ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 6 , June 2016

Secure and Load Balanced Data Gathering In WSN with Hidden Topology and Multipath Routing

Dr. Yuvaraju M., Shanthini S.

Associate Professor, Department of Electronics and Electronics Engineering, Regional Campus of Anna University, Coimbatore, India
P.G. Student, Department of Electronics and Electronics Engineering, Regional Campus of Anna University, Coimbatore, India

ABSTRACT: Wireless Sensor Networks are a prominent method for extracting local measures of interest. For secure gathering of data in the receiving side, this paper focuses on two techniques- load balancing and topology hiding in multipath routing protocol. First, Load balancing in multipath routing will avoid overloading of few nodes when compared to the other nodes. The nodes near the sink may be heavily loaded due to traffic. Depleted batteries of the node may cause connectivity problem in the network. So, load balancing is used to maintain connectivity of the network. Next, Topology hiding in multipath routing is used for improving security and reliability of the network. There are possibilities of various attacks due to Topology-exposure. Results show that Load balancing is capable of increasing the energy efficiency per node as well as shorter delivery time. Topology hiding can resist attacks at a low overhead and short routing convergent time.

KEYWORDS: Load balancing, Topology hiding, multipath routing, secure data gathering

I INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring and health care applications. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. They are expected to support a wide variety of applications, many of which demand life time network connectivity and strict security against various attacks.

Practically, sensors are densely deployed and randomly scattered over a sensing field and left unattended after being deployed, which make it difficult to recharge or replace their batteries. After sensors form into autonomous organizations, those sensors near the data sink typically deplete their batteries much faster than others due to more relaying traffic. When sensors around the data sink deplete their energy, network connectivity and coverage may not be guaranteed. Due to these constraints, it is crucial to design an energy-efficient data collection scheme that consumes energy uniformly across the sensing field to achieve long network lifetime in terms of connectivity.

Majority of the security threats arise due to the topology exposure problem. Topology-exposure is a serious problem, which makes it possible for the malicious nodes to launch many kinds of attacks, such as black hole attack, wormhole attack, rushing attack and sybil attack. Topology-exposure is much more serious in multipath routing protocols than in other routing protocols considering that multipath routing protocols usually carry a lot of routing information in route messages in order to find sufficient routes. In some cases, data packets are also required to carry routing information. For example, Dynamic Routing Protocol (DSR) carries the whole route from source to destination in packet headers. Malicious nodes can deduce part or the whole network topology based on the captured routing information and it is hard to ensure the confidentiality of routing information because of the open media network environment in which any node can capture packets within its transmission range.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 6 , June 2016

So, the focus of this paper is to provide solution for the above mentioned two problems by means of traffic aware load balancing and topology hiding protocol respectively. Secure data gathering with Load Balancing and Hidden Topology (LBHT) protocol not only provides solution for the two problems but ii also guarantees increase in throughput, more stabilized packet delivery ratio, lower packet loss and increased efficiency in attacker detection.

II. RELATED WORKS

A. A coordinated data collection approach: design, evaluation, and comparison

The problem of collecting a large amount of data from several different hosts to a single destination in a wide-area network is being considered. It is important since improvements in data collection times in many applications such as wide-area upload applications, high-performance computing applications, and data mining applications are crucial to performance of those applications. Often, due to congestion conditions, the paths chosen by the network may have poor throughput. By choosing an alternate route at the application level, we may be able to obtain substantially faster completion time. This data collection problem is a nontrivial one because the issue is not only to avoid congested link(s), but to devise a coordinated transfer schedule which would afford maximum possible utilization of available network resources. This approach for computing coordinated data collection schedules makes no assumptions about knowledge of the topology of the network or the capacity available on individual links of the network. This approach provides significant performance improvements under various degrees and types of network congestions. A comprehensive comparison study of the various approaches to the data collection problem which considers performance, robustness, and adaptation characteristics of the different data collection methods is given. The adaptation to network conditions characteristics are important as the above applications are long lasting, i.e., it is likely changes in network conditions will occur during the data transfer process. This approach can be used for solving arbitrary data movement problems over the Internet.

B. Load balanced routing protocols for ad hoc mobile wireless networks

Mobile ad hoc networks are collections of mobile nodes that can dynamically form temporary networks without the need for pre-existing network infrastructure or centralized administration. These nodes can be arbitrarily located and can move freely at any given time. Hence, the network topology can change rapidly and unpredictably. Because wireless link capacities are usually limited, congestion is possible in MANETs. Hence, balancing the load in a MANET is important since nodes with high loads will deplete their batteries quickly, thereby increasing the probability of disconnecting or partitioning the network. This article discusses the various load metrics and summarizes the principles behind several existing load balanced ad hoc routing protocols. Finally, a qualitative comparison of the various load metrics and load balanced routing protocols is presented.

C. Load-aware on-demand routing Load balanced routing protocols for ad hoc mobile wireless networks

Mobile ad hoc networks are collections of mobile nodes that can dynamically form temporary networks without the need for pre-existing network infrastructure or centralized administration. These nodes can be arbitrarily located and can move freely at any given time. Hence, the network topology can change rapidly and unpredictably. Because wireless link capacities are usually limited, congestion is possible in MANETs. Hence, balancing the load in a MANET is important since nodes with high loads will deplete their batteries quickly, thereby increasing the probability of disconnecting or partitioning the network. This article discusses the various load metrics and summarizes the principles behind several existing load balanced ad hoc routing protocols. Finally, a qualitative comparison of the various load metrics and load balanced routing protocols is presented.

D. Routing with Load Balancing in Wireless Ad Hoc Networks

An ad hoc wireless mobile network is an infrastructure-less mobile network that has no fixed routers; instead, all nodes are capable of movement and can be connected dynamically in an arbitrary manner. In order to facilitate communication of mobile nodes that may not be within the wireless range of each other, an efficient routing protocol is

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 6 , June 2016

used to discover routes between nodes so that messages may be delivered in a timely manner. In this paper, we present a novel Load-Balanced Ad hoc Routing (LBAR) protocol for communication in wireless ad hoc networks. LBAR defines a new metric for routing known as the degree of nodal activity to represent the load on a mobile node. In LBAR routing information on all paths from source to destination are forwarded through setup messages to the destination. Setup messages include nodal activity information of all nodes on the traversed path. After collecting information on all possible paths, the destination then makes a selection of the path with the best-cost value and sends an acknowledgement to the source node. LBAR also provides efficient *path maintenance* to patch up broken links by detouring traffic to the destination. A comprehensive simulation study was conducted to evaluate the performance of the proposed scheme. Performance results show that LBAR outperforms existing ad hoc routing protocols in terms of packet delivery and average end-to-end delay.

E. Neighbour Traffic-Aware Load Balancing Method in Ad Hoc Networks

Load balancing in ad hoc networks is more challenging issue than that in wired networks because the nature of decentralized network management and terminal mobility makes it difficult to realize appropriate controls for the whole network. Although some traffic-based load balancing methods that work with rerouting mechanisms have been proposed, they are, due to the overhead for rerouting, hard to adapt the environment where the traffic or the topology changes in a short period. Furthermore, the conventional methods cannot always find appropriate routes since they only give attention to the current transmission route. This paper proposes a load balancing method based on adaptive transmission rate control using neighbouring terminals' status. The proposed method does not adopt a rerouting mechanism but introduce a rate control so that we do not have to consider the overhead for rerouting. Computer simulation showed that, depending on terminals' status, our method achieves more effective load balancing, as well as better throughput, than the conventional rerouting-based methods.

F. Design and performance study of a Topology-Hiding Multipath Routing protocol for mobile ad hoc networks

Existing multipath routing protocols for MANET ignore the topology-exposure problem. This paper analyzes the threat of topology-exposure and proposes a Topology-Hiding Multipath Routing protocol (THMR). THMR doesn't allow packets to carry routing information, so malicious nodes cannot deduce topology information and launch various attacks based on that. The protocol can also establish multiple node-disjoint routes in a route discovery attempt and exclude unreliable routes before transmitting packets. We formally prove that THMR is loop-free and topology-hiding. Simulation results show that our protocol has better capability of finding routes and can greatly increase the capability of delivering packets in the scenario where there are attackers at the cost of low routing overhead.

G. TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks

Existing multipath routing protocols in MANETs ignore the topology-exposure problem. This paper analyzes the threats of topology-exposure and propose a TOpology-HIding multipath Protocol (TOHIP). TOHIP does not allow packets to carry routing information, so the malicious nodes cannot deduce network topology and launch various attacks based on that. The protocol can also establish multiple node-disjoint routes in a route discovery attempt and exclude unreliable routes before transmitting packets. We formally prove that TOHIP is loop-free and does not expose network topology. Security analysis shows that TOHIP can resist various kinds of attacks efficiently and effectively. Simulation results demonstrate that TOHIP has better capability of finding routes and can greatly increase the capability of delivering packets in the scenarios where there are malicious nodes at the cost of low routing overhead.

III. SCOPE OF RESEARCH

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity.

The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 6 , June 2016

control, machine health monitoring and health care applications. They are expected to support a wide variety of applications, many of which are important for in our day to day life.

The major issues that affect the design and performance of a wireless sensor network are as follows: Hardware and Operating System for WSN, Wireless Radio Communication Characteristics, Medium Access Schemes, Deployment, Localization, Synchronization, Calibration, Network Layer, Transport Layer, Data Aggregation and Data Dissemination, Database Centric and Querying, Architecture, Programming Models for Sensor Networks, Middleware, Quality of Service and Security issues.

In this paper we focus on few important issues like increased life time of the network by balancing the load, reducing the attacks in the network by multipath routing and topology hiding. In wireless sensor networks, finding solution for the above mentioned issues is very important and challenging due to several characteristics that distinguish them from contemporary communication and wireless ad hoc networks.

IV. PROPOSED METHODOLOGY AND DISCUSSION

In the proposed system, the nodes are created first. The nodes are grouped in to clusters and informed about their regional coordinator. As the regional coordinator is the node that communicates with nodes inside the same cluster and also with other regional coordinators, it should be energy efficient node. Next the packet travels to the nearest neighbours by means of multipath routing. Load balancing is employed along with multipath routing in order to avoid overloading of few nodes. In case of attacker the packet get forwarded through the other nodes.

A. Flow diagram

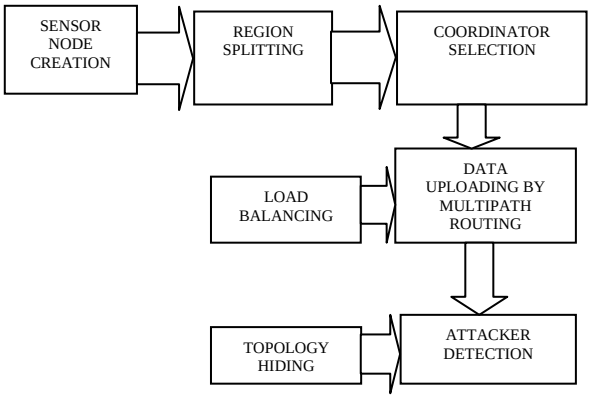

Fig. 1: Flow diagram

B. Algorithm

Load balancing with Hidden topology (LBHT)
Phase i

- Sensor nodes are created
- Each node becomes aware of its neighbouring node.

Phase ii

- Sensors are in different geographical locations are grouped together by clustering mechanism.

Phase iii

- For each cluster, a coordinator node is selected. This node acts as the gateway for that cluster.
- All nodes inside the cluster are informed about its regional coordinator

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 6 , June 2016

Phase iv

- Node disjoint path are created
- Packets of information are forwarded to neighbouring nodes by multipath routing technique.
- Load balancing is employed in this phase. If any few cluster members are overloaded, the load can be shared by the other under loaded nodes inside the same cluster and find a alternative path.

Phase v

In case of an attacker, topology hiding is employed here. When a node sends a message to all its neighbour nodes, only the intended node will acknowledge it. So, only that path will be active and all the other path will be hidden .If there is an attacker in the intended node, a different path will be selected to forward the message.

C. Load balancing

Load balancing refers to efficiently distributing incoming network traffic across a group of backend nodes.A load balancer acts as the "traffic cop" routing node requests across other nodes capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one node is overworked, which could degrade performance. If a single node goes down, the load balancer redirects traffic to the remaining nodes. When a new node is added to the cluster, the load balancer automatically starts to send requests to it.
In this manner, a load balancer performs the following functions:

- Distributes node requests or network load efficiently across multiple nodes
- Ensures high availability and reliability by sending requests only to nodes that are active.
- Provides flexibility to add or subtract nodes as demand dictates
    - Load Balancing Algorithms

Different load balancing algorithms provide different benefits; the choice of load balancing method depends on needs:
Round Robin – Requests are distributed across the group of nodes sequentially. Least Connections – A new request is sent to the node with the fewest current connections, the relative computing capacity of each node is factored into determining which one has the least connections. Node identity – The address of the node is used to determine which node receives the request.

- Clustered load balancing

The main objective of this approach is to cluster sensor network efficiently around few high-energy gateway nodes. Clustering enables network scalability to large number of sensors and extends the life of the network by allowing the sensors to conserve energy through communication with closer nodes and by balancing the load among the gateway nodes. Gateways associate cost to communicate with each sensor in the network. Clusters are formed based on the cost of communication and the load on the gateways.

Network setup is performed in two stages; Bootstrapping and Clustering. In the bootstrapping phase, gateways discover the nodes that are located within their communication range. Gateways broadcast a message indicating the start of clustering. We assume that receivers of sensors are open throughout the clustering process. Each gateway starts the clustering at a different instance of time in order to avoid collisions. In reply the sensors also broadcast a message with their maximum transmission power indicating their location and energy reserve in this message. Each node discovered in this phase is included in a per-gateway range set.

In the clustering phase, gateways calculate the cost of communication with each node in the range set. This information is then exchanged between all the gateways. After receiving the data from all other gateways each gateway start clustering the nodes based on the communication cost and the current load on its cluster. When the clustering is over, all the sensors are informed about the ID of the cluster they belong to.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 6 , June 2016

Since gateways share the common information, sensors are generally equipped with data processing and communication capabilities. The sensing circuit measures parameters from the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensors. Typically the sensor sends such sensed data, usually via radio transmitter, to a base station or Command node, either periodically or based on events. The command node can be statically located in the vicinity of the sensors or it can be mobile so that it can move around the sensors and collect data. In either case, the command node cannot be reached efficiently by all sensors in the system. To avoid long haul communication with the command node some high-energy nodes called Gateways are typically deployed in the network. These Gateways, group sensors to form distinct clusters in the system and manage the network in the cluster, perform data fusion to correlate sensor reports and organize sensors by activating a subset relevant to required missions or tasks as shown in Fig 2. Each sensor only belongs to one cluster and communicates with the command node only through the gateway in the cluster.

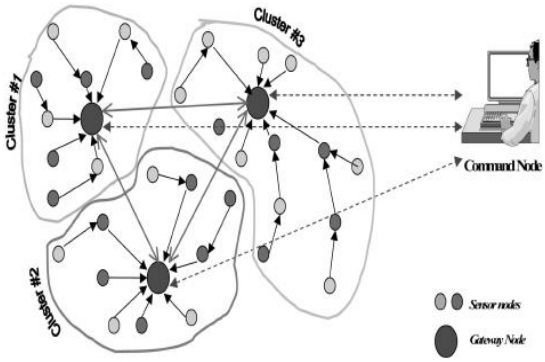

Fig. 2: Multi-gateway clustered sensor network

It is assumed that among the three types of resource heterogeneity, the most important heterogeneity is the energy heterogeneity because both computational heterogeneity and link heterogeneity consumes more energy resource.

D. Topology Hiding

Attacker emanating from network may be protected through topology hiding. This increases the robustness of the system in terms of security.
This section presents protocol TOpology-HIding multipath routing Protocol (TOHIP). There are three objectives in designing TOHIP: (1) the link connection information is hidden as much as possible in route messages, so that the malicious nodes cannot deduce network topology; (2) even with prerequisite of hiding topology, TOHIP can find as many node-disjoint routes as possible, such that both load balancing and reliable packet delivery can be achieved; (3) TOHIP can exclude the malicious nodes from routes and detect the unreliable routes before transmitting packets. To achieve the goals, TOHIP employs the following mechanisms.

- Hide topology: TOHIP does not contain link connectivity information in route messages. Thus no node can deduce network topology by capturing route messages.
- Once a route is established, TOHIP will advertise a set containing the nodes that have been placed on routes, which prevents a node from being placed on another route.
- Defend against attacks: TOHIP uses the combination of hop count and round-trip time as routing metrics. Thus neither single wormhole attack nor single rushing attack can disrupt route discovery.
- Exclude unreliable routes: TOHIP detects and excludes the unreliable routes by means of application-layer route probe messages before transmitting packets.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 6 , June 2016

IV. EXPERIMENTAL RESULTS

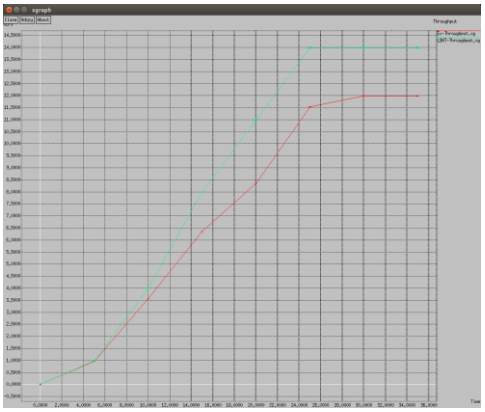

Fig.3: Graph comparing throughput

The above graph compares the existing method and the proposed system with respect to throughput. The LBHT has a higher throughput compared to the conventional method.

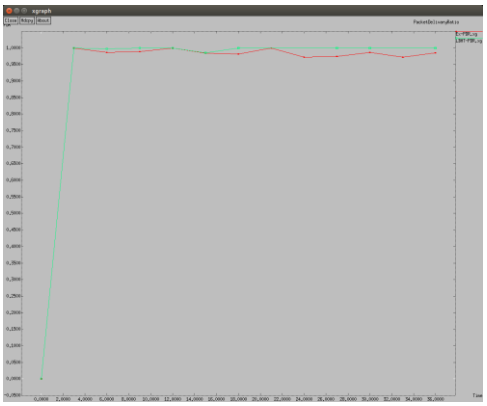

Fig.4: Graph comparing packet delivery ratio

The above graph compares the existing method and the proposed system with respect to packet delivery ratio. The LBHT has much stabilized packet delivery ratio compared to the conventional method.

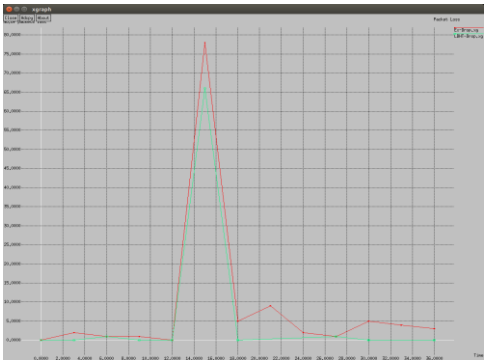

Fig.5: Graph comparing packet loss

The above graph compares the existing method and the proposed system with respect to packet loss. The LBHT has a lower packet delivery ratio compared to the conventional method.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 6 , June 2016

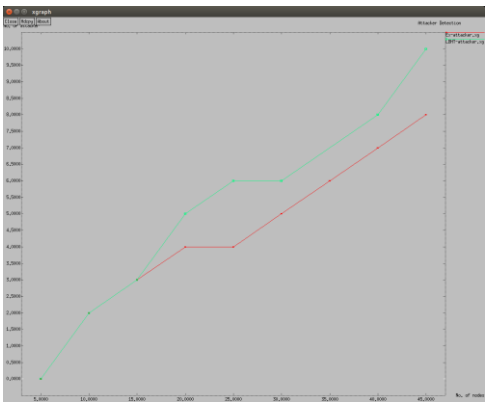

Fig.6: Graph comparing attacker detection efficiency

The above graph compares the existing method and the proposed system with respect to efficiency of attacker detection. The LBHT has a higher attacker detection efficiency compared to the conventional method.

V. CONCLUSION

This study mainly focused on two major issues existing in wireless sensor nodes: lifetime network connectivity and security issues. Traffic aware load balancing was suggested as a solution for lifetime network connectivity and topology hiding was suggested as a solution for security issues like black hole attack, wormhole attack and rushing attacks. The results showed an increase in throughput, attacker detection efficiency, stabilized packet delivery ratio and reduced packet loss. Energy consumption was little higher than the conventional method. So this study can be further extended which may concentrate on reducing the energy consumption factor.

REFERENCES

[1] S. Chen, S. Tang, M. Huang, and Y. Wang, "Capacity of data collection in arbitrary wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 52–60, Jan. 2012.

[2] M. Zhao, Y. Yang ; C. Wang, " Mobile Data Gathering with Load Balanced Clustering and Dual Data Uploading in Wireless Sensor Networks" IEEE Transactions on Mobile Computing, Volume:14, Issue:4,pp 770 – 785, July 2014.

[3] W. C. Cheng, C. Chou, L. Golubchik and Y. C. Wan, "A coordinated data collection approach: Design, evaluation, and comparison", *IEEE J. Sel. Areas Commun.*, vol. 22, no. 10, pp. 2004-2018, 2004

[4] C.K. Toh, A.N. Le, et al., Load balanced routing protocols for ad hoc mobile wireless networks, IEEE Communication Magazine 47 (8) (2009) 78–84.

[5] J.-H. Song , V. Wong and V. Leung, "Load-Aware On-demand Routing (LAOR) Protocol for Mobile Ad Hoc Networks", *Proc. 57th IEEE VTC-Spring*, pp. 1753-1757, 2003

[6] Gerhards-Padilla, N. Aschenbruck, et al., Detecting black hole attacks in tactical MANETs using topology graphs, in: IEEE Conference on Local Computer Networks (LCN), 2007, pp. 1043– 1052.

[7] Y. C. Hu, A. Perrig, et al. Rushing Attacks and Defense in Wireless Ad Hoc Routing Protocols. ACM workshop on Wireless Security (WiSe), pages 30-40, 2003.

[8] Rushing Attacks and Defense in Wireless Ad Hoc Routing Protocols. ACM workshop on Wireless Security

[9] Yujun Zhang, Guiling Wang, Qi Hu, Jie Tian, "Design and performance study of a Topology-Hiding Multipath Routing protocol for mobile ad hoc networks" INFOCOM, 2012 Proceedings IEEE,pp 10-18, March 2012

[10] R. Yamamoto, T. Miyoshi; Y. Tanaka, "Neighbour Traffic-Aware Load Balancing Method in Ad Hoc Networks" IEEE conference on Intelligent Networking and Collaborative Systems (INCoS), pp 193-197, Sep. 2012.

[11] S. Masuda, N. Hagiya, T. Matsuo, Y. Goto, and S. Sakata, "Load-balancing method considering the traffic of relay nodes in ad hoc networks," IEICE Tech. Rep., IN2006-190, vol.106, no.578, pp.61-66, March 2007.

[12] J.Jose, Rigi C.R, "A comparative study of topology enabled and topology hiding multipath routing protocols in MANETs" International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), pp 1-4, Jan 2015.

[13] W. Galuba, P. Papadimitratos, et al., Castor: scalable secure routing for ad hoc networks, in: IEEE Conference on Computer Communications (INFOCOM), 2010.

[14] Rahul K Ghotekar, Deepak C Mehetre, " Load Balancing for Achieving the Network Lifetime in WSN-A Survey" International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp53, May2014