International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 11, November 2014

Efficient Routing Protocol with Security for Transferring the Medical data in Wireless Body Area Networks

M.Pushpavalli[1], P.Mahalakshmi[2], Sanjana Prasad[3], R.Swathi [4]
[1]*Assistant Professor (Sr.G), ECE Department, Bannari Amman Institute of Technology, Erode, India*
[2,3,4]*PG Scholars, ECE Department, Bannari Amman Institute of Technology, Erode, India*

***Abstract*—Wireless Body Area Network (WBAN) technology has significantly increased the potential of remote healthcare monitoring systems. It contains more number of sensors that can be attached directly on the skin or placed under clothes for monitoring vital sign-related data of patients and route this data towards a sink using wireless technology. The data mostly consists of medical information. So, high reliability and low delay is required when routing the data. The medical data of patients can be transferred using the efficient routing protocols. The main objective of this paper is to evaluate the performance of routing protocols and to determine the suitable routing protocol with security for Wireless Body Area Networks. The performance of sensor nodes can be calculated using NS2. The results computed here for throughput, end to end delay. Here, various routing protocol are analyzed and suggest that AODV as the best routing protocol. It increases throughput and reduces delay. In WSN, Secure data transmission is must. So, security key is added with AODV.**

***Index Terms* — Routing metrics, Routing protocol, Security, Wireless Body Sensor Networks (WBSNs)**

I. INTRODUCTION

The new type of network architecture generally known as Wireless Body Sensor Networks (WBSNs) or Wireless Body Area Networks (WBANs) is used for long term continuous monitoring the patients. It has advantages on lightweight, small-size, ultra-low-power, and it is intelligent monitoring Wearable sensors. In WBANs, sensors continuously monitor human physiological activities and actions such as health status and motion pattern. Modern health care related technologies and many other field key technologies rely on it as WBANs have many applications. One of them is medical monitoring which have the specific hardware and network requirements to insure their functions and to solve encountered problems. Sensor, battery, and processor have built up in WBAN. The security of WBAN is also another very critical issue.

WBAN can be used not only on remote patients but also enables to make patients wireless within the hospital, especially, in intensive care units and operating theatres. Not only this would enhance patient comfort but also it would make the work of doctors and nurses a lot more efficient and easy.

The main purpose of the WBAN is to make it possible for patients who need permanent monitoring to be fully mobile. The WBAN is worn by a patient and basically consists of a set of lightweight devices that monitor and wirelessly transmit certain bio signals (vital signs) to a Backend System at a Health care centre. A monitoring healthcare specialist retrieves the patient data over a reliable wired connection. It is a technology for communications in, on and around the human body.

II. ROUTING ISSUES AND CHALLENGES IN WBSNS

A. Network Topology

Proper network topology is very important for WBSNs because of the energy constraint, body postural movements, heterogeneous nature of the sensors and short transmission range. Some protocols use single hop communication, where each node communicates directly with the destination, while others use cluster based multi-hop routing. The proposed routing protocol should adapt for topology changes.

B. Topological Partitioning

The network topology of WBSNs often faces the problem of disconnection or partitioning because of body postural movements and short range transmissions. The proposed routing protocol tried to solve the problem of disconnection and partitioning problem in different ways.

C. Energy Efficiency

Energy efficiency covers both the local energy consumption of nodes and the overall network life time. For implanted bio-medical sensors, it is not possible to replace the power source, while for wearable bio-medical sensors replacing the batteries might lead to discomfort of patients. Therefore, both energy consumption and network lifetime are major challenges in wireless body sensor networks. Communication among the sensor nodes consumes more energy as compared to sensing and processing.

D. Quality of Service (QoS)

In WBSNs, different types of data require different quality of services as it deals with vital signs of the human body. Different data acquires from human body are ECG, EEG, heart beat rate, respiration rate, etc. The proposed protocol need to be aware of the different types of quality of service.

E. Security and Privacy

Like other applications of WSNs, security and privacy are among the basic requirements of WBSNs. It is impossible to apply the conventional techniques of security and privacy because of the low energy availability, limited resources and other constraints. The proposed protocol should take care of the privacy and security of the patient's data while designing routing protocols for WBSNs.

III. ROUTING METRICS

Consider three main routing metrics to determine the efficient routing protocol among AODV (Adhoc On demand Distance Vector), DSR (Dynamic Source Routing), DSDV (Destination Sequence Distance Vector) and TORA (Temporary Ordered Routing Algorithm) for health care applications.

A. Packet Delivery Ratio (PDR)

It is the rate of successfully delivering the data packets to the sink. It is denoted as PDR = (D/S)*100, Where D is the number of packets received by the destination and S the number of packets sent by the source node.

B. Throughput

It is the number of bits successfully received through a network in one second. It is measured in bits per second. It measures how fast data can pass through. The throughput of a node is measured by counting the total number of data packets successfully received at the node and computing the number of bits received, which is finally divided by the total simulation run time.

Throughput of a Node = (Total Data Bits Received)/ (Simulation Runtime).

The throughput of the network is defined as the average of the throughput of all nodes involved in data transmission.

Network Throughput = (Total throughput of nodes involved in data transmission)/(Number of nodes).

C. Average End to End Delay

It indicates difference between the time at which the sender generated the packet and the time at which receiver received the packet.

It indicates the length of time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. The average end-to-end delay of a packet depends on delay at each hop comprising of queuing, channel access and transmission delays and route discovery latency.

IV. VARIOUS ROUTING PROTOCOLS USED IN NS2 ENVIRONMENT

A. DSDV (Destination-Sequence Distance Vector)

DSDV has one routing table, each entry in the table contains: destination address, number of hops towards destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains destination address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old and new route for preventing loop.

DSDV use two types of packet to transfer routing information: full dump and incremental packet. The first time two DSDV nodes meet, they exchange all of their available routing information in full dump packet. From that time, they only use incremental packets to notice about change in the routing table to reduce the packet size. Every node in DSDV has to send update routing information periodically. When two routes are discovered, route with larger sequence number will be chosen. If two routes have the same sequence number, route with smaller hop count to destination will be chosen.

Advantages
(i) Simple routing table format
(ii) Simple routing operation and guarantee loop-freedom.

Disadvantages
Large overhead caused by periodical update. Waste resource for finding all possible routes between each pair, but only one route is used.

B. DSR (Dynamic Source Routing)
In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets.

Route Discovery

If node A wants to set a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started:

1. Node A (initiator) sends a Route Request packet by flooding the network.
2. If node B has recently seen another Route Request from the same target or if the address of node B is already listed in the Route Record, Then node B discards the request.
3. If node B is the target of the Route Discovery, it returns a Route Reply to the initiator. The Route Reply contains a list of the "best" path from the initiator to the target. When the initiator receives this Route Reply, it caches this route in its Route Cache for use in sending subsequent packets to this destination.
4. Otherwise node B isn't the target and it forwards the Route Request to his neighbors (except to the initiator).

Route Maintenance
In DSR every node is responsible for confirming that the next hop in the Source Route receives the packet. Also each packet is only forwarded once by a node (hop-by-hop routing). If a packet can't be received by a node, it is retransmitted up to some maximum number of times until a confirmation is received from the next hop.

Only if retransmission results then in a failure, a Route Error message is sent to the initiator that can remove that Source Route from its Route Cache. So the initiator can check his Route Cache for another route to the target. If there is no route in the cache, a Route Request packet is broadcasted.

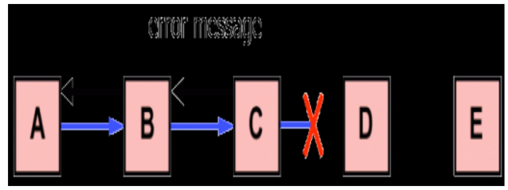


Fig. 1 Transmission of Error message

1. If node C does not receive an acknowledgement from node D after some number of requests, it returns a Route Error to the initiator A.
2. As soon as node receives the Route Error message, it deletes the broken-link-route from its cache. If A has another route to E, it sends the packet immediately using this new route.
3. Otherwise the initiator A is starting the Route Discovery process again.

Advantages
Reactive routing protocols have no need to periodically flood the network for updating the routing tables like table-driven routing protocols do. Intermediate nodes are able to utilize the Route Cache information efficiently to reduce the control overhead. The initiator only tries to find a route (path) if actually no route is known (in cache). Current and bandwidth saving because there are no hello messages needed (beacon-less).

Disadvantages
The Route Maintenance protocol does not locally repair a broken link. The broken link is only communicated to the initiator. The DSR protocol is only efficient with less than 200 nodes. Problems appear by fast moving of more hosts, so that the nodes can only move around in this case with a moderate speed. Flooding the network can cause collusions between the packets. Also there is always a small time delay at the beginning of a new connection because the initiator must first find the route to the target.

C. TORA (Temporary Ordered Routing Algorithm)

TORA is based on link reversal algorithm. Each node in TORA maintains a table with the distance and status of all the available links. TORA has three mechanisms for routing:

Route Creation: TORA uses the "height" concept for discovering multiple routes to a destination. Communication in TORA network is downstream, from higher to lower node. When source node does not have a route to destination, it starts Route Creation by broadcasting the Query messages (QRY). QRY is continuing broadcasted until reaching the destination or intermediate node that have the route to the destination. The reached node then broadcast Update (UPD) message which includes its height. Nodes receive this UPD set a larger height for itself than the height in UPD, append this height in its own UPD and broadcast. This mechanism is called reversal algorithm and is claimed to create number of direct links from the originator to the destination.

Route Maintenance: Once a broken link is discovered, nodes make a new reference height and broadcast to their neighbors. All nodes in the link will change their reference height and Route Creation is done to reflect the change.

Route Erasure: Erases the invalid routes by flooding the "clear packet" through the network.

Advantages

It having multiple paths to destination decreases the route creation in link broken case therefore decrease overhead and delay to the network. TORA is also claimed to be effective on large and mildly congested network.

Disadvantages

It requires node synchronization due to "height" metric and potential for oscillation. Besides that, TORA may not guarantee to find all the routes for reserving in some cases

D. Efficient Routing Protocol
AODV (Adhoc On Demand Distance Vector)

In AODV, each node maintains one routing table. Each routing table entry contains:
(i) Active neighbor list: a list of neighbor nodes that are actively using this route entry. Once the link in the entry is broken, neighbor nodes in this list will be informed.
(ii) Destination address
(iii) Next-hop address toward that destination
(iv) Number of hops to destination
(v) Sequence number: for choosing route and prevent loop
(vi) Lifetime: time when that entry expires

Routing in AODV consists of two phases: Route Discovery and Route Maintenance.
When a node wants to communicate with a destination, it looks up in the routing table. If the destination is found, node transmits data in the same way as in DSDV.
If not, it start **Route Discovery mechanism**: Source node broadcast the Route Request packet to its neighbor nodes, which in turns rebroadcast this request to their neighbor nodes until finding possible way to the destination. When intermediate node receives a RREQ, it updates the route to previous node and checks whether it satisfies the two conditions: (i) there is an available entry which has the same destination with RREQ (ii) its sequence number is greater or equal to sequence number of RREQ. If no, it rebroadcast RREQ. If yes, it generates a RREP message to the source node.
When RREP is routed back, node in the reverse path updates their routing table with the added next hop information. If a node receives a RREQ that it has seen before (checked by the sequence number), it discards the RREQ for preventing loop. If source node receives more than one RREP, the one with greater sequence number will be chosen. For two RREPs with the same sequence number, the one will less number of hops to destination will be chosen.
During route discovery from the source to the destination the energy values along the route are accumulated in the RREQ packets. At the destination or intermediate node (which has a fresh enough route to the destination) these values are copied into the Route Reply packet (RREP) which is transmitted back to the source. The source considers the maximum remaining energy capacity route and minimum mobility route every time it performs route discovery. This action will make the AODV routing protocol choose an alternative node or change the whole route to the destination node.
When a route is found, it is maintained by **Route Maintenance mechanism**: Each node periodically send Hello packet to its neighbors for proving its availability. When Hello packet is not received from a node in a time, link to that node is considered to be broken. The node which does not receive Hello message will invalidate all of its related routes to the failed node and inform other neighbor using this node by Route Error packet. The source if still want to transmit data to the destination should restart Route Discovery to get a new path.

Advantages

- Decreasing the overhead control messages
- Throughput increases, delay decreases
- Quick adapt to network topology change
- More scalable up to 10000 mobile nodes

Disadvantage

AODV only accepts bi-directional link and has much delay when it initiates a route and repairs the broken link.

V . RESULTS AND DISCUSSION

Software used : NS 2.35 (Network Simulator)

Operating system : Fedora

Packets (Medical data of patients) are transmitted from Body sensors to doctor in hospital, mobile (in movement) and home receiver via Access Point. The sensor can be attached to any one of the portion (e.g. ECG sensor for monitoring heart condition) of the body of patients.

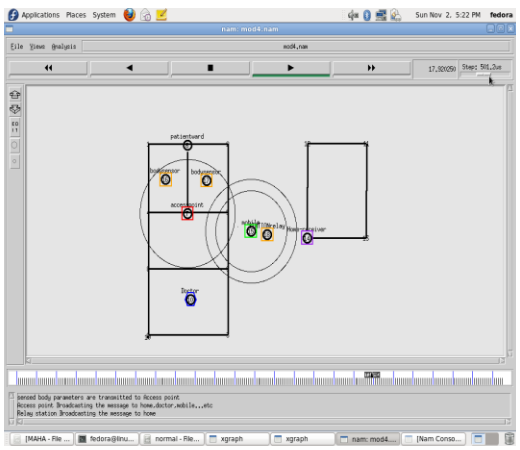


Fig. 2(a) Transmission of patient data (packets) to doctor, home receiver, mobile

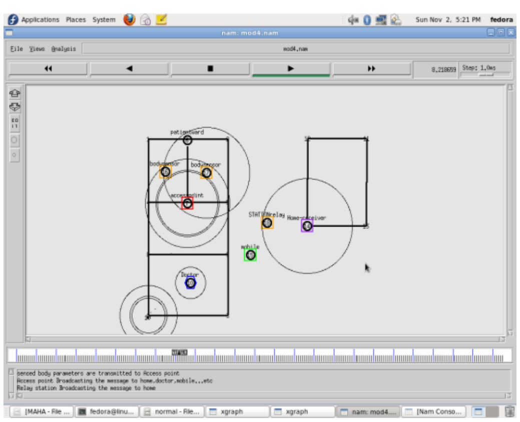


Fig. 2(b) Transmission of patient data (packets) to doctor, home receiver, mobile

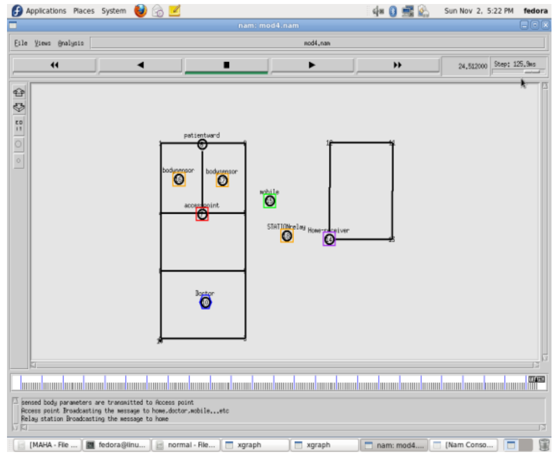


Fig. 2(c) Transmission of patient data (packets) to doctor, home receiver, mobile

A. Security Key added with AODV protocol for Secure Communication

The security key is provided for patients, doctors, home receiver and mobile for secure communication of patient data between them. When the medical data is transferred from body sensor, the data can be encrypted using security key. Doctor or anyone can decrypt that data using the key.

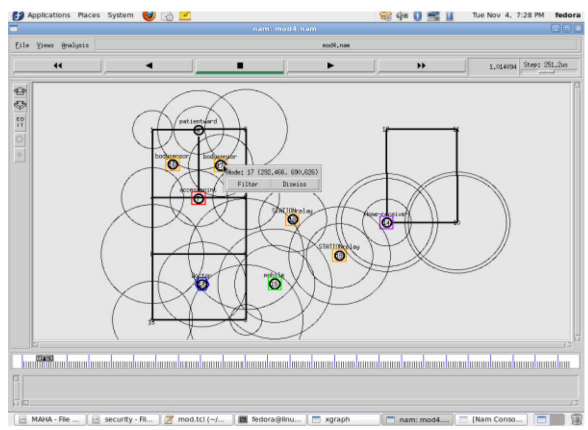


Fig. 3(a) Secure transmission of Patient data using security key

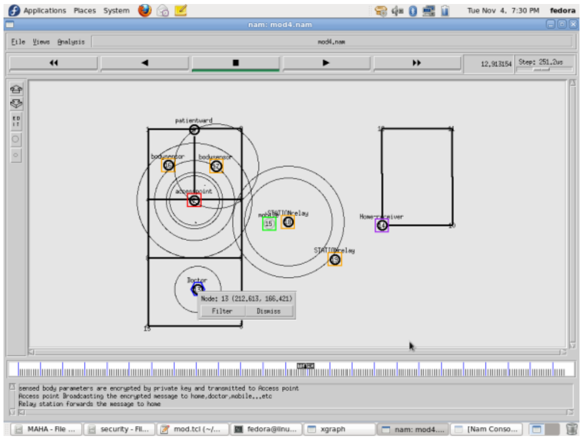


Fig. 3(b) Secure transmission of Patient data using security key

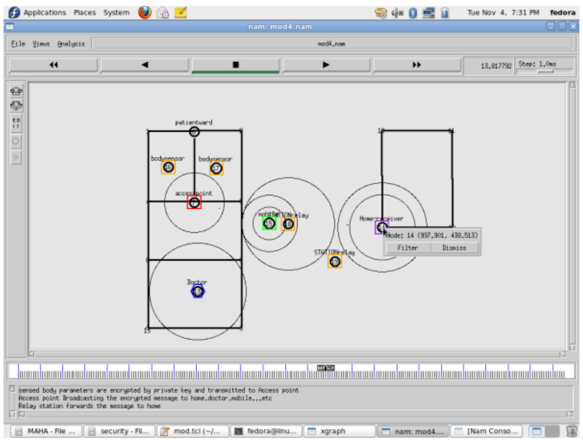


Fig. 3(c) Secure transmission of Patient data using security key

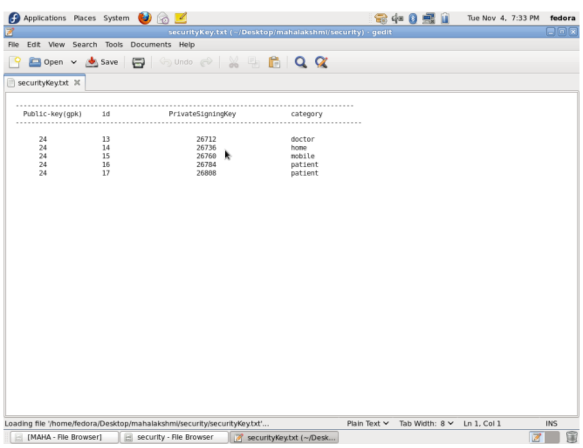


Fig. 3(d) Security key provided for doctor, patients, home, station and mobile

B. Throughput calculation for using AODV with security protocol in WBAN

TCL- Tool Command Language
It generates trace file with all simulation events in NS2 recorded in it.
Throughput can be calculated by using awk script which processes the trace file and produces the result in x-graph with .xg extension and it is plotted. The graph is plotted between time in seconds and throughput in bytes. It is calculated for time to time.

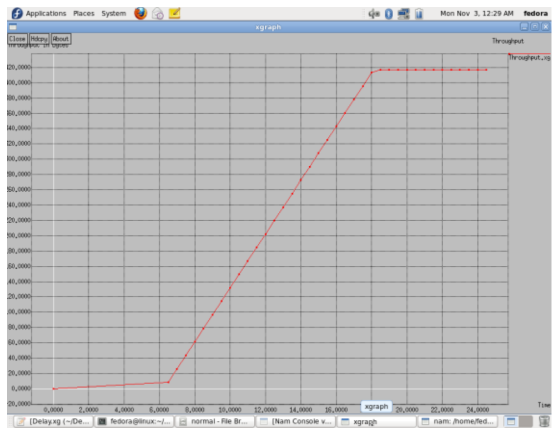


Fig. 4(a) Throughput calculation for AODV protocol

X axis: time in seconds

Y axis: throughput in bytes

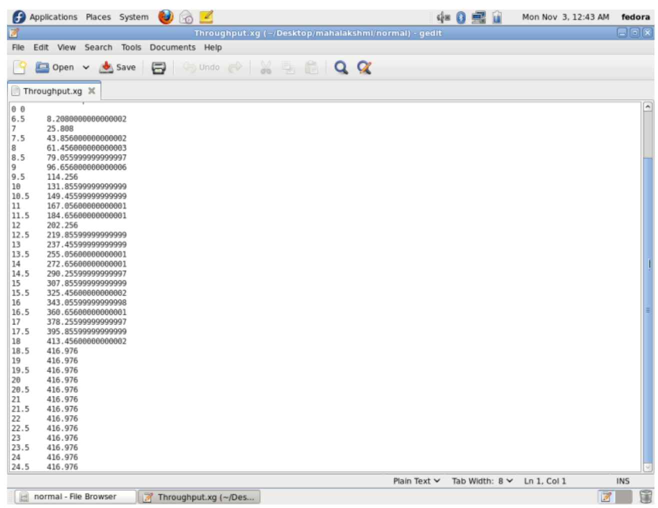


Fig. 4(b) Throughput calculation for AODV protocol

C. Average end to end delay calculation for using AODV with security protocol in WBAN

The average end to end delay can be calculated by using awk script which processes the trace file and produces the result in x-graph with .xg extension and plotted. It is calculated for time to time.
The graph is plotted between time in seconds and end-to-end delay in milli seconds.

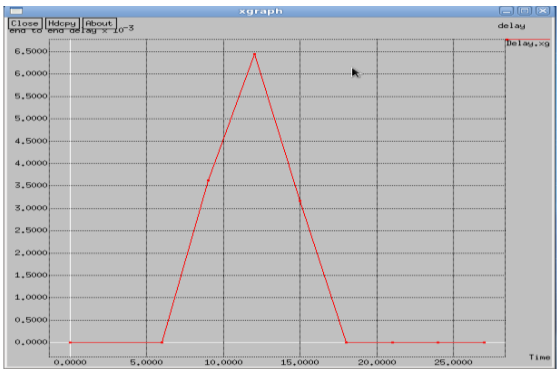
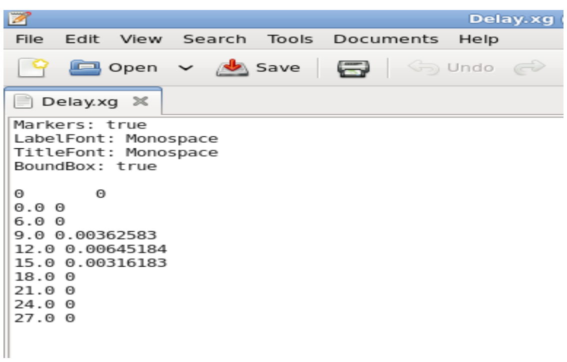


Fig. 5 Average End to End Delay calculation



X axis: time in seconds

Y axis: end to end delay in ms

VI. CONCLUSION

Investigations made on wireless mobile routing protocols like DSDV, AODV, DSR and TORA using CBR application in wireless sensor network. Quality of service metrics (average end-to-end delay, throughput) are used to compare those routing protocols. The findings suggest that AODV with security produces highest throughput with minimum delay with and without mobility. Therefore this routing protocol is the suitable one for Wireless Body Area Networks for data transmission. Security added with AODV used to transfer the secure data packets between the nodes. It achieves good throughput and minimum end to end delay in NS2 environment.

REFERENCES

[1] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman and K. S. Kwak, "A Comprehensive Survey of Wireless Body Area Networks on PHY, MAC, and Network Layers Solutions," *Journal of Medical System*, Vol. 36, No. 3, 2012, pp. 1065-1094.

[2] A. Bhatia and P. Kaushik, "A Cluster Based Minimum Battery Cost AODV Routing Using Multipath Route for Zigbee," *ICON* 2008 16*th IEEE International Conference on Networks*, New Delhi, 12-14 December 2008, pp. 1-7.

[3] N. Golmie, D. Cypher and O. Rebala, "Performance Analysis of Low Rate Wireless Technologies for Medical Applications," *Computer Communications*, Vol. 28, No. 10, 2005, pp. 1266-1275.

[4] S. Mohanty, "Energy Efficient Routing Algorithms for Wireless Sensor Networks and Performance Evaluation of Quality of Service for IEEE 802.15.4 Networks," Mas- ter's thesis, National Institute of Technology, Rourkela, Orissa, 2010.

[5] C. Perkins, E. Royer and S. Das, "Ad hoc On Demand Distance Vector (AODV) Routing," The Zone Routing Protocol, Internet Draft,1999.

[6] Quwaider, M.; Biswas, S. Probabilistic Routing in On-Body Sensor Networks with Postural Disconnections. In Proceedings of the 7th ACM International Symposium on Mobility Management and Wireless Access, Tenerife, Canary Islands, Spain, 27–30 October 2009; pp. 149–158. *Sensors* **2014**, *14* **1354.**

[7] Quwaider, M.; Biswas, S. DTN routing in body sensor networks with dynamic postural partitioning. *Ad Hoc Netw.* **2010**, *8*, 824–841.

[8]Kandris, D.; Tsioumas, P.; Tzes, A.; Nikolakopoulos, G.; Vergados, D.D. Power conservation through energy efficient routing in wireless sensor networks. *Sensors* **2009**, *9*, 7320–7342.

