Research Journal of Applied Sciences, Engineering and Technology 12(5): 516-521, 2016
DOI:10.19026/rjaset.12.2678
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 5, 2015 Accepted: September 14, 2015 Published: March 05, 2016

Research Article

Energy Efficient and Secure Data Transmission for Cluster-based WSN using Routing Algorithm

[1]R. Arun and [2]V. Jeyalakshmi
[1]Electronics and Communication Engineering, St. Peter's University,
[2]Electronics and Communication Engineering, Anna University, Chennai, India

Abstract: Secure data transmission is a very critical issue for WSN, Clustering is an effective and practical way to enhance the system performance of WSN. Providing security to transmit data is a demanding issue for Wireless Sensor Networks (WSNs). Clustering is a technique which is more effective to upgrade system performance. SET-IBS and SET-IBOOS are two Secure and efficient data transmission protocol for cluster based WSNs. They use Identity-Based digital Signature (IBS) method and Identity-Based Online/Offline digital Signature (IBOOS) method, where the clusters are formed dynamically and periodically. Even though SET-IBS and SET-IBOOS are secured routing protocols, it has some issues like energy efficiency, trustability and elongating network lifetime. To overcome these issues, Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER) are two routing algorithms proposed for MANET in which trustability is ensured either hop-by-hop or end-to-end retransmissions. It considers the energy level in a battery of a node and also passable links to find energy efficient and trustable paths that improves the working longevity of the network.

Keywords: Efficient routing, energy aware routing algorithm, MANETs, routing protocol, secure routing

INTRODUCTION

To handover reliable and secure communication in MANET is trickier. MANETs are surrounded by menace and at the same time, many WSNs are deployed in rugged, disregarded and often adversary environments for certain applications, such as military domains and sensing tasks with distrustful surroundings. Aiiouat and Harous (2012) says, the energy constraint of WSNs makes energy saving become the most important goal of various routing algorithms. EEICCP has shown remarkable improvement over already existing LEACH and HCR protocols in terms of reliability and stability. Providing security to transmit data is most vital and is demanded in many such practical WSNs in their own hallmark for soldiers in their war field, which could be frequently changed. Referring to Balasubramanian *et al*. (2007) this Disruption Tolerant Network (DTN) architecture, it is enabled only when the mobile nodes are connected only intermittently to transfer data. Energy-efficient routing is an intelligent methodology for reducing energy, data communication cost in MANETs. Typically, paths are disclosed considering the consumption of energy for end-to-end (E2E) packet traversal detecting trusted routes can enrich QoS. These difficulties are inherent to their constrained specificities which require adapted solutions unrelated to classical wire networks. As long as, accounting the leftover energy of nodes in routing can dodge nodes from being overexpose and can ultimately lead to an increase in the working lifetime of the network. Dong *et al*. (2005) says, in present system of Wireless Sensor Network, sensor nodes are used to observe physical surroundings a clustering-based protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network. Each sensor node is qualified of perceiving their surroundings, process the information and sends data to one or multiple assemblage in a WSN. Efficient transmission of data is one of the vital issues for WSNs the fact (shown by our analysis) that direct (expensive) transmissions to the sink are needed only rarely.

Lu *et al.* (2014) says, Efficient and Secure transmission of data is required and is demanded in many practical WSNs. For that purpose, two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) method and the Identity-Based Online/Offline digital Signature (IBOOS) method are proposed. Computational and storage costs are reduced by applying digital signatures to message packets, which are efficient in

Corresponding Author: R. Arun, Electronics and Communication Engineering, St. Peter's University, Chennai, India

communication and applying the key management for security. In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the Base Station initially. We compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations respectively, both computation and communication. Vijayalakshmi *et al*. (2013) says a novel energy-aware routing algorithm, called Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER) is proposed. It finds efficient energy and trusted routes that improve the working lifetime of the network. RMECR is proposed for networks with Hop-By-Hop (HBH) retransmissions providing link layer reliability and networks with E2E retransmissions providing E2E trustability. Finally, routing algorithm RMECR is included in these SET routing protocols to enrich the interpretation and security of MANET.

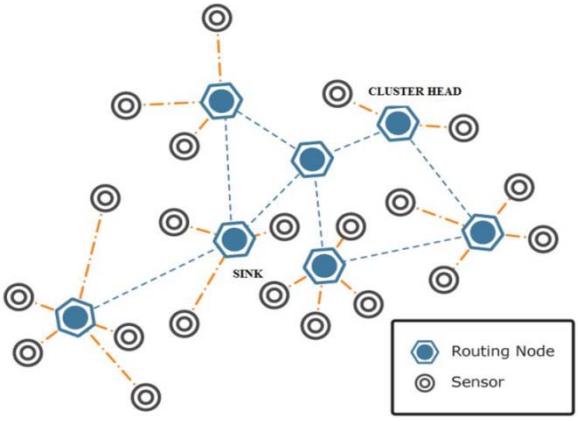

Fig. 1: Proposed architecture

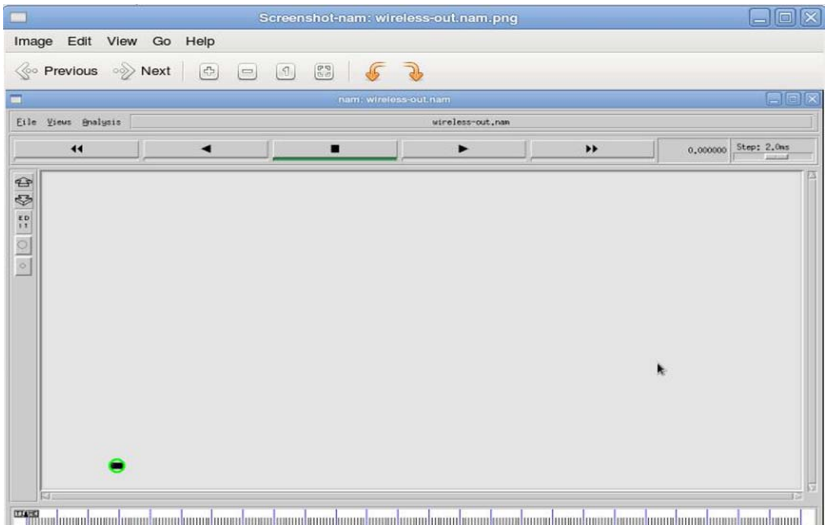

Fig. 2: Forming of node

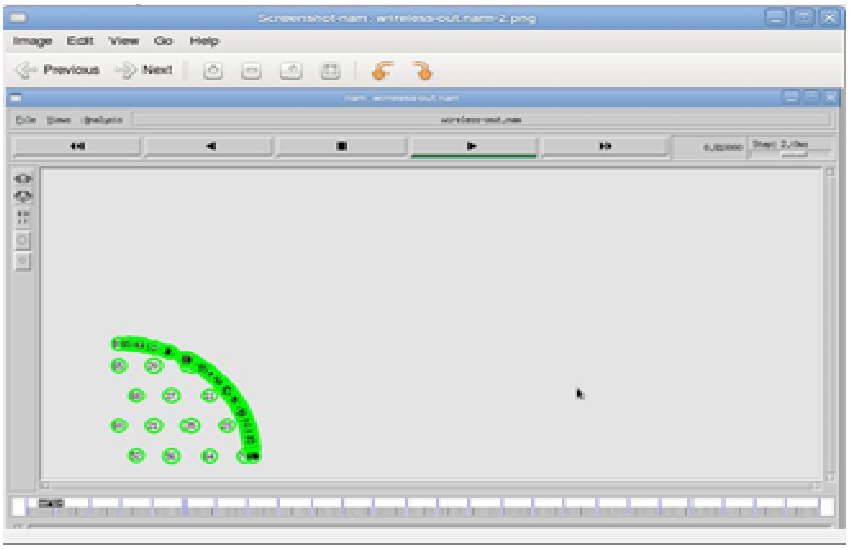

Fig. 3: Forming of nodes

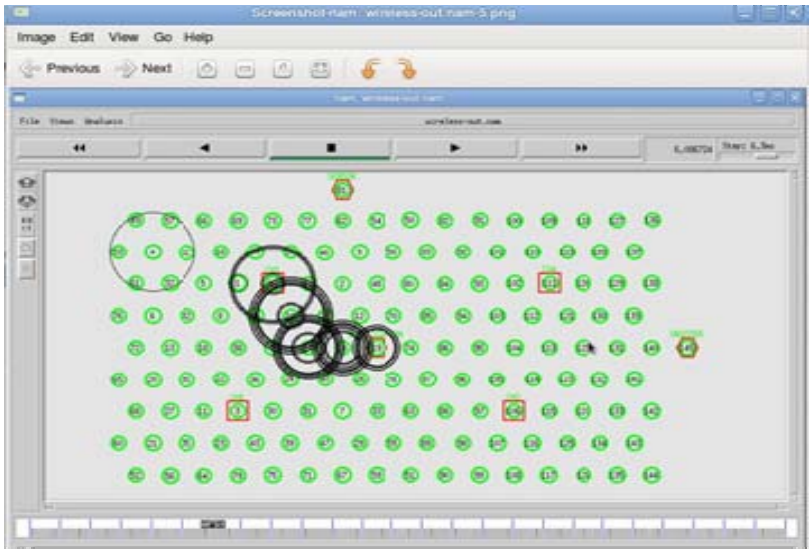

Fig. 4: Grouping of nodes

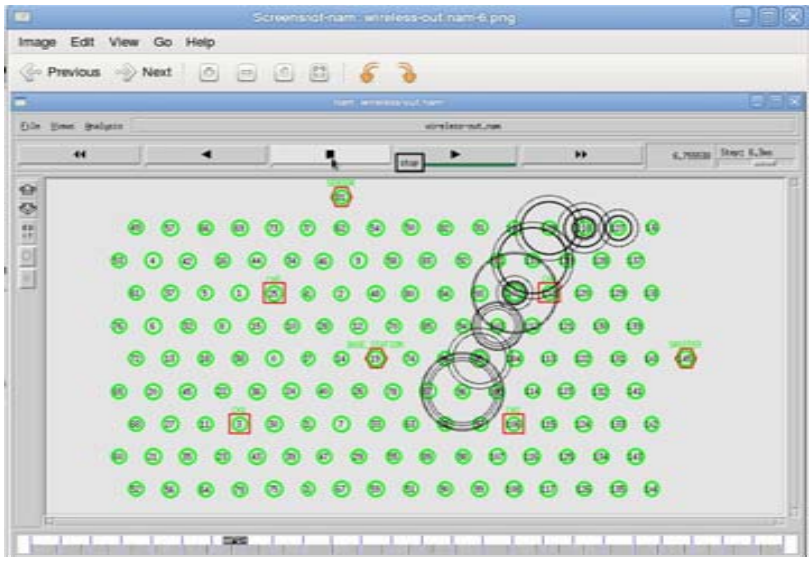

Fig. 5: Transferring data between source node and destination node

PROPOSED ARCHITECTURE

System Architecture is a process of explaining the data is transmitted efficiently. Architecture consists of sensor nodes formed into groups where one in a group will act as master node called as cluster head and other nodes will act as slave node. The cluster head has to manage the nodes of its own cluster and to communicate with other clusters. The step by step process clearly explains how a node is formed and how it communicates with other cluster to transmit data effectively. The step by step process is explained below: Initially the first stage nodes are formed and then stage two forms groups called clusters. Later cluster head is selected from the group already formed. After we can see sensor sending information or data is sensed to base station and base station sends in to cluster head. Normally cluster heads are the one who sends data to the one whom requested based on routing protocol its selects shortest path in the network. The role of sniffer is to identify the hacker nodes and delete it. After deleting, network becomes secured and efficient. This process is involved in architecture and the same is explained with Fig. 1.

Steps involved in System Architecture: Figure 2 shows how node is formed in NS-2 and Fig. 3 shows how nodes are formed in multiple numbers.

Figure 4 shows grouping of nodes and also clustering is formed. Data is transferred between source node and destination node and is clearly shown in Fig. 5.

ROUTING STRATERGY

IBS Scheme for CWSNs: Following operations consists of an IBS scheme implemented for CWSNs, specifically, setup at the BS, key extraction and signature signing at the data sending nodes and verification at the data receiving nodes:

- **Set up:** The BS generates a master key msk and public parameters for the Private Key Generator (PKG) and gives to all sensor nodes.
- **Extraction:** Given an ID string, a sensor node generates a private key sec ID associated with the ID using msk.
- **Signature signing:** Given a message M, time stamp t and a signing key, generates a signature SIG by sending the nodes.
- **Verification:** Given the ID, M and SIG, the receiving node outputs "accept" if SIG is valid and outputs "reject" otherwise.

IBOOS Scheme for CWSNs: Following three operations consists of an IBOOS scheme implemented for CWSNs, specifically, setup, key extraction, at the BS and offline signing at the CHs, the data sending nodes at online signing and verification at the receiving nodes: Setup as same in the IBS scheme:

- **Set up:** The BS generates a master key msk and public parameters for the Private Key Generator (PKG) and gives to all sensor nodes.
- **Extraction:** Given an ID string, a sensor node generates a private key sec ID associated with the ID using msk.
- **Offline signing:** The CH sensor node generates an offline signature SIG offline and transmits it to the leaf nodes in its cluster.
- **Online signing:** SIG offline and message M sending node (leaf node) generates online signature SIG online.
- **Verification:** Given ID, message M and SIG online receiving node (CH node)
- **Protocol features:** The protocol characteristics and the features of the proposed SET-IBS and SET-IBOOS protocols as follows:
  - The proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for ID-based settings, this protocol use for ID information and digital signature for authentication. SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs.
  - The proposed secure and efficient data transmission protocols are ID-based signature, uses the ID information and digital signature for verification. In SET-IBOOS, the offline signature is executed by the sensor nodes. This sensor node has to execute the offline algorithm before it wants to sign on a new message (Fig. 6).

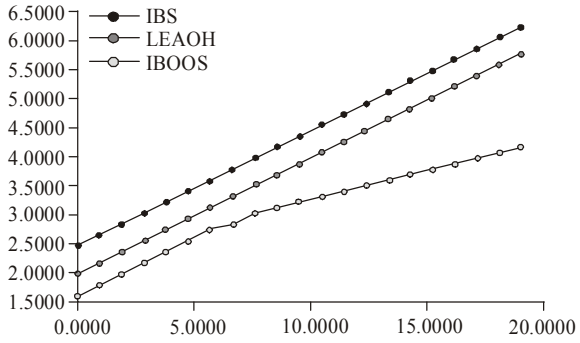

Fig. 6: Calculation of DD comparison

RESULTS AND DISCUSSION

Energy efficient wireless Adhoc routing: Dijkstra's routing algorithm was considered as a solution for less energy consuming in MANETs, which is also a shortest path algorithm. But it didn't satisfy the requirement of consuming less energy during packet data routing. It is also possible only if number of retransmissions on each link is more to assure complete trustability of links. Efthymiou *et al*. (2006) says in common, paths are discovered based on energy consumption for end-to-end (E2E) packet data traversal. Moreover it should neither use the same links frequently nor less trustable links in a network. Efficient energy routing in MANET should be based on trustability/reliability of links and node's energy level.

Minimum energy paths for reliable communication in multi-hop wireless networks: Existing algorithms like BAMER (basic algorithm for minimum energy routing, GAMER (General algorithm for minimum energy routing), DAMER (Distributed algorithm for minimum energy routing) prefer minimum cost multihop paths. In situations like where transmission power is standard, each link layer has same cost and minimum hop path and when transmission power can be varied, link cost is higher for longer hops. The energy aware routing algorithms choose a path with short distance hops. Cost of the links deal with energy required and link error rate. This cost shows that total energy used for reliable and unreliable link layers. Also, it's proven from simulations that performance can be improved in this method.

Figure 7 is the packet delivery ratio of DAMER which is comparatively more than BAMER and GAMER.

Comparison of protocols: According to Fasolo *et al*. (2007) existing protocols like AODV protocol is only used when two end points do not have a valid active

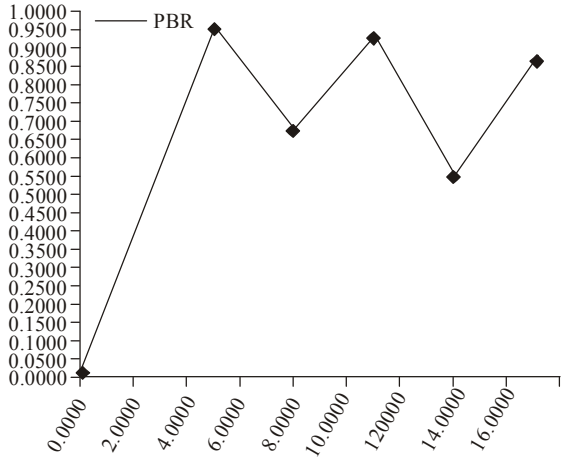

Fig. 7: Comparison of PDR

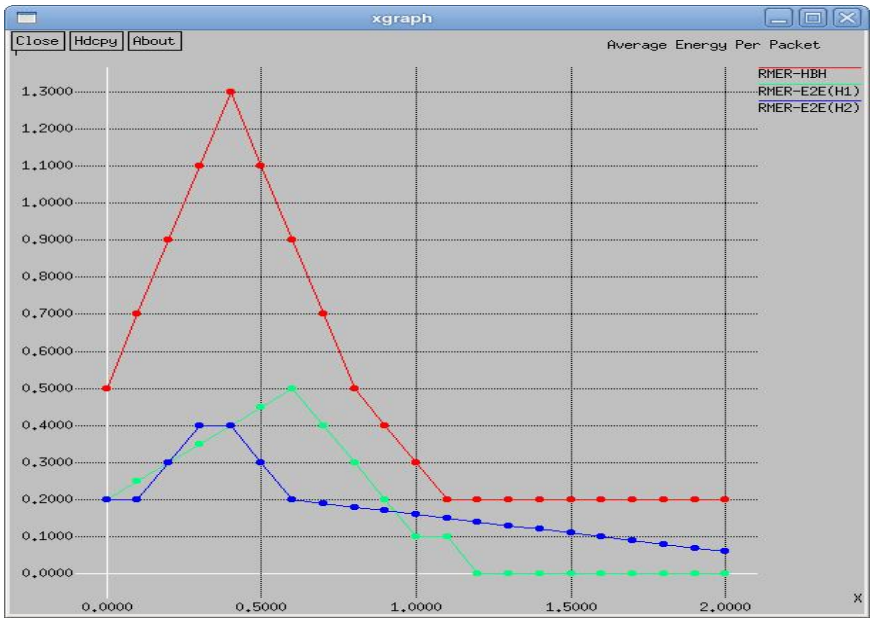

Fig. 8: Comparisons of protocols

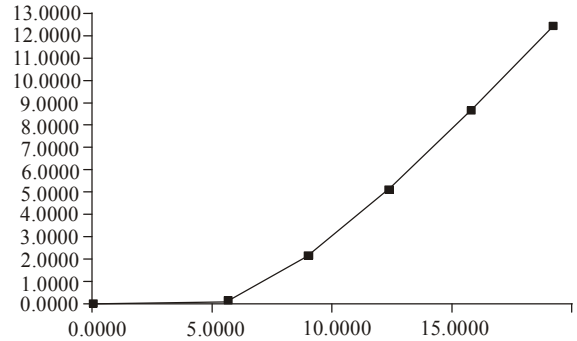

Fig. 9: Throughput of RMER

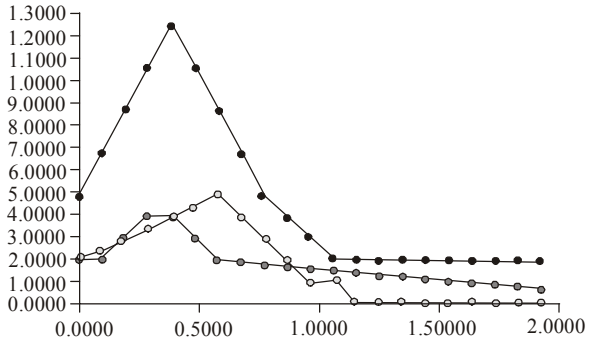

Fig. 10: Comparison of RMER

route to communicate with each other. Dynamic State Routing (DSR) is on demand routing protocol which calculates route only when required and its self organized and self configured. Session Initiation Protocol works independently of underlying transport protocols. Comparing all these protocols our

proposed protocol with proposed algorithm is more efficient and secured. Expected transmission count metric (ETX) which finds high throughput paths on multi hop wireless networks. ETX minimizes the expected total number of packet transmission (including retransmission) required successfully deliver the packet to the ultimate destination. The ETX metric incorporates the effects link loss ratios, asymmetric in the loss ratios between the two directions of each link and interference among the successive links of the path. Tang *et al*. (2010) says the minimum hop count metric chooses arbitrarily among the different paths of the same minimum length, regardless of the often large difference in throughput among those paths and ignoring the possibility that a longer path might offer higher throughput.

This study describes the design and implementation of ETX as a metric for the DSDV and DSR routing protocols, as well as modifications to DSDV and DSR which allow them to use ETX. Measurement taken from a 29 node 802.11b test bed demonstrate the poor performance of minimum hop count, illustrate the causes of that poor performance and confirm that ETX improves performance. For long paths, the throughput improvement is often a factor of two or more, suggesting that ETX will become more useful as networks grow larger and paths become longer.

Figure 8 shows the comparison of routing protocols such as RMER, BAMER. Figure 9 shows the throughput of RMER. Toh (2001) present five different metrics based on battery power consumption at nodes. We show that using this metrics in a shortest-cost routing algorithm reduces the cost/packet of routing packets by 5-30% over shortest hop routing (this cost reduction is on top of a 40-70% reduction in energy consumption obtained by using PAMS, our MAC layer protocol). Furthermore, using this new metrics ensure that the mean time to node failure is increased significantly. An interesting property of using shortest-cost routing is that packet delays do not increase. Finally, we note that our new metrics can be used in most traditional routing protocols for adhoc network Fig. 10.

CONCLUSION

In this study, SET-IBS and SET-IBOOS are the security requirements and this protocol analysis against routing attacks. SET-IBS and SET IBOOS communications are efficient and which are applied on the ID based crypto system and achieves security requirements in CWSNs. proposed SET-IBS and SET-IBOOS protocols have greater performance than existing secure protocols for CWSNs. This study mainly focuses on NAM analysis and an innovative technique Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER) which is used to improve the SET-IBS and SET-IBOOS protocol. RMECR and RMER can improve the working lifetime of the network using efficient energy and trusted routes, it is noticed that RMECR and RMER discovers path that are energy efficient and trusted high paths.

REFERENCES

Aiiouat, Z. and S. Harous, 2012. An efficient clustering protocol increasing wireless sensor networks life time. Proceeding of the IEEE International Conference on Innovations in Information Technology, pp: 194-199.

Balasubramanian, A., B. Levine and A. Venkataramani, 2007. DTN routing as a resource allocation problem. Proceeding of the 2007 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM'07), pp: 373-384.

Dong, Q., S. Banerjee, M. Adler and A. Misra, 2005. Minimum energy reliable paths using unreliable wireless links. Proceeding of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05), pp: 449-459.

Efthymiou, C., S. Nikoletseas and J. Rolim, 2006. Energy balanced data propagation in wireless sensor networks. Wirel. Netw., 12(6): 691-707.

Fasolo, E., M. Rossi, J. Widmer and M. Zorzi, 2007. In-network aggregation techniques for wireless sensor networks: A survey. IEEE Wirel. Commun., 14(2): 70-87.

Lu, H., J. Li and M. Guizani, 2014. Secure and efficient data transmission for cluster-based wireless sensor networks. IEEE T. Parall. Distr., 25(3): 750-761.

Tang, F., H. You and S. Guo, 2010. A chain-cluster based routing algorithm for wireless sensor networks. Springer Science.

Toh, C.K., 2001. Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks. IEEE Commun. Mag., 39(6): 138-147.

Vijayalakshmi, G., S. Hema and S. Geethapriya, 2013. Secure data aggregation & query processing in wireless sensor networks using enhanced leach protocol. Int. J. Emerg. Sci. Eng. (IJESE), 2(1).