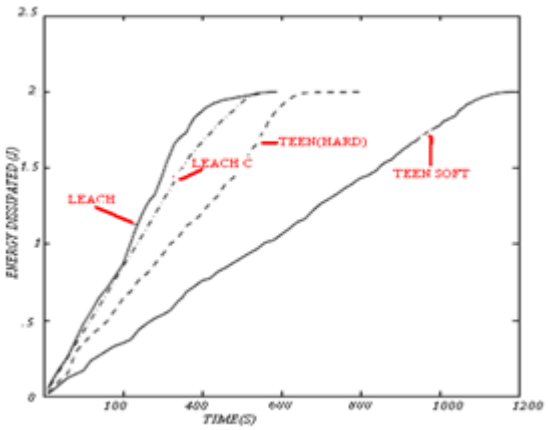

Fig. 7. Comparasion of average enrgy dissipated.

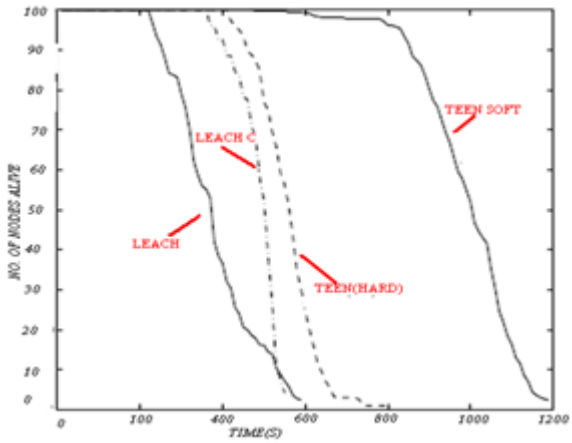

Fig. 8. Comparasion of no. of nodes alive.

Energy-Aware Routing Protocol

In this routing algorithm cluster heads are less energy constrained than the sensors and are named gateways. The location of sensor nodes are assumed by the gateways that tend to maintain the status of the sensors and sets up multi hop routes for collection of the sensor data which is send from nodes to gateways using a TDMA based MAC protocol. Each node is informed by the gate way about the slots in which it should listen to other nodes transmission and also slots which it can use for its own transmission. The sensor is operable at low power standby mode or active mode that is one of following four states in a cluster:

- *Sensing state*: when nodes probe the environment and generate the data at constant rate.
- *Relaying state*: here the node communication circuitry is switched on in order to relay the data from the other active nodes.
- *Sensing relaying state*: A node is in this state when a node is sensing as well as relaying the data messages from other nodes.
- *Turn off state*: the node gets inactive and its sensing and communication circuitry can be turned off by the node.

The gateway tends to monitor the available energy level at every active sensor active for data processing, sensing and relaying data packets. Cost function, defined between two nodes in terms of energy consumption, delay optimization and other performance metrics is used as a link cost to determine the least cost path between the sensor node and the gateway [2], [3].

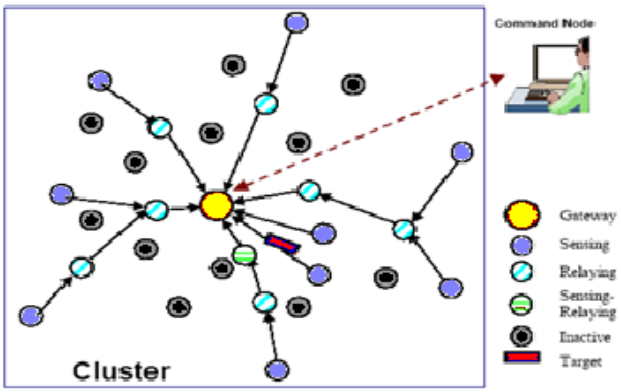

Fig. 9. Energy-aware routing for cluster-based sensor networks.

Self Organizing Rouing Protocol

The backbone of communication constitutes of the stationary router nodes or simply the routers through which the collected data is forwarded to more powerful sink nodes. Moreover the sensing nodes can be identified through the address of the routing node it is connected to. The routing architecture is hierarchical. The SELF ORGANIZING algorithm organizes the router nodes thereby creating routing tables. The routing tables further consist of four phases as follows:

- *Discovery phase*: in which nodes in the neighborhood are discovered.
- *Organization*: group formations and merging to form a hierarchy.
- *Maintenance phase*: updating of routing tables and energy levels of the node as well.
- *Self-reorganization phase*: group reorganizations occur in case of node failures.

Working principle: This algorithm utilizes the router nodes and forms a dominating set in order to keep all the sensors connected thereby reducing energy consumption since requires limited subset of nodes.

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, "Design challenges and comparative analysis of hierarchical based routing", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

Advantage and limitation: Small cost is the major advantage since it requires just maintaining the routing table and balancing strictly the routing hierarchy. The limitation of this algorithm is that introduction of extra overhead in organization phase of the algorithm which is continuous and no based on demand which needs more energy. Also when there exist many cuts in the network during hierarchy formation the use of his protocol for routing is limited [3].

VI. Security Goalsin WSNs

Conventionally, security is achieved if every eligible node receives all the messages intended to them. The significance of security holds in presence of the resourceful adversary in present scenarios and security goals guarantees the confidentiality, integrity, authenticity etc as follows:

- *Confidentiality*: While communicating in the network the data should be understood by the intended recipient only that is the data should not leak by the sensor nodes to the other networks. Confidentiality is achieved by the standard technique like cryptography.
- *Integrity*: This means that the data should reach the intended destination without any alteration and also that no adversary can manipulate the communicated data since the data loss can occur even due to the communication environment. Message digest and Mac are such techniques to maintain the integrity of the data. [11], [14].
- *Authenticity*: Data authentication is necessary for maintaining the network, coordinating with the sensor node and sending or receiving the data. It is essential for receiver to ensure the message originated from the correct source and allows receiver to verify that the sent data is authentic i.e. send from the authorized user.
- *Availibility*: It is required to ensure that the services of the network are available always even in the presence of internal and external attacks such as a denial of a service attack i.e. DOS.
- *Freshness*: It ensures that the receiver receives the recent and fresh data and also that no adversary can replay the old data significantly in WSNs where shared keys are used by nodes for message communications. The mechanisms like nonce and time stamp are added to each packet in order to achieve he freshness of data.

VII. Attacks on Routing Protocols

As discussed earlier most of the wireless sensor networks are developed with energy efficiency as the main goal there by skipping the security issues in mind which can result in various attacks by the consequent adversaries in the network and the main sufferer is the network layer protocol that is the routing protocol. These attacks include spoofing or altering the route information, selective forwarding, sinkhole attack, wormhole attack and even the Sybil attacks and many more like hello flood attack etc. [7]

- *Spoofing or altering or replay the route information*: It includes the routing information corruption launched by an adversary which can attract or redirect the route information there by increasing the traffic as well. This latency further generates routing loops and creates false errors [10], [11], [14]
- *Selective forwarding attack*: In this mode of attack the malicious node refuses to forward certain packets and drop them simply. If an adversary causes the dropping of the entire received packet, the attack is called a black hole attack and the adversary includes explicitly the path of the data flow to perform the selective forwarding.
- *Sinkhole and wormhole attack*: In both of these attacks the adversaries tries to attract whole traffic from a particular area by means of a compromising node. Sinkhole attack works mainly by making this compromised node look more attractive to the neighbor nodes in order to route the data packets and hence spoofing or dropping the packet there by resulting in various attacks such as selective forwarding, black hole attack or tempering.. Wormhole attack is caused by an adversary and uses two malicious nodes that try to attract the traffic by showing one hop distance to the sink [16].
- *Sybil attack*: The Sybil attack is a great threat to many geographic and multipath routing protocols. It employs a single node that presents further multiple identities to the other nodes in the network thereby misleading the node in the neighbor detection, route formation and topology maintenance.
- *Hello flood attack*: The hello flood attack affects the routing protocols that employ local topology like neighbor information for route creation and topology maintenance etc. In this attack an adversary rebroadcasts overhead packet with enough power to be received by every node in the network.

VIII. Secure Hierarchical Routing Protocols

Many previous hierarchical routing protocols assume a safe and secure environment where all sensor nodes cooperate with no attack present. But the real world environment is totally opposite; there are many attacks that affect the performance of routing protocol. Attacker use different kinds of technique to launch attack and damage or harm the data and the network. In order to secure the hierarchical routing protocol many works have been proposed. We tabulated the basic protocol, energy efficiency and security keys respectively in table 1 and table 2 [10].

Table 1: Analysis of secure routing protocols

Secure protocol	Basic protocol	Energy efficiency
LHA-SP		Medium
F LEACH	LEACH	Medium
SLEACH	LEACH	Medium
SHEER		Good
NHRPA		Good
Ss LEACH	LEACH	Good
R.srinath et al.	LEACH	Medium
Sec LEACH	LEACH	Medium
R LEACH	LEACH	Medium

Table 2: Evaluation of secure routing protocols on security mechanism

Secure protocol	Asymmetric key	Symmetric key	Pairwise key	MAC
LHA-SP		✓	✓	
F LEACH		✓		
SLEACH		✓		✓
SHEER		✓		
NHRPA				
Ss LEACH		✓		
R.srinath et al.	✓	✓		
Sec LEACH		✓		
R LEACH	✓	✓	✓	

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, "Design challenges and comparative analysis of hierarchical based routing", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

IX. CONCLUSION

The Wireless sensor networks employs hierarchical routing protocols for the data communication which is cluster based. Most of them are developed keeping energy efficiency as the main goal and few with security issues in mind for applications such as military etc as discussed before. Since the performance of such networks is determined in form of energy efficiency, security, lifetime of the network and resiliency which are further affected by the routing protocols so the efficiency of such sensor networks depends upon the secure robust and efficient routing protocol chosen for the network. In this paper light is thrown on a number of energy efficient and secured hierarchical routing protocols that have been discussed and analyzed for wireless sensor networks which may prove beneficial to understand the significance of chain based hierarchical routing protocols in the present scenario in context with the wireless sensor networks.

REFERENCES

[1] M. J. Handy, M. Haas, and D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," *IEEE 4th International Workshop on Mobile and Wireless Communications Network*, pp. 368 – 372, 2002.

[2] D. Song, "Probabilistic modeling of leach protocol and computing sensor energy consumption rate in sensor networks," 2005.

[3] Kuan-Ta Lu and Q. Wu, "A survey on routing protocols for wireless sensor networks," 2010.

[4] S. Lindsey and C. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," Computer Systems Research Department The Aerospace Corporation, Los Angeles, CA.

[5] A. Manjeshwar and D. P. Agrawal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," *IEEE Proceedings 15th International Parallel and Distributed Processing Symposium*, pp. 2009 – 2015, 2000.

[6] S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks," M.Tech thesis, Department of Computer Science and Engineering National Institute of Technology Rourkela, Orissa, India, 2009.

[7] M. Ilyas and I. Mahgoub, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, by CRC Press, 2004.

[8] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. *"uAMPS ns Code Extensions"*.

[9] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," *In Proceedings of Hawaiian International Conference on Systems Science*, 2000.

[10] B. Heinzelman. "Application-specific protocol architecture for wireless networks," PhD thesis, Massachusetts Institute of Technology, 2000.

[11] Hong-bing, Y. Geng, and H. Su-jun, "NHRPA: A novel hierarchical routing protocol algorithm for wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, issue 3, pp. 75–81, 2008.

[12] J. Ibriq and I. Mahgoub, "A secure hierarchical routing protocol for wireless sensor networks," *In Proceedings 10th IEEE Singapore International Conference on Communication Systems*, pp. 1–6, 2006.

[13] S. Jung, Y. Han, and T. M. Chung, "The concentric clustering scheme for efficient energy consumption in the pegasis," *In Proceedings 9th International Conference on Advanced Communication Technology*, vol. 1, pp. 260–265, 2007.

[14] C. Karlof and D.Wagner, "Secure routing in sensor networks: attacks and countermeasures," *Ad Hoc Networks*, 1, pp. 293–315, 2003.

[15] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," *In IEEE Aerospace Conference Proceedings*, vol. 3, pp. 1125–1130, 2002.

[16] V. Loscri, G. Morabito, and S. Marano, "A two-level hierarchy for low-energy adaptative clustering hierarchy (tl-leach)," *In Proc. VTC2005,*, Dallas (USA), pp. 1809–1813, 2005.

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, "Design challenges and comparative analysis of hierarchical based routing", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.

ISSN: 2454-1532

Akhil Vaid, Harneet Kour Khajuria and Loveneesh Talwar, “Design challenges and comparative analysis of hierarchical based routing”, *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 59-65, 2015.