Hybrid Routing Protocol for Wireless Body Area Networks

Prabhjot Kaur, Sandeep Singh Kang

Abstract: ***Healthcare is an application where the Wireless Body Area Network (WBAN), the emerging field of Wireless Sensor Network (WSN), can give assistance to the person in case of detection of abnormal activities of the human body without demanding the presence of the doctor. The small-sized sensors can be deployed for continuous monitoring of the physical activities of the human body. In the case of abnormal activity, the sensors will alert the person as well as share the data with the health expert. The information to be sent is very critical so the routing nodes selection must be done in such a manner that the malicious nodes will not get the information. There are various factors which we can count as the selection parameters for taking a node as part of the route. The Trust of the sensor node is very important as if the node is not trustworthy the chances of delivering correct data to the destination node are very less. This may lead to a threat to a person's life. In this paper we are presenting a routing algorithm which will count the trust of the node as an important factor and update the path if it found any malicious node in between the route.***

Index Terms: ***Wireless Body Area Networks, Quality of Service, routing challenges, routing protocols in WBAN, applications of WBAN***

I. INTRODUCTION

Healthcare is most a promising application of Wireless Body Area Networks as it concerns with the physiological parameters as well as psychological conditions of the person. With the availability of the deployable tiny sensors during the hectic lifestyle and the costly healthcare, the sensors which can help in health monitoring are preferred to assist the human in the absence of the health expert. Various sensors are available which are of tiny size and can be easily deployed/implanted on human body for observing the activities of a person on regular basis. The device through which the person is getting the information sent by the sensor nodes will help to improve his health condition. The physiological parameters which can be monitored by these sensor nodes are heart rate, body temperature, glucose level, and blood pressure of the person. These parameters can be useful in observing and detecting the health condition and the behavior of the person. The tiny sensors, which are capable of sensing the activities of the human body, will be deployed on the body and communicate with each other as well as with the health center through a wireless medium. This will create a wireless body area network where the nodes deployed on the human body communicate with each other and sharing the information with the health center.

Figure 1 represents the Wireless Body Area Network (WBAN) where the small sized nodes are deployed on human body and they are communicating with each other for sharing the information they have collected to the control unit or to medical centre. For communication, the topology used in WBAN is Star Topology. The central node is deployed on the human body and it will collect the information from the nodes deployed at a distance of 1.5m away from the central node.

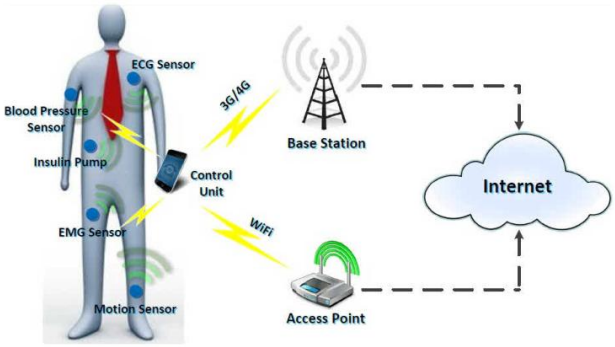

Figure 1: Wireless Body Area Network

The central node is the master node to which rest of the nodes, the slave nodes, will send the information collected. The central node can be a Personal Digital Assistant device to which nodes will pass the information and the device will share this information with the external medical server. This device is equipped with computational capabilities, enough energy resources, and memory space to operate efficiently. The areas of applications are very wide when we discuss Wireless Body Area Networks. There are various applications like healthcare, rehabilitation, military, interactive gaming, etc. Healthcare is one of the important applications of WBAN. The deployed sensors will assist the person in the absence of a health expert. Similarly, in Rehabilitation the sensor nodes can play an important role. The sensor nodes can alert a person about exercise he requires to recover to his normal routine. In the military, the sensor nodes can continuously monitor the health condition of the person and can alert the person to take appropriate action on time [14]. Similarly, for making gaming more interactive, the sensor nodes can be deployed on the person's body for visualizing during the game [15]. The routing of the information is a challenge in Wireless Body Area Networks. The routing algorithms used in WSN cannot be used for routing in WBAN as the architecture and application model of WBAN is different from WSN.

Revised Manuscript Received on August 05, 2019.

Prabhjot Kaur, Department of Computer Science & Engineering, Chandigarh University, Mohali, India.
Sandeep Singh Kang, Department of Computer Science & Engineering, Chandigarh University, Mohali, India.

As the nodes are to be implant in the human body, it is not easy to change the sensors again and again by operating the person. So the sensors must be energy efficient that is the node must use its energy efficiency to share the information by observing the distance between the nodes, the importance of the data, etc. Another challenge for routing in WBAN is the Fault tolerance ability of the sensor. As the data sensed by the sensor node is very critical to the link failure can cause harm to the person's life. So, the node must be able to handle the link failure if any there.

Secure and reliable communication between the nodes is another major challenge in WBAN. The unattended and unsupervised nature of the nodes can lead the nodes to be attacked or captured physically. The data must be handed over to the trustworthy node as the data is very critical and private. If the node is not trustworthy, there is no surety of transmission of the correct data to the destination. While sharing the information, the node must verify whether the next node is trustable or not. The next node may possibly drop the packets during forwarding the packets or pass the packets to another misbehaving node with false intentions. As the data transmitted in WBANs is of sensitive and critical nature so any threats, vulnerabilities in these networks are of main concern.

The traditional encryption methods are not suggested to be used for securing the information in these networks as the algorithms require more computational power as well as more energy to encrypt the information which can diminish the lifetime of the nodes and the network. It is preferable to detect the misbehaving nodes before passing the information directly to the next node. It can reduce the chance of manipulation of information until it reaches the destination.

In this paper, we are proposing a hybrid routing algorithm which considers the trust, temperature factor while transmitting the data and mobility parameter to deal with the link failure. The node as a forwarder node will be selected in such a manner that it will hand over the data only to the trustworthy node and can keep in count the temperature of the node. To deal with the link failure due to the mobile nature of nodes, the node will re-route the path and transmit the data through another path instead of discarding the packets.

The rest of the paper is organized as follows: In section II, the related work studied is discussed. In section III, the proposed scheme is discussed. In section IV, discussion about results is done and the last section concludes the discussion made in the above sections.

II. LITERATURE REVIEW

Routing is an important aspect of WBAN as the data collected by every the sensor node is very critical and it is important to share the collected information with the sink node as well as with the medical server on the time but by keeping the routing constraints in focus. In [28] various routing challenges for routing like power supply issues, quality of service, reliability of data, the lifetime of network etc. are discussed.

The On-Demand routing protocols basically work in three phases: Trust estimation phase- checks for the trustworthiness of the node, route discovery- looks for the reliable route for transmission of data and route maintenance phase- deals with the link failure. There are various routing algorithms proposed to improve the network's performance by including the various factors like temperature, mobility, trust factor, and energy consumption of the sensor nodes.

Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. [23], proposed a Trust and Energy aware routing protocol. The trust, both direct and indirect, of each node is calculated on the basis of the packet forwarding behavior and the estimated positive probability. The value of this composite function will choose which node can participate in routing. The composite function includes the node's trust value, the residual energy and the number of the hops in between to calculate the value. The two conditions are considered which can cause link failure during routing. The first one is the residual energy of the node. If the node's remaining energy is not enough to forward the packet. The second case is when the misbehaving nature of the node is detected. Then the source node is notified about this and re-routing is done.

Alshamsi, A. Z., & Barka, E. S. [24], proposed an energy efficient routing algorithm which covers the security of the data while routing by using lightweight encryption algorithm. The data during transmission will be in encrypted form and only the end nodes can decrypt that information. The use of encryption algorithms can consume the more energy of the node for encrypting and decrypting the data.

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. [5], gives a review on the various challenges like technology selection, routing challenges, security issues etc. for Wireless Body Area network. For the accurate communication the selection of appropriate technology is an important task. The routing challenges can be there while designing the routing protocol on the basis of various parameters like energy efficiency, temperature factor, trust, Quality of Service etc.

Bhangwar, A. R., Kumar, P., Ahmed, A., & Channa, M. I. [17], proposed a routing protocol which selects the route by counting on the temperature and the trust value of the node. A threshold value is set for both the trust and temperature of the node. If the trust is below the threshold and the temperature is above the threshold, then the node will not be allowed to take participate in routing. By using this algorithm the chances of misleading/misguiding the data is very less as it will allow only the trustworthy nodes to participate in the routing. The temperature factor will help in selecting the nodes whose temperature is lower than the threshold temperature specified to avoid the tissue damage of the human body. This will help in reducing the participation of misbehaving/ faulty nodes in the routing.

Javaid, N., Ahmad, A., Nadeem, Q., Imran, M., & Haider, N., [29] a mobility supportive routing algorithm is proposed by the authors. The movement of the can cause the reorganization of the network topology which can utilize the more energy of the nodes. For source to destination data transmission, multi-hop communication is used. The sink shares its location with the rest of the nodes of the network.

A cost function is calculated on the basis of the distance of sink from the sender node and the residual energy of the sender node. The node with the least cost function value will be selected by the sink as the forwarder node. When the node moves towards the sink node, it will create link with the sink or the forwarder node and if it moves away from the sink, the path loss is very high.

Javaid, N., Abbas, Z., Fareed, M., Khan, Z., & Alrajeh, N. [23], proposed a protocol named M-ATTEMPT which supports the mobility of nodes. The nodes were deployed in descending manner of their data rates. The nodes with high data rate can send the data directly and can easily collect the data from the node having lower data rates and pass it to the sink node. If the node gets disconnected from its parent node and goes to the coverage range of other parent node then it will send a join-request to the parent node. The parent node will check if the child nodes of it are less than 3 then it will accept the join-request of the node otherwise reject it. The stability period of network is improved as compare to the multi-hop communication.

Kim, B.-S., Kim, K., & Kim, K.-I.[31], gives a review on the significance of the mobility in WBAN various mobility models are discussed which provides the information about the different movement patterns and the location changes with the movement of the human body.

The human body can't be in same position for long time, motion is always there. So when the nodes are to be deployed on the body, the mobility factor must be considered as due to the mobility there can be link failure during the transmission of data which can affect the person's life. The data must reach on time to the sink node so that the appropriate actions can be taken. There are various routing algorithms are proposed by various authors which supports the mobility of nodes during the routing.

Navya, V., & Deepalakshmi, P.[27], M-TSIMPLE another mobility based protocol is proposed which computes the cost function on the basis of distance and the residual energy. The nodes were divided into two categories parent nodes and the child nodes. The parent nodes here use the TDMA to give time slots to the child nodes for sharing their data. The Parent-Child forwarder behavior reduces the path-loss as compared to multi-hop communication. The stability, throughput and lifetime of the network is improved as only relevant data is transmitted and redundant data is not transmitted.

Roy, M., Chowdhury, C., Kundu, A., & Aslam, N. [21], proposed a trust based algorithm which integrates with the existing AODV algorithm and it calculates the trust of the node by using the Non-homogeneous Poisson distribution. The sender node sends the route request to another node and waits for the route reply from that node. The sender node pre-calculates the delay for receiving route reply packet from other node on the basis of distance. If the node takes more time as compared to the pre-computed delay then the node is marked as a suspected node and the sender node will not send the data through that node. The malicious nodes can be detected by using this algorithm.

Salman, F & Atia, H [19], proposed the routing algorithm which uses the concept of fuzzy logic to make the network energy efficient. By using the residual energy, Received Signal Strength Indicator, and distance from source to destination, the base station calculates the fuzzy cost for each node. The node with the least fuzzy value will be selected as Cluster Head and rest of the nodes of the network will pass use TDMA method to send the information to the selected cluster head. It reduces the energy consumption of each node by avoiding the continuous sensing of the channel for transmitting the information.

Sethi, D., & Bhattacharya, P. P.[22], proposed an Energy Efficient and Reliable Data Transfer (EERDT) protocol for WBAN. The transmission of critical data is done by single-hop communication. A cost function is calculated for each node and the node with high cost function value is elected as a parent node. The higher the cost function value is the higher the chances of selection as parent node. Rest of the nodes of the network will choose their cluster heads on the basis of the distance between them and the cluster head. The stability of the network is improved by using this protocol.

As we reviewed many papers which check the trust value and temperature value of the node before passing the information. The trust is calculated by observing the packet forwarding behavior of node and the delay in the reply from other node. But we have observed that some nodes are not able to send the reply back on time due the busy channel. The mobility support is not included when trust and temperature factors are considered. So, in this we are proposing a routing algorithm which will support mobility while computing the cost function by considering trust and temperature of the nodes.

III. RESEARCH METHODOLOGY

This section is divided into two sections, first includes the flowchart and second section explains the proposed methodology of the proposed model/ There are some assumptions made while designing the protocol. These assumptions are as follow:

1. The source and destination nodes are trustworthy nodes.
2. The source and destination node can't be hotspot.
3. The source and destination has always the sufficient energy to send/receive the data.
4. The source and destination node will not get affected by the intruder.

The node selection for routing the data packet is done on the basis of the trust and the temperature factor of the node. The node with the more trust value and less temperature value will be selected for the routing. A composite function is calculated for all possible routes. The route with the less function value will be selected for routing.

During the routing there are the chances of link failure as the nodes can be displaced from their actual position with the movement of body. In the third step the route maintenance phase comes under the light. Here the node which is became faulty node will send the error message to the predecessor node which again finds for the route to the destination if succeed, the routing continues otherwise it returns the packet to the source node and source node choose the new route for transmission.

1) Proposed Methodology

The algorithm is divided into three phases according to its functionality. First Phase includes the initialization of nodes. Second Phase includes the route discovery method and third phase deals with the route maintenance in case of any link failure.

A) Initialization Phase

The nodes in the network will have a unique node_id, location, and trust and temperature value. The sink node keeps the record of the nodes available in the network. In initialization phase the sink node broadcasts its node_id and location. The nodes in the network will send their information to the sink node. The figure 2 represents the broadcast of sink's node_id and location information to rest of the nodes.

The node if any in network has some data to share with the coordinator node will initialize the route discovery phase in which it will choose appropriate route for sending the data.

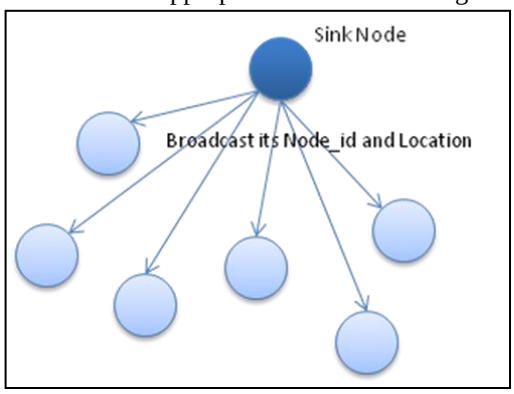

Figure 2: Initialization Phase

B) Route Discovery Phase

The network model of proposed algorithm contains the biomedical sensors and the relay nodes. The proposed model uses the connectivity graph shown in eq. 1.

$$G = (V, E, W) \quad (1)$$

Here the V indicates the set of biomedical and relay nodes, such that V = $\{B_n\} U \{R_n\}$. The B_n represents the all Biomedical nodes and R_n represents all relay nodes whereas E represents the links between both kind of sensor nodes $\{e_1, e_2, \ldots\ldots e_n\}$ and W represents the link metrics.

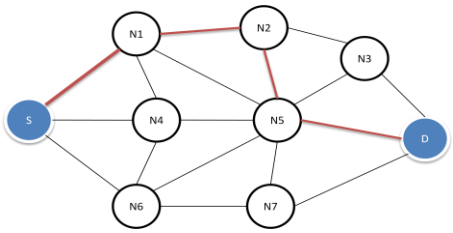

Figure 3: Route Selected

The trust and the temperature of the node are also calculated in this phase. The trust of the node is considered in two ways direct trust and indirect trust. The trust is calculated on the basis of the packet forwarding behavior of the node. The direct trust is when the next node itself a destination node. For calculating the indirect trust of the node the overhearing nature of the neighbor nodes is used. The next node which is going to receive the packet from current node will keeps the record of the packet received and sent by the current node.

If the current node drop some packets in between or try to send wrong packets then current node will be marked as malicious node.

$$Trust_{Ni,Nj}(t) = DT_{Ni.Nj}(t) + \frac{IT_{NiNj}^{Nk}}{NR_{Nj}}(t)$$

The Trust of nodes can be some fractional value between 0 and 1. The figure 3 shows the Total Trust calculated for the node.

Algorithm 1: TMRP Algorithm

1. Set n_{prec}<- Predecessor node
2. Set n_{curr}<- Current node
3. Set n_{next}<- Successor node
4. Set $Tr_{threshold}$<- Trust Threshold
5. Set $Tp_{threshold}$<- Temperature Threshold

6. **procedure** *Initialization Phase*
7. Initialize each node
8. Broadcast node_id and location of Coordinator node
9. **end procedure**

10. **procedure** *Route Discovery*
11. **while** node has packet to send **do**
12. **if** next node n_{next} destination **then**
13. Send pkt_{data} directly
14. **end if**
15. **if** relay node n_{curr} receives packet pkt_{data} from n_{prec}
16. Check routing table for next node n_{next}
17. **if** Trust of n_{next} < $Tr_{threshold}$ **then**
18. **Call procedure** *Route Maintenance*
19. **while** route reply not received **do**
20. Buffer packet pkt_{data}
21. **end while**
22. **end if**
23. **if** Trust of n_{next} < $Tp_{threshold}$ **then**
24. **Call procedure** *Route Maintenance*
25. **while** route reply not received **do**
26. Buffer packet pkt_{data}
27. **end while**
28. **end if**
29. **if** node position changes **then**
30. **Call procedure** *Route Maintenance*
31. **while** route reply not

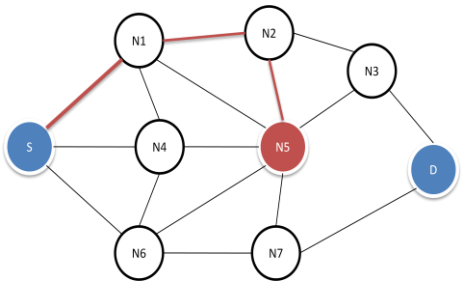

Figure 4: Link Failure

The $Trust_{Ni.Nj}$(t) indicates the total trust of node N_i over N_j at *t* time. *DT* indicates the direct trust of node N_i over node N_j at *t* time. *IT* indicates the indirect trust of the node N_i over node N_j obtained through node N_k at *t* time. The NR_{Nj} indicates the total number of neighbor relay nodes of the node N_j.

If the trust value of current node is less than equal to 0.55 then the current node will not be considered as a trustworthy node.

Similarly the temperature of the node is also considered as if the temperature of node increases; it may become the hotspot and can damage the body tissues. With the packet sharing the temperature rise by 0.1 every time the node send a packet. To avoid the participation of the hotspot node the threshold temperature is marked of value 7.18. If the value of temperature of the current node is greater than 7.18 than it will be considered as hotspot and can't be selected for the routing.

The composite function is calculated which considers the both the factors of the node i.e. the trust and the temperature value of the node. The equation eq. 2 includes the composite function.

$$CF = w1 * Trust + w2 * Tempertaure \quad (2)$$

The *w1* is weight for the trust factor and *w2* is weight for temperature factor for the node. The average value for weight is 0.47 i.e. both the factors are equally important for the selection of the route.

The algorithm 1 explains the proposed algorithm. All the three phases are described in this algorithm.

C) Route Maintenance Phase

The unsteady nature of nodes can cause the link failure during the transmission of data. The location of the sensor nodes deployed on the human body changes with the movement in the human body. The following diagram Figure 3 represents the route selected for the routing from source to destination.

The three possible situations are considered for the link failure. First scenario considered is when the node's trust value is below the threshold trust. Second scenario is when the temperature of the current node is higher than the threshold temperature. The last scenario considered is the link failure due to the displacement of the current node. The following diagram Figure 4 shows the misbehaving node N5 where the link failure occurred.

When the link failure occurs during the routing due to above mentioned situations, then to deal with it route maintenance phase generates a Route Error Report which contains the error message and sends this report to the previous node. The node again looks for other possible route for transmission.

If the previous node fails to find another node the error report will be forwarded to the Source node where the source node will check for other possible route and retransmit the data.

2) Flow Chart

The Figure 5 explains the working of the proposed algorithm. In the very first step when the nodes are deployed the sink node will send the initialization packet to the all deployed nodes which includes the information about the node. The packet includes the node_id and location of the sink node. After that the rest of the nodes will share their unique node_id and location information with sink node.

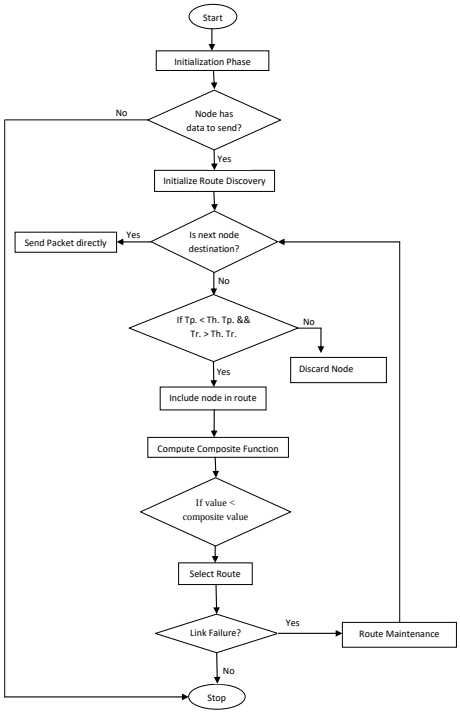

Figure 5: Flow Chart

When a node has data to send to sink node it will initialize the route discovery phase. So, in the second step the node sends the route request packet to its neighbor nodes. The nodes which have the path towards the destination node will reply back with route reply packet.

IV. COMPARATIVE ANALYSIS

The simulation of proposed method is done on MATLAB software. The used parameters in simulation are described here in Table 1. We have considered two circumstances here. First situation where the malicious node tries to attacks the nodes of the route. Second situation is where the nodes are dealing with the temperature increase in network.

The proposed protocol is compared with the existing trust and temperature aware routing algorithm TTRP.

Table 1: Parameters considered

Parameter	Value
Simulation area	1m*1m
Range	200
Threshold Trust	0.55
Threshold Temp	7.18
Function Value	2.40
Avg, wt.	0.47

The Packet Delivery Ratio is the ratio of received packets over the total transmitted packets. The figure 6 shows the comparison of packet delivery ratio of TTRP and proposed algorithm. The packet delivery ratio of the TTRP is low as in this protocol the mobility of the node is not considered while routing the packets. The packet drop is more in TTRP as the link failure occurred due to the mobility is neglected.

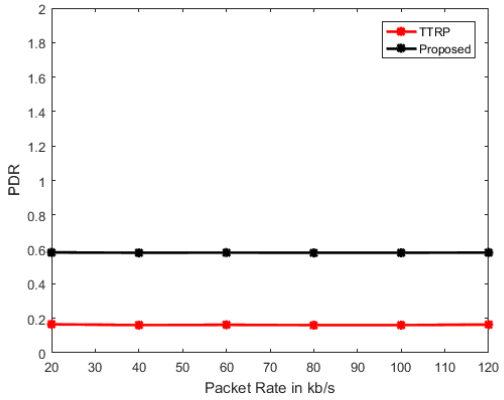

Figure 6: PDR versus Packet Rate

The end-to-end delay in a network is defined between a packet is generated at source to the time it is received by the destination. The presence of malicious nodes leads to the frequent link failures in TTRP and packet drops are more in this protocol which increases the average end-to-end delay.

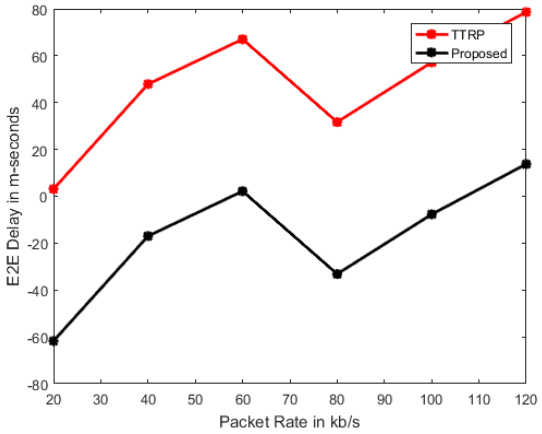

Figure 7: E2E Delay Versus Packet rate

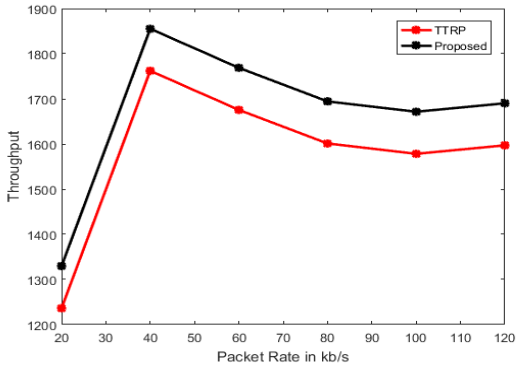

Figure 8: Throughput versus Packet rate

Figure 7 shows the comparison of both algorithms' End-to-end delay. In propose algorithm the end-to-end delay is less as the link failure is handled at the predecessor node. Throughput is the amount of packets successfully transmitted from one node to another node in a given period of time. The figure 8 shows the comparison of throughput of the both algorithms. The throughput of proposed algorithm is more as compared to the existing TTRP protocol. As the data is only forwarded to the trustworthy nodes so the chances of packet drop are very less.

V. CONCLUSION

In this paper, we propose a hybrid routing protocol (HRP) for Wireless Body Area Networks which efficiently secures the network against the misbehaving nodes. This proposed protocol efficiently handles the link failure issue due the mobility factor of nodes. The node instead of dropping the packets notifies the previous sender node to search for other route for sending packets. We compare the proposed algorithm with the existing trust and temperature aware routing protocol TTRP. It is noticed that the throughput, packet delivery ratio is improved in proposed algorithm. The end-to-end delay is reduced in the proposed algorithm. Our future direction focus will be on the performance of the network during the external interference when two human bodies deployed with sensor nodes come in the range of each others.

ACKNOWLEDGMENT

This is my sincere gratitude to Dr. Sandeep Singh Kang, Professor, Department of Computer Science & Engineering, Chandigarh University, India for providing me guidance and motivating me to learn. I am truly thankful to him for guiding me through the entire paper.

REFERENCES

1. \ Roy, M., Chowdhury, C., & Aslam, N. (2017). Designing an energy efficient WBAN routing protocol. *2017 9Th International Conference On Communication Systems And Networks (COMSNETS)*. doi: 10.1109/comsnets.2017.7945390
2. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, *18*(2), 113-122. doi: 10.1016/j.eij.2016.11.001

3. Negra, R., Jemili, I., & Belghith, A. (2016). Wireless Body Area Networks: Applications and Technologies. Procedia Computer Science, 83, 1274–1281.doi:10.1016/j.procs.2016.04.266
4. Toor, A., & Jain, A. (2016). A survey of routing protocols in Wireless Sensor Networks: Hierarchical routing. *2016 International Conference On Recent Advances And Innovations In Engineering (ICRAIE)*. doi: 10.1109/icraie.2016.7939555
5. Ling, Z., Hu, F., Wang, L., Yu, J., & Liu, X. (2017). Point-to-Point Wireless Information and Power Transfer in WBAN With Energy Harvesting. *IEEE Access*, *5*, 8620-8628. doi: 10.1109/access.2017.2695222
6. Poon, C., Yuan-Ting Zhang, & Shu-Di Bao. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, *44*(4), 73-81. doi: 10.1109/mcom.2006.1632652
7. Huang, H., Gong, T., Ye, N., Wang, R., & Dou, Y. (2017). Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System. *IEEE Transactions On Industrial Informatics*, *13*(3), 1227-1237. doi: 10.1109/tii.2017.2687618
8. He, D., Zeadally, S., Kumar, N., & Lee, J. (2017). Anonymous Authentication for Wireless Body Area Networks With Provable Security. *IEEE Systems Journal*, *11*(4), 2590-2601. doi: 10.1109/jsyst.2016.2544805
9. Poon, C., Lo, B., Yuce, M., Alomainy, A., & Hao, Y. (2015). Body Sensor Networks: In the Era of Big Data and Beyond. *IEEE Reviews In Biomedical Engineering*, *8*, 4-16. doi: 10.1109/rbme.2015.2427254
10. Usman, M., Asghar, M., Ansari, I., & Qaraqe, M. (2018). Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. *IEEE Access*, *6*, 58064-58074. doi: 10.1109/access.2018.2873825
11. Seo, S., Bang, H., & Lee, H. (2015). Coloring-based scheduling for interactive game application with wireless body area networks. *The Journal Of Supercomputing*, *72*(1), 185-195. doi: 10.1007/s11227-015-1540-7
12. Du, D., Hu, F., Wang, F., Wang, Z., Du, Y., & Wang, L. (2015). A game theoretic approach for inter-network interference mitigation in wireless body area networks. *China Communications*, *12*(9), 150-161. doi: 10.1109/cc.2015.7275253
13. Ahmed, A., Abu Bakar, K., Channa, M., Haseeb, K., & Khan, A. (2015). A trust aware routing protocol for energy constrained wireless sensor network. *Telecommunication Systems*, *61*(1), 123-140. doi: 10.1007/s11235-015-0068-8
14. Movassaghi, S., Majidi, A., Jamalipour, A., Smith, D., & Abolhasan, M. (2016). Enabling interference-aware and energy-efficient coexistence of multiple wireless body area networks with unknown dynamics. *IEEE Access*, *4*, 2935-2951. doi: 10.1109/access.2016.2577681
15. Moosavi, H., & Bui, F. (2016). Optimal Relay Selection and Power Control With Quality-of-Service Provisioning in Wireless Body Area Networks. *IEEE Transactions On Wireless Communications*, *15*(8), 5497-5510. doi: 10.1109/twc.2016.2560820
16. Tang, Q., Tummala, N., Gupta, S. K. S., & Schwiebert, L. (2005). TARA: Thermal-Aware Routing Algorithm for Implanted Sensor Networks. *Lecture Notes in Computer Science, 206–217*. doi:10.1007/11502593_17
17. Bhangwar, A. R., Kumar, P., Ahmed, A., & Channa, M. I. (2017). Trust and Thermal Aware Routing Protocol (TTRP) for Wireless Body Area Networks. *Wireless Personal Communications, 97(1), 349–364*.doi:10.1007/s11277-017-4508-5
18. Roy, M., Chowdhury, C., Kundu, A., & Aslam, N. (2017). Secure lightweight routing(SLR) strategy for wireless body area networks. *2017 IEEE International Conference On Advanced Networks And Telecommunications Systems (ANTS)*. doi: 10.1109/ants.2017.8384119
19. Sethi, D., & Bhattacharya, P. P. (2016). A Study on Energy Efficient and Reliable Data Transfer (EERDT) Protocol for WBAN. *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*.doi:10.1109/cict.2016.57
20. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network. *IEEE Sensors Journal, 15(12), 6962–6972*.doi:10.1109/jsen.2015.2468576
21. Alshamsi, A. Z., & Barka, E. S. (2017). Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks. *2017 International Conference on Informatics, Health & Technology (ICIHT)*.doi:10.1109/iciht.2017.7899139
22. Ahmed, S., Javaid, N., Yousaf, S., Ahmad, A., Sandhu, M. M., Imran, M., Alrajeh, N. (2015). Co-LAEEBA: Cooperative link aware and energy efficient protocol for wireless body area networks. *Computers in Human Behavior*, 51, 1205–1215. doi:10.1016/j.chb.2014.12.051
23. Javaid, N., Abbas, Z., Fareed, M., Khan, Z., & Alrajeh, N. (2013). M-ATTEMPT: A New Energy-Efficient Routing Protocol for Wireless Body Area Sensor Networks. *Procedia Computer Science*, *19*, 224-231. doi: 10.1016/j.procs.2013.06.033
24. Navya, V., & Deepalakshmi, P. (2017). Mobility supported threshold based stability increased throughput to sink using multihop routing protocol for link efficiency in wireless body area networks (M-TSIMPLE). *2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*.doi:10.1109/itcosp.2017.8303107
25. Liu, B., Yan, Z., & Chen, C. W. (2017). Medium Access Control for Wireless Body Area Networks with QoS Provisioning and Energy Efficient Design. *IEEE Transactions on Mobile Computing*, 16(2), 422–434. doi:10.1109/tmc.2016.2549008
26. Chen, Z., He, M., Liang, W., & Chen, K. (2015). Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network, *Journal of Sensors*, 2015, 1–10. doi:10.1155/2015/716468
27. Barakah, D. M., & Ammad-uddin, M. (2012). A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of a Virtual Doctor Server in Existing Architecture. *2012 Third International Conference on Intelligent Systems Modelling and Simulation*. doi:10.1109/isms.2012.108
28. Kim, B.-S., Kim, K., & Kim, K.-I. (2017). A Survey on Mobility Support in Wireless Body Area Networks. *Sensors, 17(4), 797*.doi:10.3390/s17040797
29. Javaid, N., Ahmad, A., Nadeem, Q., Imran, M., & Haider, N. (2015). iM-SIMPLE: iMproved stable increased-throughput multi-hop link efficient routing protocol for Wireless Body Area Networks. Computers in Human Behavior, 51, 1003–1011.doi:10.1016/j.chb.2014.10.005

AUTHORS PROFILE

Prabhjot Kaur has completed 4 Year Bachelor of Technology in Computer Science and Engineering from Punjab Technical University, Punjab in 2016. Currently, she is pursuing Masters of Engineering from Chandigarh University. Her area of interest is in energy efficient design, routing algorithms, network security, wireless sensor and body area networks. She has successfully published one review paper in IEEE International Conference on a Computing for Sustainable Global Development (INDIACOM), at Bharti Vidyapeeth in Delhi.

Dr. Sandeep Singh Kang holds a Ph. D. degree holder in Computer Science Engineering from Punjabi University Patiala. The main focus of his research is related to computer and network security. Dr. Kang is presently working in Chandigarh University as Professor in CSE department. He has made a contribution in several networking-related areas like Energy efficient design, routing algorithms, Wireless Sensor Networks, Computer, and Network Security. He is having more than 11 years of teaching and research experience. He has been attended and presented his research paper in reputed journals. He has published more than a dozen research papers in national and international journals of repute.