Study of Secure and Energy Efficient Hierarchical Routing Protocols in WSN

Roopashree H. R.
Research Scholar Christ University
Bangalore, India

Dr. Anita Kanavalli
Professor
Department of Computer Science and Engineering
MS Ramaiah Institute of Technology Bangalore, India

***Abstract*— In the advent of wireless networking, wireless sensor network (WSN) has been a constant target of research due to its potential data aggregation techniques in hostile and unsecured environment. Currently, wireless sensor network is still more under research and development and less on commercial deployment when it comes to security and energy efficiency. The past research work has witness massive volumes of algorithms using various sophisticated technologies in order to mitigate the issues of energy problems in sensor motes, however, till date none of the prior studies has yet been standardized and hence the issues of unwanted power depletion still persist because of numerous unsolved factors. This manuscript will review some of the most standard secure and energy efficient routing protocols and extracts research gap from the study.**

Keywords-component; Wireless Sensor Network, Security, battery, Energy Efficiency, LEACH

I. INTRODUCTION

The area of wireless sensor network has exhibits its potential features in the communication purpose. The wireless sensor network comprises of sensor nodes deployed in the area which are required to be monitored for certain activity of human interest [1]. The sensor nodes are small miniature electronic device that has the capability to sense certain physical attributes like water, heat, pressure, motion, smoke and many more attributes. These attributes are usually collected the sensor nodes using TDMA scheduling mechanism. There are various applications of wireless sensor network right from habitat monitoring to forest fire detection. The applications are either designed for small scale or for large scale area. However, the wireless sensor network is also found with certain flaws that has attracted the attention of the research community. A sensor node is usually smaller in size with less computational and storage capabilities. Hence, when the research work is carried out, such issues are usually not visualized in correct sense by the developers or the researchers for which reason, the evolved technique or the algorithm could not be benchmarked properly. It was also explored that energy is one of the biggest impediment in superlative performance of the routing protocols in wireless sensor network [2][3]. If the energy is depleted, it gives rise to unstabilized links that finally yields to degradation of the performance of either data aggregation process or network lifetime enhancement process. It is quite evident that right from node deployment phase to cluster formation phase, the network needs to be designed in such a way that it really optimize each and every constraints of the system for yielding better results. Also, it was seen from the literature that majority of the studies in the energy efficient routing is based on on-demand routing protocols as such routing protocols are highly capable of conserving energy considering the existing constraints of the sensor node. Hence, a better version of algorithm is required that can ensure cumulative network lifetime with computational capabilities. In this paper, we are discussing about an open issues in wireless sensor network i.e. energy efficiency of hierarchical routing protocols. Although there are many other categories of routing protocols, but we restrict our discussion in hierarchical routing techniques as it was seen that majority of the prior studies on energy efficiencies are designed on the top of hierarchical routing protocol. We are curious to understand what the significant and standard energy efficient routing protocols are and what its limitations are. Hence, to answer this question, this paper will collect only the standard papers, where some significant contributions were witnessed. We have also collected the most recent studies being undertaken to ascertain this fact and to explore the research gap in this field. Finally, we discuss about the most recent trend of adopting secure and energy efficient routing technique optimizing the routing performance and thereby enhancing the cumulative network lifetime of the wireless sensor network. The prime purpose of the paper is to enable the reader about the most recent and significant studies being done in the area of energy efficiency as well as security. The study discusses about the various standard routing protocols that ensures security as well as energy efficiency. This paper discusses about various energy efficient techniques on hierarchical routing protocols along with their classification and finally the paper also discusses about security technique and their strategical formulation. The paper finally extracts the research gap in this field, which will motivate the readers to select the routing protocols wisely for their future studies. It is also expected that the outcome of the study will generate some significant survey results which can be referred for benchmarking purpose. Section 2 discusses about the routing protocols in WSN, Section 3 discusses about the security issues in WSN followed by brief discussion on existing secure and energy efficient routing protocols in Section 4. Section 5 discusses about the research gap, while section 6 makes some concluding remarks.

II. ROUTING PROTOCOLS IN WSN

The sensor nodes are constrained to limited resources itself, so the main target is to design an effective and energy aware protocol in order to enhance the network lifetime for specific application environment. Since sensor nodes are not given a unified ID for identification and much redundant data collected at destination nodes. So, energy efficiency, scalability, latency, fault-tolerance, accuracy and QoS are some aspects which must be kept in mind while designing the routing protocols in wireless sensor networks. Classically most routing protocols are classified as data-centric, hierarchical and location based protocols depending on the network structure and applications. All major routing protocols classified into main categories discussed below:

A. Location Based Protocols:

The location information based routing protocol uses location information to guide routing discovery and maintenance as well as data forwarding, enabling directional transmission of the information and avoiding information flooding in the entire network [4].

- **Geographical and Energy Aware Routing (GEAR)**: In this algorithm [5], each node keeps an estimated cost and a learning cost of reaching the destination through neighbors. The estimated cost is a combination of residual energy and distance to destination. Hole occurs when a node does not have any closer neighbors to the target. If there are no holes, the estimated cost equal to the estimated cost is equal to the learned cost. The learned cost is propagated one hop back every time a packet reaches the destination so that route set up for next packet will be adjusted.
- **Geographic Adaptive Fidelity (GAF):** GAF [6] is used for WSN because it favors energy conversation. The state transition diagram has three stages, discovery, active and sleeping. When a sensor enters the sleeping state, it turns off radio for energy saving .In discovery state, a sensor exchange discovery messages to learn about other sensors in the grid. In active state, a sensor periodically broadcast its discovery message to inform equivalent sensors about its state.
- **MECN and SMECN**: Minimum energy communication network set up and maintains a minimum energy network for wireless networks by utilizing low power GPS. This protocol has two phases: 1) It takes the positions of a two dimensional plane and constructs a sparse graph, which consists of all the enclosures of each transmit node in the graph. The enclose graph contains globally optimal links in terms of energy consumption. 2) Finds optimal links on the enclosure graph. It uses distributed shortest path algorithm with power consumption as a cost metric. The small minimum energy communication network (SMECN) is an extension to MECN. In SMECN protocol; every sensor discovers its immediate neighbors by broadcasting a discovery message using some initial power that is updated incrementally [7].

B. Data Centric Routing Protocols:

In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. Here data is usually transmitted from every sensor node within the deployment region with significant redundancy.

- **Flooding and Gossiping**: Flooding and gossiping [8] are the most traditional network routing. They do not need to know the network topology or any routing algorithms. In flooding mechanism, each sensor receives a data packet and then broadcasts it to all neighboring nodes. When the packet arrives at the destination or the maximum number of hops is reached, the broadcasting process is stopped. On the other hand, gossiping is slightly enhanced version of flooding where the receiving node sends the packet to randomly selected neighbors, which pick another random neighbor to forward the packet to and so on.
- **Sensor Protocol for Information via Negotiation (SPIN):** Joanna Kulik et al. in [9] proposed a family of adaptive protocol, called SPIN (Sensor Protocol for Information via Negotiation) that efficiently disseminate information among sensors in an energy-constrained wireless sensor network and overcome the problem of implosion and overlap occurred in classic flooding. Nodes running a SPIN communication protocol name their data using high-level data descriptors, called metadata. SPIN nodes negotiate with each other before transmitting data. Negotiation helps to ensure that the transmission of redundant data throughout the network is eliminated and only useful information will be transferred.
- **Directed Diffusion**: Ramesh Govindan et al. in [10] proposed a popular data aggregation paradigm for wireless sensor networks called directed diffusion. Directed diffusion is data-centric and all nodes in a directed diffusion-based network are application-aware. This enables diffusion to achieve energy savings by selecting empirically good paths and by caching and processing data in network (e.g. data aggregation). The main advantages of directed diffusion are: 1) Since it is data centric, communication is neighbor-to-neighbor with no need for a node addressing mechanism. Each node can do aggregation and caching, in addition to sensing. Caching is a big advantage in term of energy efficiency and delay. 2) Direct Diffusion is highly energy efficient since it is on demand and there is no need for maintaining global network topology.
- **Rumor Routing**: Rumor routing is proposed in [11], which allows queries to be delivered to events in the network. It is mainly determined for context in which geographic routing criteria is not applicable. Rumor

routing is a logical compromise between flooding queries and flooding events notification. Rumor routing is tunable and allows for tradeoff between setup overhead and delivery reliability.

- **Gradient-Based Routing**: The algorithm makes an improvement on Directed Diffusion, in order to get the total minimum hop other than the total shortest time. In the traditional gradient minimum hop count algorithm, hop count is the only metric, which measures the quality of route. Li Xia [12] gradient routing protocol which not only consider the hop count but also energy of each node while relaying data from source node to the sink. This scheme is helpful in handling the frequently change of the topology of the network due to node failure. A new gradient routing scheme also aims path from the source node to the sink.

C. Hierarchical protocols:

Hierarchical clustering in WSN is an energy efficient protocol with three main elements: sensor nodes (SN), Base station (BS) and Cluster Heads (CH). The SNs are sensors deployed in the environment to collect data. The main task of a SN in a sensor field is to detect events, perform quick local data processing, and transmit the data. The BS is the data processing point for the data received from the sensor nodes, and from where the data is accessed by the end-user. The CH acts as a gateway between the SNs and BS. The CH is the sink for the cluster nodes, and the BS is the sink for the cluster heads. This structure formed between the sensor nodes, the sink and the base station can be replicated many times, creating the different layers of the hierarchical WSN.

- *Low Energy Adaptive Clustering Hierarchy* (LEACH): This is one of the most frequently studied routing protocols for any research work aiming at energy efficiencies. The model was introduced in 2000 and has considered designing an effective radio and energy model, which is highly adopted even in current studies. LEACH [13][14] algorithm considers homogenous wireless sensor network where the base station is located in the center of the simulation area and surrounded by multiple clusters. The selection of the cluster head is always done depending on the highest residual energy. The cluster head uses TDMA scheduling to aggregate the physical data from the member nodes on one cluster. The entire operation of the LEACH is carried out using set up phase and steady phase. The energy depletion is controlled by reducing the cost of communication between the member node and cluster head using sleep scheduling algorithms. Hence, lifetime of the network is maximized in LEACH.
- **Power-Efficient Gathering in Sensor Information Systems (PEGASIS):** Just like HEED, it is also an enhanced version of LEACH routing protocol where the outcome shows that energy efficiencies capabilities are doubled up even compared to conventional LEACH [15]. The aggregated data are not forwarded to base station directly, inspite, the aggregated data are transmitted through a communication channel to the neighbor networks, which is finally forwarded to the base station. The phenomenon of cluster formation is evaded in PEGASIS and considers that all the sensor nodes have prior information about the wireless sensor network using greedy algorithm
- **Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN):** This is another hierarchical routing protocol mainly designed for mission critical requirements in any applications in reactive networks [16]. The aggregated data from the cluster head is forwarded to the upper level of clusterhead and this phenomenon is continued for all the clusters until the forwarded data reaches base station. TEEN maintains energy conservation by occasionally using threshold base approach forwarding the unique data (although the member node spontaneously generates the data to the cluster head).
- **Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol (APTEEN):** It is an enhanced version of conventional TEEN protocol primarily targeting at periodic collection of physically sensed data from member node and promptly responding in mission / time critical applications [17]. The selection of the clusterhead is almost like that of LEACH protocol. APTEEN also used enhanced TDMA scheduling thereby allocating a precise slot for transmission for preventing data redundancies.
- **Hybrid, Energy-Efficient Distributed Clustering**

(HEED): It is an enhanced version of LEACH routing protocols that considers residual power as well as node density as a selection criteria of clusterhead [18], [19]. The outcome of the HEED routing protocol is found with better energy efficiencies even compared to LEACH with better reduction in overhead and maximizing the network lifetime.

- **Clustered Aggregation Technique (CAG)**: Just like TEEN, CAG [20] is primarily designed for the reactive network. All the sensor nodes that sense equivalent physical data are formulated as one cluster and perform operation to check redundancies of data by filtering out unwanted elements thereby reducing the response time. CAG also addresses better storage efficiency and efficient cost of communication. Updated CAG Algorithm [21] is an improvement of CAG algorithm, where the clusters are still formed from nodes sensing similar values within a given threshold, but in this case, the clusters remain as long as the sensor values stay within a given threshold over time(temporal correlation). This ensures that the performance of CAG become independent of the magnitude of sensor readings and network topology. When used in the interactive mode, the protocol alternates query and response phases. Usually, energy Efficient Homogeneous Clustering Algorithm for Wireless Sensor Networks [22] is a algorithm that proposes homogeneous clustering for WSNs that save power and prolongs network life.

Table 1 Summary of Most recent studies in energy efficient routing techniques

Authors	Problem Focused	Techniques Applied	Inference
Xu et al.[23]-2014	Energy efficiency in routing	Density-based Energy-efficient Clustering Heterogeneous Algorithm	-The CH selection procedure is same as conventional
Lee et al.-[24]-2014	Energy efficiency in routing	Energy-Efficient QoS-aware Routing Algorithm	-No evidence of standard benchmarking with significant routing protocols
Zytoune-[25]-2014	Energy efficiency in routing	Time Based Clustering Technique	No evidence of standard benchmarking with significant routing protocols
Poostfroushan et al. –[26]-2014	Energy efficiency in routing	Particle Swarm Optimization Algorithm	-No evidence of standard benchmarking with significant routing protocols -Energy variation is not discussed
Haider et al.-[27]-2014	Energy efficiency in routing	-REECH-ME: Regional Energy Efficient Cluster Heads based on Maximum Energy Routing Protocol with Sink Mobility	-Better network lifetime achieved. --Energy variation is not discussed
Zhang et al.-[28]-2014	Energy efficiency in routing	-distributed energy-efficient unequal clustering routing protocol	- better balance energy consumption, improve energy efficiency and then prolong the network lifetime -Algorithm convergence behaviour not discussed -Multiple hop not addressed
Shu & Wang-[29]-2013	Energy efficiency in routing	An Optimized Multi-hop Routing Algorithm Based on Clonal Selection	-Better performance compared to PEGASIS -No discussion on comparison with LEACH -possible control overheads are not discussed -Result achieved from less simulation rounds
Deng et al.-[30]-2013	Prolong the lifetime of the network.	Balancing Energy Consumption LEACH (BEC-LEACH) protocol	-Result achieved from less simulation rounds -Only 5 clusters are evaluated. -Energy variance is not discussed.
Alia-[31]-2013	Extending Wireless Sensor Network Lifetime	Harmony Search Algorithm	-Energy variance is not discussed. -Result achieved from less simulation rounds -Overheads not discussed
John & Ramson-[32]-2013	Efficient data collection	Energy-Aware Duty Cycle Scheduling	-Not compared with LEACH -doesn't address any optimization.
Zhao & Yang-[33]-2014	prolong the lifetime	LEACH-A	- performs better than the LEACH
Kim et al.-[34]-2014	Optimization	IC-ACO: Inter cluster Ant colony Optimization Algorithm	Selection of CH is just like LEACH
Zungeru et al.-[35] [2013]	Optimization of swarm approaches	-Comparative study of the routing performance of swarm based techniques	Energy aware routing objectives increases the network lifetime

III. SECURITY ISSUES IN WSN

From the past few decades, there is an ongoing research towards solving the security issues in WSN. However, various researchers has come up with various solutions, but majority of them feels that multiple security challenges should be met for providing the optimal security to WSN. The initial research challenges in performing wireless communication establishments among the sensor nodes usually maximized the insecurity factors of the network owing to various security attacks e.g. spoofing, replay attack, eavesdropping, illegitimate access to network, man in middle attack, and denial of service to name few attacks. The second biggest research challenge is the resource constraint sensor nodes along with limited storage and battery life. Because of such limited resources availability in sensor nodes, performing cryptographic mechanism with sophisticated processing of encryption and decryption sometimes creates a large overhead and affects quality of service (QoS). The third critical security issues in WSN are inefficient routing mechanism. Majority of the routing algorithm are design for static network where sometimes the delivery of the packets falls in wrong hand (man-in-middle attack/eavesdropping). Therefore, it can be said that sensor nodes are highly susceptible to physical capture where the nature of tampering the sensor nodes are out of control or out of surveillance for any users. Fourth, designing a secure routing algorithm along with ensuring energy efficient is a big computational challenging design aspect. The next section will discuss about the existing secure routing protocols in WSN.

IV. EXISTING SECURE ROUTING MECHANISM

Accomplishing security in conventional cluster based routing protocols in WSN is specifically challenging task. Major research works have been presented in the past to safeguard the conventional routing protocols. This section discusses some of the significant standard security protocols introduced by the researchers in the past. The comparative analyses of the discussed secure energy efficient routing protocols are shown in Table 1.

- **RLEACH**: It is a secure energy efficient routing technique for conventional WSNs that deploy group key management [36]. The prime aim of the RLEACH is to solve the security issues of conventional LEACH protocol. In RLEACH, the clusters are formulated dynamically and periodically. The algorithm deploys enhanced arbitrary pair-wise key management scheme that deploys the one-way hash chain, symmetric and asymmetric cryptography to ensure security in LEACH. The protocol is designed for mitigating sinkhole attacks, selective forwarding, hello flood attack, and Sybil attacks. The algorithm has the good potential to balance the network security as well as energy consumption.
- **EECBKM:** It is also called as Energy-Efficient Cluster Based Key Management approach in WSNs [37]. The clusters are formulated initially in the network and the cluster leaders are selected based on the coverage, energy cost, and processing capacity. An EBS key set is assigned by the sink to every cluster leader and cluster key to every cluster. The EBS key set contains the pair-wise keys for intra-cluster and inter-cluster communication. The data is made to pass through two phases of encryption during data transmission towards the sink. The keys are distributed to the nodes by the cluster leader prior to communication. Secure channel is established between the nodes and the CH after the key distribution. The algorithm highly mitigates node-capture attacks and efficiently maximizes packet delivery ratio with reduced energy consumption.
- **SHEER**: It is a secure hierarchical energy-efficient

routing protocol [38] that furnishes energy-efficiency and secure communication on the network layer. For key distribution and authentication, securing the routing mechanism, SHEER uses HIKES (Hierarchical Key Establishment System) and also uses a non-deterministic transmission procedure to enhance the network energy performance and lifetime. The protocol highly mitigates Sybil attack and hello flood attack. The sinkhole attack will also fail because the attacker does not possess all keys, required for authentication. However, the protocol doesn’t works against selective forwarding attacks.

- **SecLEACH**: It is a routing protocol for securing node-to-

node communication in LEACH-based networks [39]. The protocol deploys random key pre-distribution, and furnishes security in LEACH. It also introduces symmetric key and one-way hash chain to provide different performance numbers on efficiency and security depending on its various parameter values. However, the routing protocol is susceptible to key collision attacks.

- **SS-LEACH**: it is another enhanced version of LEACH

algorithm [40] that emphasizes the energy efficiency and security. The protocol formulates dynamic stochastic multipath cluster leader chains by deploying sensor nodes self-location technology and key predistribution tactics.
Therefore, it potentially enhances the energy-efficiency. The protocol mainly mitigates selective forwarding, Sybil attack, and hello flooding.

- **NSKM:** It is abbreviated for a Novel Secure Key Management module for Hierarchical Clustering WSNs [41] and furnishes an efficient scalable post-distribution key establishment that allows the hierarchical clustering topology platform to furnish an acceptable security services. The protocol uses i) pre-deployed keys, ii) network generated keys and iii) the BS broadcasted keys. The protocol is energy-efficient, has strong flexibility against susceptible attacks on WSNs, keeping the resource starved nature of sensor nodes. NSKM also ensures that the whole network is never compromised even if there has been an attack in the network. Furthermore, it is highly lightweight and scalable and is acceptable to be used in large WSNs.

- **AKM:** It is an Authenticated Key Management scheme for hierarchical networks based on the random key predistribution [42]. The protocol ensures confidentiality, global and continuous authentication of nodes in the network by periodically refreshing the network key. In general AKM scheme can be applied for different energy- efficient data dissemination techniques for sensors networks.

Table 1: Comparison summary based on security mechanisms

Name	Key distribution	Authentication	Storage	Communication Load	Scalability	Robustness	Connectivity	Energy Efficiency
RLEACH	Improved Random pair-wise key management (IRPK)	Authentication is achieved via IRPK	High	Medium	Good	Good	Probabilistic	Medium
EECBKM	EBS-based key Management schemes	Via Key Management	Low	Low	Medium	Good	100%	Good
SHEER	Hierarchical key management and authentication scheme	Authentication is achieved via HIKES	Medium	Low	Good	Good	100%	Good
SLEACH	-	MAC	High	Medium	Medium	Limited	Probabilistic	Medium
Sec-LEACH	Random key predistribution scheme	Don't provide broadcasts authentication	High	Medium	Medium	Limited	Probabilistic	Medium
SS-LEACH	-	-	Medium	Low	Medium	Limited	100%	Good
NSKM	MAC	MAC	Low	Low	Good	Good	100%	Good
AKM	Via Key Management and MAC	Via Key Management and MAC	High	Medium	Good	Good	Probabilistic	Medium
SRPSN	MAC	MAC	Medium	Low	Medium	Low	100%	Good
SecRout	MAC	MAC	Low	Low	Good	Limited	100%	Good
IKDM	Via polynomial key predistribution mechanism	Via polynomial key predistribution mechanism	Low	Low	High	Good	100%	Good

- **SRPSN**: It is a Secure Routing Protocol for Sensor Networks consists of a hierarchical network with CHs and cluster member nodes [43]. The protocol is designed to mainly secure the data packet transmission on the sensor networks under different types of attacks using group key management scheme. However, the protocol fails to protect against attacks like altering, spoofing, replaying, Sybil attack.
- **SecRout**: It is a Secure Routing Protocol for sensor networks [44] to provide security against attack from compromised nodes in sensor networks. SecRout can detect if packets are dropped or modified by malicious nodes. In the SecRout protocol, only high efficient symmetric cryptography is used to secure messages, and the partial routing path is recorded in sensor nodes memory. The protocol ensures that the messages received are not tampered, hence guarantees freshness.
- **IKDM**: It is an Improved Key Distribution Mechanism, based on hierarchical network architecture and bivariate polynomial-key pre-distribution mechanism [45]. In IKDM, each sensor has a unique id in the network. An offline Key Distribution Server (KDS) first initializes sensors before deployment by giving each sensor node a polynomial share. In order to setup a pair-wise key between two sensor nodes, they exchange their node ids first, and then nodes evaluate their stored polynomial. Since, sensors nodes can obtain the same value from the two distinct calculations, which can be used as their pair-wise communication key. Note that in IKDM, two communicating parties can establish a unique pair-wise key between them. IKDM scheme can achieve better network resilience against node capture attack, hence can provide efficient security and is not affected by the number of compromised sensors. IKDM scheme provides

better scalability, network throughput, fixed key storage overhead, full network connectivity and is suitable for large-scale WSNs. Therefore IKDM scheme is more energy-efficient due to the lower communication overhead for sensor nodes during the pair-wise key establishment process.

V. RESEARCH GAP

The previous section discusses about the existing secure and energy efficient routing protocols in wireless sensor network. The cumulative outcome of the study is that NSKM, SHEER, EECBKM, IKDM, and SecLEACH provide all the standard security requirements in wireless sensor network and have higher degree of authentication mechanism. It can be also seen that majority of the enhancement work are carried out in LEACH protocol itself, hence technical adoption of LEACH in research for energy efficiency can be observed. The discussion also shows that routing attacks are mainly mitigated by adopting NSKM, AKM, IKDM, RLEACH, and SecRout as compared to other routing protocols. Overhead is another factor for determining the energy efficiency, where it can be seen that SHEER, IKDM, and SS-LEACH substantially posses lower communication overhead. The prime reason behind the overhead is that while performing communication, it drains more energy essentially as compared to the source code execution. The Table.1 also highlights that certain protocol e.g. Sec-LEACH and SLEACH doesn't provide much energy efficiency as compared to IKDM approach. The prime reason behind this is whenever a probabilistic key is used, it produces volume of message occupying more storage. On the other hand, deterministic key distribution technique may overcome the storage issue but requires more computational time. Another important finding is that computation in WSN requires substantially less energy as compared to the exchange of messages between sensor nodes. When scalability is concerned, the study shows that probabilistic approaches are less scalable compared to other schemes of energy efficient and security in WSN. Hence, a dent of research gap is explored where none of the discussed secure and energy efficient studies have successfully mitigate the energy drainage factor along with efficient security system. The study performed by author in [38] has however considered all the techniques for energy efficiency which is discussed in previous section for accomplishing energy efficiency. The study doesn't emphasize on energy constraints while multiple security techniques are applied. This consideration is supposed to be extremely critical as energy consumption is not actually correlated with probabilistic or deterministic techniques. Moreover, the author [38] didn't benchmark their study to future research to follow it.

VI. CONCLUSION

Although there has been lots of attempts in addressing the security and energy efficient routing in wireless sensor network, but very few works are seemed to be benchmarked. It was also seen that frequently considered algorithm like LEACH, which various academician as well as various research scholar considers to be benchmarked is also accompanied by various flaws. It was seen that majority of the research work is symptomatic, which will mean that if the researcher is focusing on a particular security or routing issues, he misses out other associated aspects that are also connected with routing. In short the selection of performance parameters are found not wise enough, as while proposing a new routing protocol, the literatures didn't found any description of reliability, optimization as well as security although it may have good packet delivery ratio, latency, energy etc. Hence, it is very important to visualize the performance parameters in order to justify how much efficient the routing protocols are in addressing energy conservation in wireless sensor network. This paper has discussed very briefly about the evolution of hierarchical routing protocols. The paper starts discussing about the possible design challenges which are yet to be address in the viewpoint of energy efficiency routing principles. Various hierarchical routing protocols like LEACH, TEEN, APTEEN, PEGASIS, and CAG etc are discussed briefly along with their explored limitations. Various approaches of swarm based approaches are briefly discussed to explore the research gap and open issues. The direction of our future work will towards formulating an energy efficient secure hierarchical routing algorithm that addresses the issues discussed in this paper.

REFERENCES

[1] Dargie, W, Poellabauer, C. 2010. Fundamentals of Wireless Sensor Networks: Theory and Practice, John Wiley & Sons, Technology & Engineering - 336 pages

[2] Ma, C. 2007. Battery-aware and Energy-efficient Algorithms for Wireless Networks, Doctorial Thesis of Stony Brooks University

[3] Raghavendra, C, Krishna, K, Znati, T. 2004. Wireless Sensor Networks, Springer-Verlag.

[4] R. Alasem, A. Reda, and M. Mansour, "Location based energy efficient reliable routing protocol for wireless sensor network," World Scientific and Engineering Academy ANDC Society(WSEAS), Stevens Point, Wisconsin, USA, 2011

[5] Y. Yu, R. Govindan, D. Estrin, "Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks", IEEE Workshop on Multi-Object Tracking, 2001

[6] S. Roychowdhury, C. Patra, "Geographic Adaptive Fidelity and Geographic Energy Aware Routing in Ad Hoc Routing", Special Issue of IJCCT, Vol.1 Issue 2-4; 2010

[7] L. Li, J.Y. Halpern, "Minimum-Energy Mobile Wireless Networks Revisited," Proceedings of the IEEE International Conference on Communications, vol.3, pp.1633-1639, 1998

[8] J. Kulik, H. Balakrishnan and W. R. Heinzelman, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", Proceedings on the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 174-185, 1999

[9] J.Kulik, H.Balakrishnan and W. R. Heinzelman, "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks", Wireless Networks, vol. 8, pp.169–185, 2002

[10] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann and F Silva, "Directed Diffusion for Wireless Sensor Networking", IEEE/ACM Transactions on Networking (TON), vol. 11, pp. 2-16, February 2003.

[11] D. Braginsky, D. Estrin, "Rumor routing algorithm for sensor networks", Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, pp. 22-31, October 2002.

[12] L. X. Chen and X. Guan, "A New Gradient-Based Routing Protocol in Wireless Sensor Networks", Proceedings of the First international conference on Embedded Software and Systems, pp. 318-325, 2004

[13] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks", IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000, vol. 8, pp. 8020

[14] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Tmnsactions on Wireless Communications, vol. 1(4), 2002

[15] S. Lindsey and C.S. Raghavendra, "PEGASIS: Power-efficient Gathering in Sensor Information System", Proceedings IEEE Aerospace Conference, vol. 3, pp. 1125-1130, 2002

[16] A.Manjeshwar and D.P. Agarwal, "TEEN : A Protocol for Enhanced Efficiency in Wireless Sensor Networks", Proceedings of the 1 st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001

[17] A.Manjeshwar and D.P. Agarwal," APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless in Wireless Sensor Networks," Proceedings of the 2nd International Workshop of Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco CA, April 2001.

[18] O. Younis and S. Fahmy, "Heed: A Hybrid, energy, Distributred Clustering Approach for Ad-hoc Networks", IEEE Transactions on Mobile Computing Issues in Wireless Networks and Mobile Computing, vol 3, no. 4, pp.366-369, 2004

[19] O.Younis and S. Fahmy, "Distributed Clustering in Ad-hoc sensor Networks: A Hybrid Energy - efficient Approach", International Journal of Computer Science, 2002..

[20] S. Yoon, C. Shahabi, "Exploiting Spatial Correlation Towards an Energy Efficient Clustered Aggregation Techique (CAG)", IEEE Conference on Communications, 2005.

[21] S. Yoon, C. Shahabi, "An Experimental Study of the Effectiveness of Clustered Aggregation (CAG) Levaraging Spatial and Temporal Correlations in Wireless Sensor Networks" ACM Transactions on Sensor Networks,USC,CS Dept Technical Report 05-869, August 2005.

[22] S.K.Singh, M.P.Singh and D.K.Singh, "Energy– efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug.2010,vol.2.no 3,pp 49-61

[23] Xu, Z., Yin, Y., Wang, J., Kim, J-Uk.2014. A Density-based Energy-efficient Clustering Heterogeneous Algorithm for Wireless Sensor Networks, International Journal of Control and Automation, vol.7, no.2, pp.175-188

[24] Lee, S-K., Koh, J-G., Jung, C-R.2014. An Energy-Efficient QoS-aware Routing Algorithm for Wireless Multimedia Sensor Networks, International Journal of Multimedia and Ubiquitous Engineering, vol.9, No.2 (2014), pp.245-252

[25] Zytoune, O., Aboutajdine, D.2014. A Low Energy Time Based Clustering Technique for Routing in Wireless Sensor Networks, American Journal of Sensor Technology, vol. 2, no. 1, pp.1-6

[26] Poostfroushan, S., Sarram, M.A., Sheikhpour, Razieh. 2014. Energy Efficient Backbone Formation Using Particle Swarm Optimization Algorithm in Wireless Sensor Networks, International Journal of Grid and Distributed Computing, vol.7, no.1, pp.123-134

[27] Haider, A., Sandhu, M. M., Amjad, N.2014. REECH-ME: Regional Energy Efficient Cluster Heads based on Maximum Energy Routing Protocol with Sink Mobility in WSNs, Journal of Basic and Applied Scientific Research, vol.4(1),pp.200-216

[28] Zhang, C., Liu, Fangai., WU, Nan.2014. A Distributed Energy-e_cient Unequal Clustering Routing Protocol for Wireless Sensor Networks, Journal of Computational Information Systems, vol. 10: 6, pp. 2369-2376

[29] Shu, W., Wang,J.2013. An Optimized Multi-hop Routing Algorithm Based on Clonal Selection Strategy for Energy-efficient Management in Wireless Sensor Networks, Sensors & Transducers, vol. 22, pp. 8-14

[30] Deng, H., Yang,C., Sun,Y.2013. A Novel Algorithm for Optimized Cluster Head Selection, Science Journal of Electrical & Electronic Engineering

[31] Moh'd A- O., Al-A ,Alaa.2013. Extending Wireless Sensor Network Lifetime by Relocating of Base Station using Harmony Search Algorithm, Wireless Sensors and Cellular Systems

[32] John,J.T., Ramson, S. R. J.2013. Energy-Aware Duty Cycle Scheduling for Efficient Data Collection in Wireless Sensor Networks, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol.2, Issue. 2

[33] Zhao, J., Y. Lirong. 2014.LEACH-A: An Adaptive Method for Improving LEACH Protocol, Sensors & Transducers, vol. 162 , Issue. 1, pp. 136-140

[34] Kim, J-Y., Sharma, T., Kumar, B., Tomar, G.S., Berry, K., Lee, W-H. 2014. IC-ACO: Inter cluster Ant colony Optimization Algorithm for Wireless Sensor Network in Dense Environment, International Journal of Distributed Sensor Network

[35] Zungeru, A.M., Yahaya, E.A. 2013.Caroline Omoanatse Alenoghena3, Performance Evaluation of Energy-aware Swarm Intelligence Based Routing Protocols for Wireless Sensor Networks Based on Different Radio Models, International Journal of Computing, Communications and Networking, Vol. 2,no.4

[36] S. Sahraouri, S. Bouam, Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks, International Journal of Communication Networks and Information Security, Vol.5, No.3, 2013

[37] T. Lalitha and R. Umarani, "Energy efficient Cluster Based Key Management Technique for Wireless Sensor Network," International Journal of Advances in Engineering & Technology (IJAET), Vol. 3 No. 1, 2012, pp. 186-190.

[38] S. Sharma, SK Jena, A Survey of Secure Hierarchical Routing Protocols in Wireless Sensor Network, ACM, 2011

[39] L. B. Oliveira, A. Ferreira, M. A. Vilaca, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "Secleach-on the security of clustered sensor networks," Signal Processing, Vol. 87, No. 12, 2007, pp. 2882–2895.

[40] A. Beniwal, N. Chaudhary, V. Sen, LEACH: Implementation of Routing Protocols in Wireless Sensor Network, International Journal of Engineering Technology & Computer Research, Vol.2, pp.25-29, 2013

[41] QI. Sarhan, Security Attacks and Countermeasures for Wireless Sensor Networks: Survey, International Journal of Current Engineering and Technology, 2013

[42] B. Kadri, D. Moussaouni, M. Feham, An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks, Wireless Sensor Network, 2012, 4, 155-161

[43] A. Diop, Y. Qi, Q. Wang, and S. Hussain, AN Advanced Survey on Secure Energy efficient Hierarchical Routing protocols in WSN, Retreived from http://arxiv.org/ftp/arxiv/papers/1306/1306.4595.pdf

[44] A. Modirkhazeni, N. Ithnin, M. Abbasi, Secure Hierarchal Routing Protocols in Wireless Sensor Networks; Security Survey Analysis, International Journal of Computer Communications and Networks, 2012

[45] AK Das, Improving Identity-based Random Key Establishment Scheme for Large-scale Hierarchical Wireless Sensor Network S, International Journal of Network Security, Vol.14, No.1, PP.1{21, Jan. 2012