

Secured and Trust –Multipath Optimized Link State Routing in Wireless Body Area Network

S.Veena, D.John Aravindhar, K.B.Aruna, L.Sudha

Abstract: A Wireless Body Area Network (WBAN) are used to connect wearable computing devices and are designed to operate autonomously in a wireless environment. The research is on progress in designing a system of health observance to meet the technical demand especially in a Wireless Body Area Network. In these Body Area Networks, the parameters such as Packet Loss Rate (PLR), Delay, Quality of Service (QoS) and throughput have to be addressed in order to provide an efficient real-time data transmission. In this system, Trust Secure Energy Optimized Aggregation Protocol (TSEOAP) and a Secure Trust-Multipath Optimized Link State Routing (STMOLSR) is proposed where TSEOAP is a reactive protocol, which has higher latency since the routes are discovered when the source node initiates a request, STMOLSR is a proactive routing protocol, which has low latency based on routing operation. So, by comparing these two protocols, proactive is a better one as prevention is better than cure. A Retransmission Scheme based on Priority is designed in which the emergency packets are given a higher priority so that the performance of the system is increased. The behaviour of each node will be evaluated by using trust based reasoning which uses the OLSR protocol. For detection of malicious node, a Detection System is used to detect the intruders. Crypto Encryption is known for its tremendous speed and effective when compared to other encryption techniques. To enhance the security aspects, the encryption and decryption algorithms should be improved.

Index Terms: Body Sensor Network, Cryptography, Energy efficiency, Resource allocation, Routing protocol, Quality of Service.

I. INTRODUCTION

Body Area Network is called as Personal Area Networks initially and Wireless Body Area network was introduced in 1996 by T.G.Zimmerman. Wireless Body area Network is network of wearable devices used in a wireless environment. In WBAN, various sensors can be introduced and has led to many applications in Wireless Sensor Network. It can be deployed to measure physiological signals in a wireless biomedical sensors. This network has nodes or sensors to operate in the human body for communication and to monitor the parameters of the body. The signals from these nodes can be collected by any device, which may be a smart phone or a personal device. These devices are the sink nodes, which

transmits the data to the main unit, which takes care of health. During the implementation of Wireless Body Area Network, various problems are identified in the technology especially in security. In Wireless Body Area Network, two devices are often identified such as sensors and actuators. The sensors can be used to determine the anatomy by means of parameters, either outwardly or internally. Examples of such measurements include the heart beat, temperature or recording a chronic Electro Cardio Gram (ECG). The actuators respond with actions, which are in consistent either with the received information. In some cases, the interaction with the user can be handled by a smart phone or a personal device.

In various real time critical applications, like detection of fire in forests, monitoring the gases in coal mines, battlefield reconnaissance, a special type of wireless network such as Wireless Body Area Networks (WBANs) can be used. These networks are deployed in a wide range of areas with a large number of nodes. These sensor nodes are detected and generate a report to the end-users. In this network, infrastructure is not used for communication, the users are equipped with communicating device, which are sensor nodes. When any critical event like fire or gas leak occurs in the monitoring area, these events are detected by a sensor node which generates an alarm, which are then broadcast to the other nodes immediately. Then, these sensor nodes can send a warning to the users so that they can take a response to the event. The modern networks are generally bi-directional, thus it enables to control the activity of the sensor.

In the past few years, there is advancement in distributed computing and also in micro electro mechanical systems, and these have been applied for disaster management, military, industry health, and environment and in other domains. In Wireless Sensor Network, the nodes are characterized by limited processing, power, and memory resources. As these nodes are powered by batteries, recharging or replacing the batteries is difficult because of cost and also due to few geographic reasons.

Wireless Body Area Network consists of various types of sensors which are energy-constrained and hub, which are an energy-rich one. Thus it is called as a heterogeneous system. In these networks, a variety of physiological signals can be collected based on the Quality of Service requirements. The size of the body sensors is very small for the lightweight and non-intrusive applications. When compared with the conventional wireless sensor, the resources like storage, processing and battery energy supply of these networks is extremely constrained. The factors like fading of the channels between the sensors, the link distance of the hub and obstructions can also be taken into account. In Wireless Body Area network, the link factors will

Revised Manuscript Received on April 06, 2019.

S.Veena, Computer Science and Engineering, S.A.Engineering College, Chennai, India.

D.John Aravindhar, Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.

K.B.Aruna, Computer Science and Engineering, S.A.Engineering College, Chennai, India.

L.Sudha, Computer Science and Engineering, S.A.Engineering College, Chennai, India.

inevitably change, when there is a change in the human posture. Therefore, the link dynamism in the Body sensor networks have to dealt. Thus, when there is a change in the human posture or when there is a change in the communication environment, it is very hard to guarantee the requirements of Quality of Service. Thus in the existing system, there is no algorithm which can improve the efficiency of the Energy or the efficiency in discovering the routes.

II. RELATED WORK

Z. Liu, B. Liu, C. Chen, and C. W. Chen [1] discusses about the Resource allocation scheme which focuses on Energy efficiency and also on Quality of Service provided in a wireless environment of body area networks. The proposed method is a unified framework designed for wireless network. In this scheme, metrics of Quality of Service and the Dynamic links are considered.

S. Manfredi [2] proposed “Congestion control for differentiated healthcare service delivery in emerging heterogeneous wireless body area networks”. The proposed system is developed for the modern heterogeneous wireless network and used for healthcare traffic control. This method avoids congestion in the network and also achieves the Quality of Service by means of good responsiveness and system reliability.

Y. He, W. Zhu, and L. Guan [3] introduces a “Optimal resource allocation for pervasive health monitoring systems with body sensor networks”. The proposed method is used in health monitoring systems and uses optimization techniques for the resource allocations to obtain a sustainable and high-quality service. The authors have considered two types of resource optimization problems, formulated and solved them.

Khan, Shafiullah,[4] discusses “Secure Routing Protocol using Cross Layer Design and Energy Harvesting in Wireless Sensor Networks”. The Energy Harvesting scheme is used in routing protocols to address the energy efficiency in Wireless Sensor networks. The author have proposed to secure the attacks and prevention mechanism to avoid the attacks. To ensure the energy usage efficiently, the parameters are exchanged in the cross layer design. This paper uses Energy harvesting system is used to store and extract energy, also it can be used to take decisions for the routing issues and the node state. The simulation results specifies that the routing protocols perform better in various scenarios especially in hostile attack prone environment.

Gimer Cervera, Michel Barbeau , Joaquin Garcia-Alfaro[11] had proposed a method, which constructs the multiple disjoint points, which may lead to the increase the resilience against the failure in the network or malicious attacks. Generally, in OLSR type of networks, the link state information is generated partially and it is exclusively flooded in the network. Thus, the node can view the network topology partially. Also, flooding may also affect the propagation of the traffic information. This may lead to reduced construction of multiple disjoint paths. The proposed method in this paper computes many path between any two nodes, which are disjoint in the Mobile Adhoc network, which improves the view of the topology.

De-gan Zhang , Ting Zhang , Yue Dong had discussed a new protocol in Mobile Adhoc network, which improves the quantum genetic method. The Q-learning strategy, which updates the routing path dynamically in the network through interaction. This Q- learning strategy has been used in the quantum genetic strategy, which improves the performance in transmission.

III SYSTEM MODEL

In the Wireless Body Area Network, the classical Bluetooth and Zigbee are not suitable since it leads to various issues such a maintaining the links dynamically, to save the energy in an efficient manner and to provide a good Quality of Service. This paper had proposed a method based on IEEE 802.15.6 protocol for Wireless body Area Network. In the proposed methods, TDMA in beacon mode access mechanism with super frame boundaries are used to avoid collisions.

When the Wireless Body area network grows, the network is vulnerable to attacks, thus it needs a security method to overcome. Thus, a suitable cryptography mechanism for Wireless sensor network is an important challenge, since these networks has a limitation in energy, storage resources and computation capability. A new routing algorithms for energy efficiency has to be proposed for networks, which is a ad hoc and which uses a Trust Secure Energy Optimized Aggregation Protocol(TSEOAP). This protocol addresses important requirements of energy-efficiency, reliability, data aggregation and attacker’s detection in Wireless Body Area network. Trust Secure Energy Optimized Aggregation protocol is also a routing algorithm, which uses the energy in an efficient manner, find the routes, which reduces the total energy needed for end-to- end packet transmission and thus enhances the detection of the malicious nodes. A cryptography based security mechanism is proposed to apply Elliptic Curve Cryptography technique in WSN.

The objective of the proposed TSEOAP is to find more routes, in terms of the reliability in the communication link and to find the routes, which are energy-efficient. This method increases the lifetime of the network by finding the routes, which has the nodes of high battery and with more security.

The advantages of TSEOAP are Maximizing the lifetime of the network and achieves the security level significantly, overall energy consumption is reduced and increases network performance. Also, the Network Lifetime can be enhanced, it shows an improvement in the Packet delivery ratio and Throughput and also it reduces the overhead of the routing and the average end-to- end delay.

Secure Trust Multipath OLSR(STMOLSR)

The existing system used a link state protocol, which are then optimized to form a new protocol named as Optimized Link State Protocol. This protocol is used to find the best routes and make it available immediately or as and when needed, so it is called as proactive routing protocol. But, the changes in the topology, which are made available to all the host in the network leads to the flooding in the network. This can be overcome by using the multipoint relays. This Multipoint relays reduces the same broadcast messages

to be sent to few regions in the network, thus reducing the flooding of broadcast messages.

The Optimized Link State Protocol has two types of special messages such as “Hello” and “Topology Control”. The message “Hello” are used to find the status of the link and the also the neighbours of the host. The “Topology Control” message are used for broadcasting the packet of information about the neighbours, by the process of advertising. The Optimized link state protocol has a proactive characteristic, since it sends all the routing information to the host, which participates in the network. But, the major drawback of this protocol, it requires each host to send the information about the updated topology through out the network, which may lead to increase in usage of bandwidth. But, then the Multipoint relay reduces the flooding, which restricts the broadcast messages to be forwarded.

The Advantages of STOLSR are Trusted nodes and perfect Intrusion Detection System’s (IDS), Reduces the IDSs’ active time as much as possible without compromising on its effectiveness, Maximizing the lifetime of the network and achieved security level significantly and Overall energy consumption is reduced and increases network performance.

Difference Between TSEOAP and OLSR protocol

i. PACKET TRANSMISSION

TSEOAP: The packet transmission will takes place one after other.

OLSR: Parallel transmission takes place which reduces the time and maximizing the network lifetime.

ii. CONGESTION

TSEOAP: Whenever congestion occurs the transmission of packets are stopping.

OLSR: Controlled the congestions by using congestion control techniques. If the congestion occurs the packet wont stop packet forwarding.

iii. ROUTING

TSEOAP: It will determine the route only when there is a data to send.

OLSR: Route is already known when the packet needs to be forwarded.

iv. LATENCY

TSEOAP: Higher latency since the routes are discovered when the source nodes initiates a request.

OLSR: Low latency due to maintenance of routes.

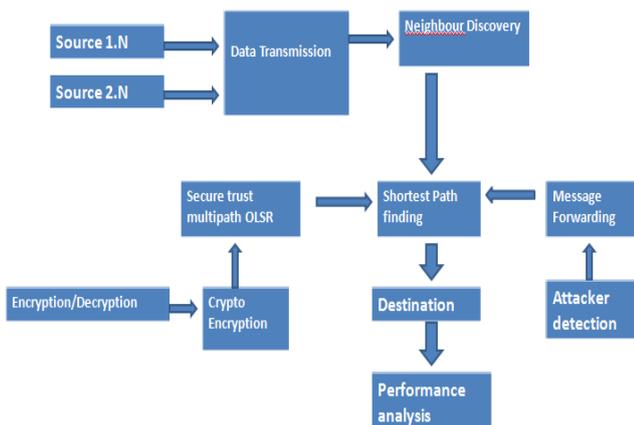


Figure 1 Architecture of Secure Trust Multipath OLSR (STMOLSR)

IV Trust Secure Energy Optimized Aggregation Protocol(Tseoap) And A Secure Trust-Multipath Optimized Link State Routing (StmolSr) System

A. Trust Secure Energy Optimized Aggregation Protocol(TSEOAP)

Trust Secure Energy Optimized Aggregation Protocol addresses important requirements of Wireless Body Area Networks such as Energy-efficiency, reliability, data aggregation and attacker’s detection. Trust Secure Energy Optimized Aggregation Protocol is a routing algorithm, which is an energy efficient one, to find the routes required for end to end packet traversal, by reducing the total energy and also enhances the detection of malicious nodes. A cryptography based security mechanism is proposed to apply Elliptic Curve Cryptography technique in Wireless Sensor Network. The proposed system provides an excellent security mechanism by improving encryption and decryption aspects of the algorithm.

The objectives of the proposed TSEOAP is to find more routes, in terms of the reliability in the communication link and to find the routes, which are energy-efficient. This method increases the lifetime of the network by finding the routes, which has the nodes of high battery and with more security.

Trust Computation

There is a need to estimate the risk factor on the task or also called as a computed trust value in a network so that a decision has to be taken based on the trust value. This is accomplished by defining a trust value or Threshold value to each task. For each task, the threshold value may vary, which depends on the security. Finally, the trust value computed in a system is compared with the threshold value, to identify whether the trustee node satisfies the requirement of the trust or not.

Trust computation based attacker detection

T_{ij}^d -Trust value
i and j nodes

Formula :

$$T_{ij}^d = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}$$

α - positive value
 β - negative value

B. Secure Trust-Multipath Optimized Link State Routing (STMOLSR)

Optimized Link State Protocol

The existing system used a link state protocol, which are then optimized to form a new protocol named as Optimized Link State Protocol. This protocol is used to find the best routes and make it available immediately or as and when needed, so it is called as proactive routing protocol.



But, the changes in the topology, which are made available to all the host in the network leads to the flooding in the network. This can be overcome by using the multipoint relays. This Multipoint relays reduces the same broadcast messages to be sent to few regions in the network, thus reducing the flooding of broadcast messages.

The Optimized Link State Protocol has two types of special messages such as "Hello" and "Topology Control". The message "Hello" are used to find the status of the link and the also the neighbours of the host. The "Topology Control" message are used for broadcasting the packet of information about the neighbours, by the process of advertising. The Optimized link state protocol has a proactive characteristic, since it sends all the routing information to the host, which participates in the network. But, the major drawback of this protocol, it requires each host to send the information about the updated topology through out the network, which may lead to increase in usage of bandwidth. But, then the Multipoint relay reduces the flooding, which restricts the broadcast messages to be forwarded.

Attack Prevention Model

In this model, both public key and private key are generated. The sender uses receiver's public key to encrypt the message and the receiver uses its private key to decrypt. The user generates a random number 'r' in the range of 't'.

The user computes the public key by using the random number and the point on the curve as follows,

$$1) U = r * P$$

'r' is the random number selected within the range of (1 to t-1). 'P' is the called as a point on the curve.

'U' is the public key and 'r' is the private key.

ENCRYPTION

Let the sending message be represented by 's' and the user represents this message on the curve.

Consider 's' has the point 'S' on the curve 'E'. 'k' is selected random within a range of (1 - (t-1)).

Two cipher texts will be generated let it be T1 and T2.

$$2) T1 = k * P$$

$$3) T2 = S + k * U$$

C1 and C2 will be sent.

DECRYPTION

The user have to get back the message 's' that was send to destination,

$$S = C2 - r * C1$$

S is the original message sent by the user.

C. QoS CONSTRAINTS

This section discusses about three metrics for Quality of Service such as Packet Delivery Ratio, Average End-end Delay and Throughput ratio. These metrics plays a major role in the design of the resource allocation scheme, thus these metrics are also called as Quality of Service constraints.

i. Packet Delivery Ratio:

Packet Delivery Ratio is the ratio of the packed delivered successfully to the packets generated at the source.

In the ISM band, the Differential Phase Shift Keying (DPSK) modulation and Broadcasting channel coding scheme are adopted in Wireless Body Area Network, as per the recommendation of IEEE 802.15.6 standard.

The bit error may occur during the process of transmission, thus the Rate of Packets Lost can be computed as

$$RLP(\gamma) = 1 - (1 - P_{b, B(\gamma)})^L$$

where γ is the bit Signal to Noise Ratio. L is the length of a packet in bits.

The two criteria for an efficient routing protocol are the Packet Delivery Ratio must be high and the packet loss rate must be less. But in real time communications, the routing protocol which has high Packet Delivery Ratio may not be better than the one with lower Packet Delivery Ratio, since the packets which are arrived late may be useless even though these packets are delivered successfully to the destination.

ii. Average End-to-End Delay:

Average End-to-end delay is calculated as the delay during the successful transmission of the packets from the source to the destination.

The traffic is sensitive to delay in real time. The delay includes various delays such as queuing in the interface queue, latency in route discovery, delay in the retransmission, propagation delay and delay in transfer time. The end to end delay plays a major role in Quality of service aware routing protocols. The proposed system reduces the delay drastically due to the maintenance of routes in each host.

iii. Throughput Ratio:

The throughput ratio improves the network performance of the network.

V RESULTS AND DISCUSSIONS

A. Experimental Results

TSEOAP and TMOLSR

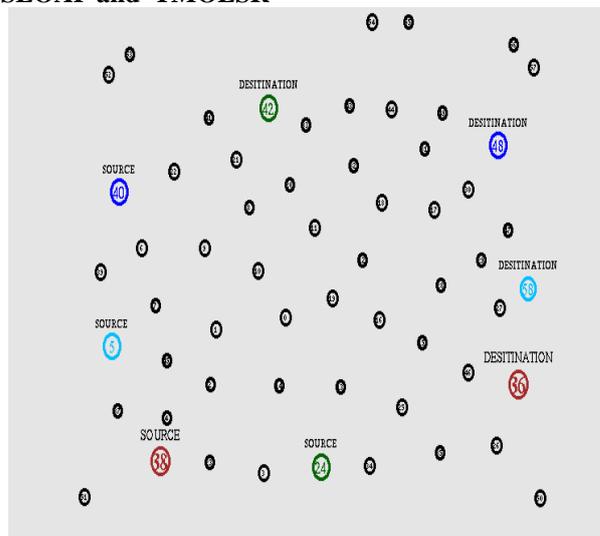


Figure 2 Packet transmission



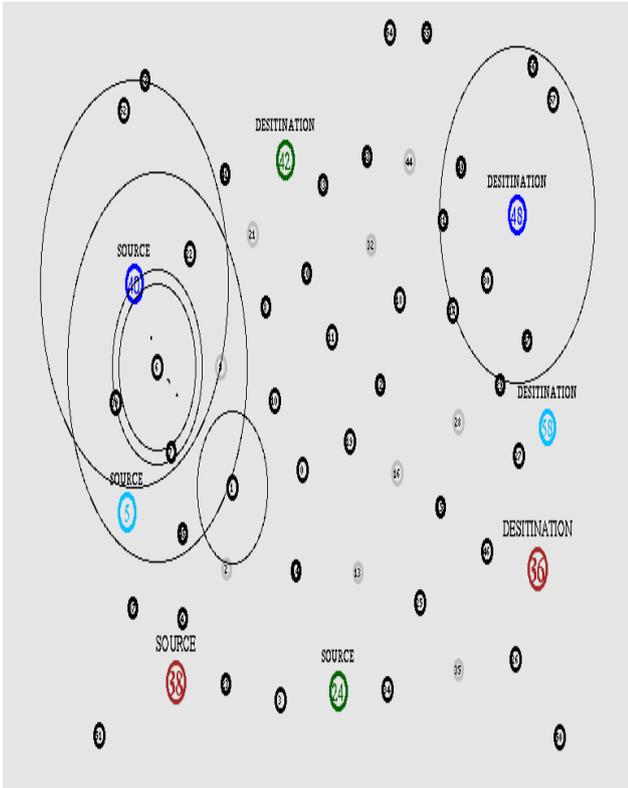


Figure 3 Finding the Shortest path and the packet transmission

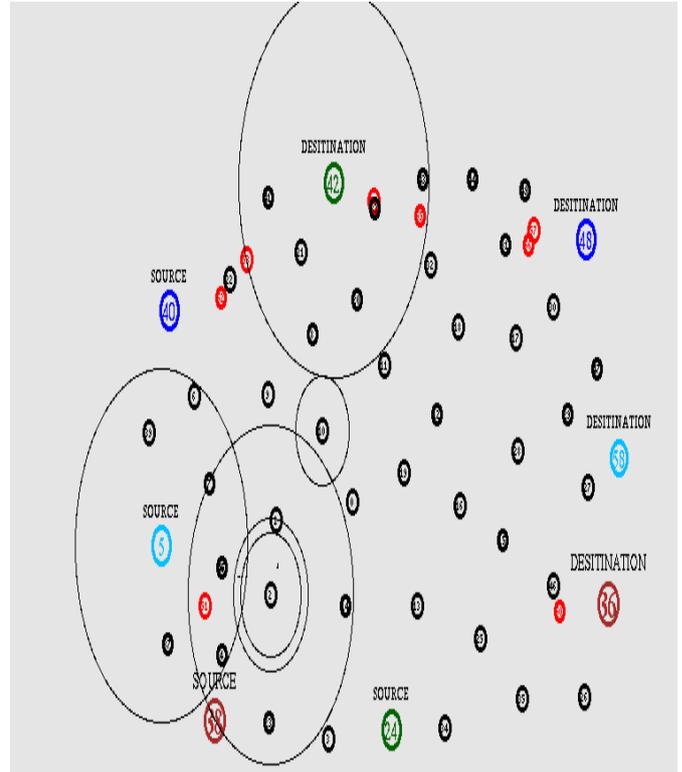


Figure 5 Detection of Attackers, which are indicated in red color

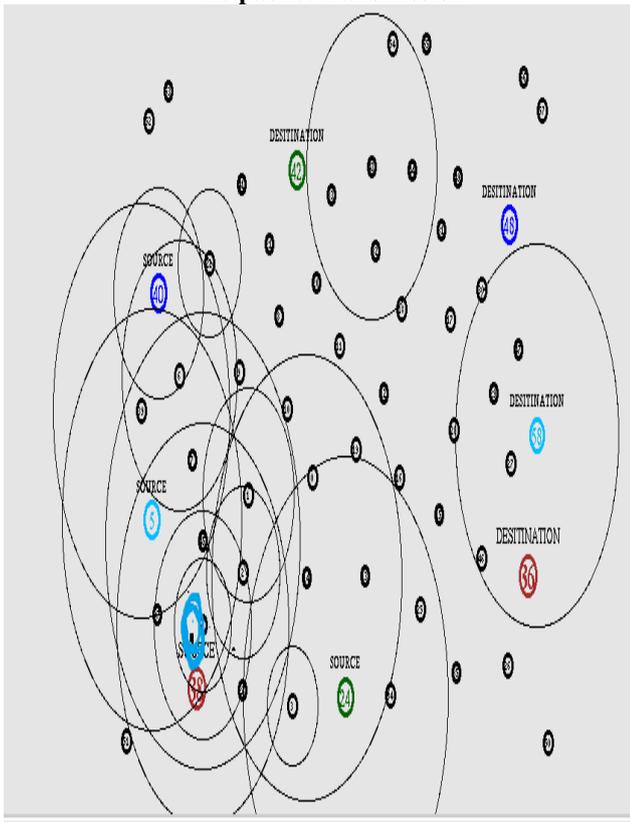


Figure 4 Dropping of packet due to congestion

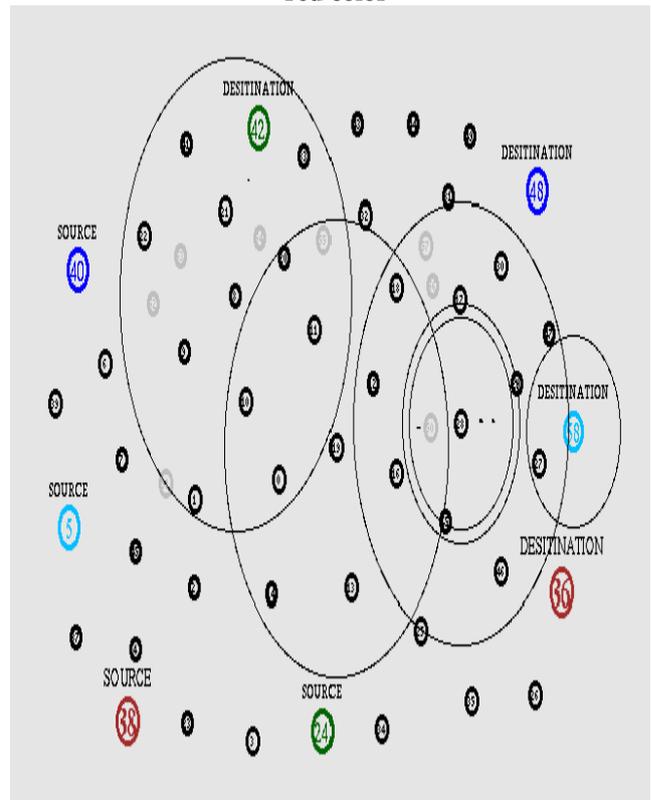


Figure 6 Attacker Prevention Model makes the attacker nodes to get disappeared

TSOLSR



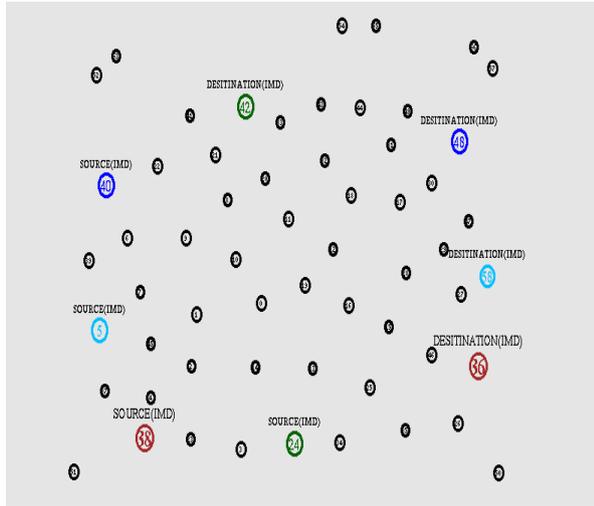


Figure 7 Packet Transmission from source to destination

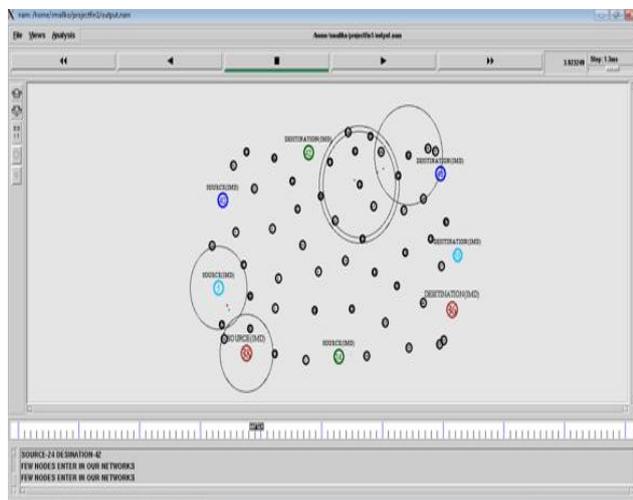


Figure 8 Parallel Packet transmission without waiting for the previous one to finish its delivery

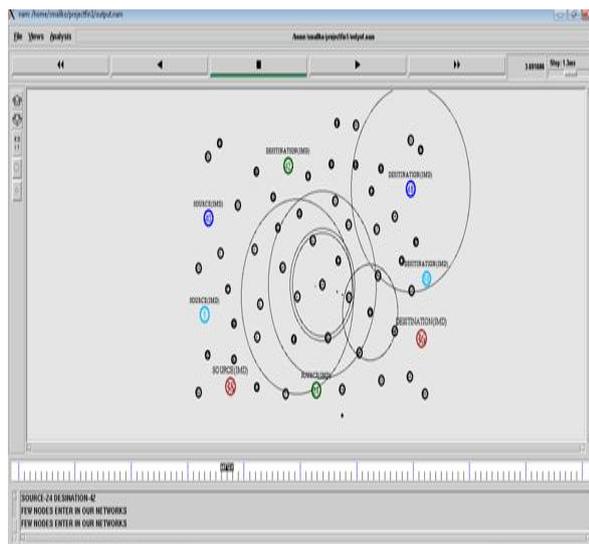


Figure 9 Continuous packet transmission even after the occurrence of congestion



Figure 10 Intrusion Detection System detects the attackers

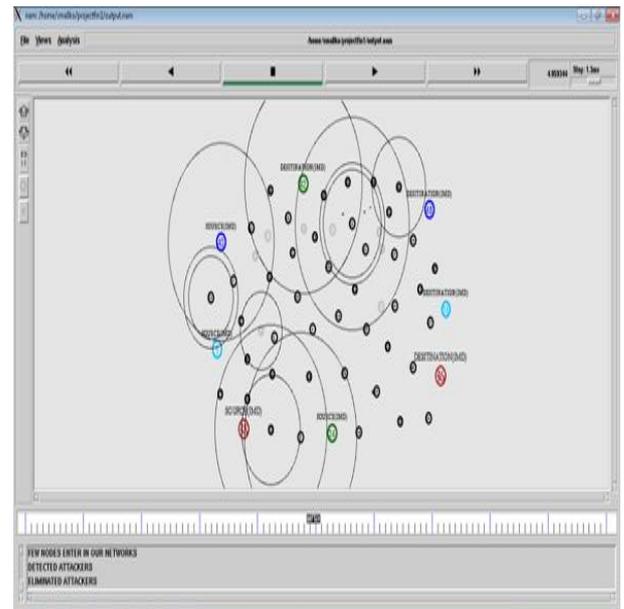


Figure 11 Attacker Prevention Model eliminates the attacker

B. DISCUSSIONS

The performance of the proposed system is valuated based on the routing and data transmission. NS2 was used to execute over a simulation area 1000 meters x 1000 meters level gap in service.

TABLE 1: PERFORMANCE VALUES

PARAMETERS	VALUES
MAC type	802.11
Routing protocol	Energy Efficient QOS
Nodes	41
Mobility Model	Stable
Mobility Speed	5,10,15,20,25 ms
Pause time	5ms
Propagation Model	TwoRayGround
Traffic Type	CBR
Traffic sources	5,10,15,20,25
Area	1000*1000

TSEOAP Performance Metrics:

The performance of the proposed system is evaluated based on the following metrics.

Throughput Ratio:

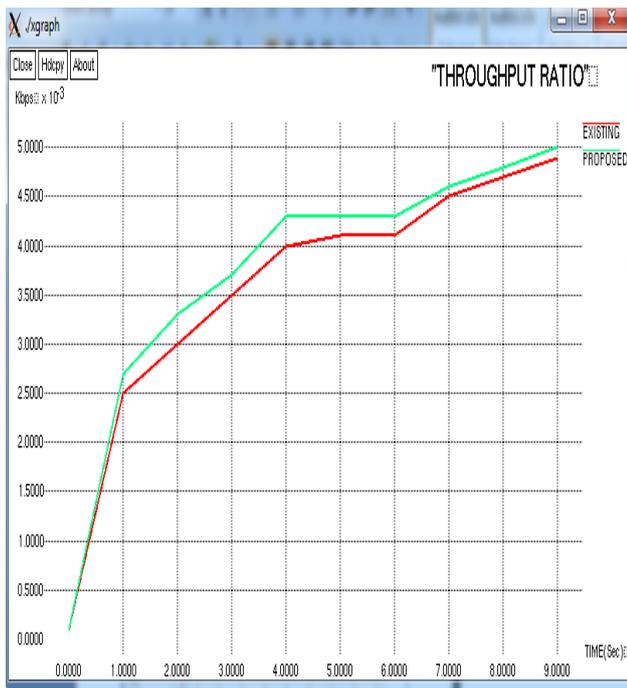


Figure 12 Throughput ratio

Packet Delivery Ratio:

Packet Delivery Ratio is the ratio of the packets delivered successfully to the packets generated at the source. In the ISM band, the Differential Phase Shift Keying (DPSK) modulation and Broadcasting channel coding scheme are adopted in Wireless Body Area Network, as per the recommendation of IEEE 802.15.6 standard.

The two criteria for an efficient routing protocol are the Packet Delivery Ratio must be high and the packet loss rate must be less. But in real time communications, the routing protocol which has high Packet Delivery Ratio may not be better than the one with lower Packet Delivery Ratio, since the packets which are arrived late may be useless even though these packets are delivered successfully to the destination.

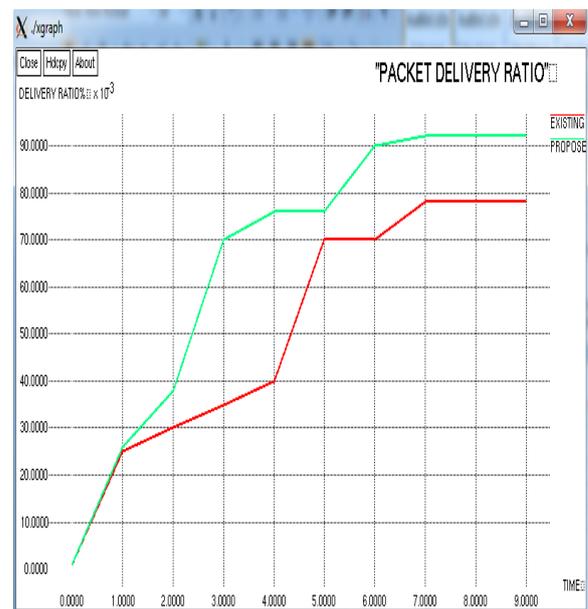


Figure 13 Packet Delivery Ratio

Average End-to-End Delay:

Average End-to-end delay is calculated as the delay during the successful transmission of the packets from the source to the destination.

The traffic is sensitive to delay in real time. The delay includes various delays such as queuing in the interface queue, latency in route discovery, delay in the retransmission, propagation delay and delay in transfer time. The end to end delay plays a major role in Quality of service aware routing protocols. The proposed system reduce the delay drastically due to the maintenance of routes in each host.

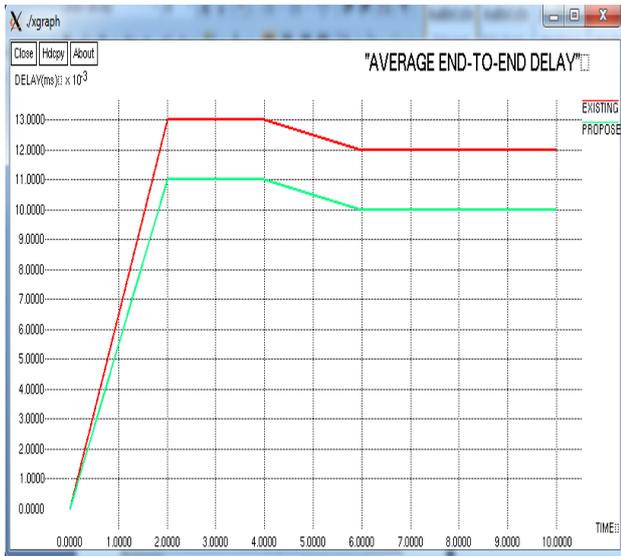


Figure 14 Delay

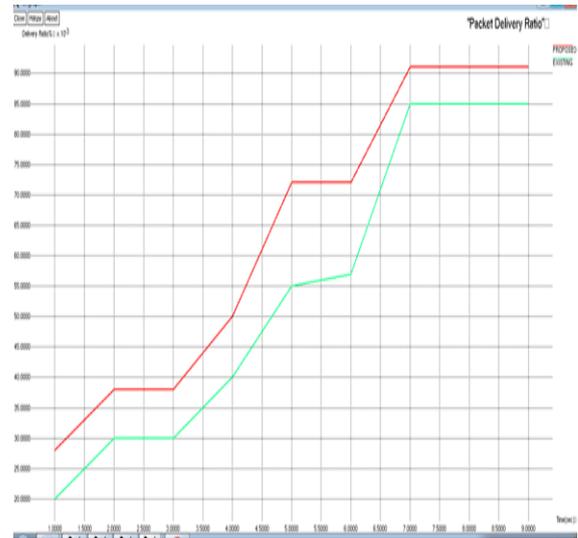


Figure 16 Packet Delivery Ratio

Energy Consumption:

Energy consumption rate for sensors in a wireless sensor network varies greatly based on the protocols the sensors use for communications



Figure 15 Energy consumption

Average End-to-End Delay:

Average End-to-end delay is calculated as the delay during the successful transmission of the packets from the source to the destination. The end-to-end delay include the various delays such as delays due to buffering in the route discovery process, delay in the interface queue, retransmission delays at the MAC, delays in propagation and time to transfer. This delay is the time duration for a packet to travel from the application layer of the source node to the destination node. This delay is one of the major metric to be considered for performance evaluation in QoS aware routing protocols. The average end-to-end delay is the average value of the end to end delay calculated for all the successfully transmitted packets. The delay is reduced drastically due to the maintenance of routes in OLSR.

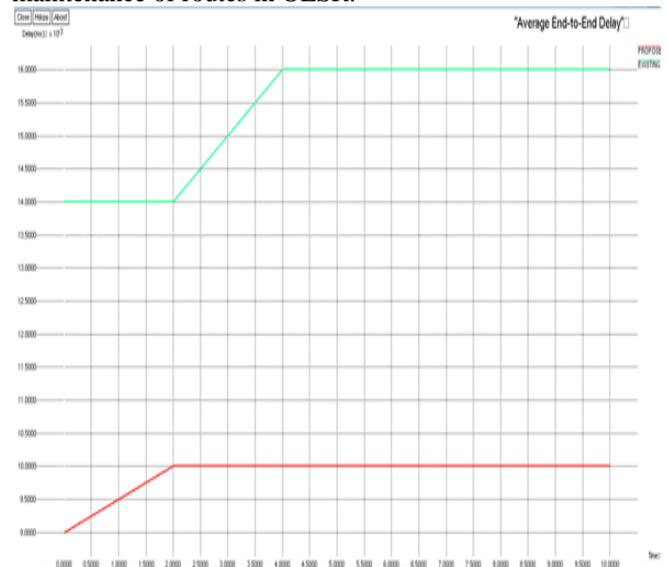


Figure 17 Delay

OLSR Performance Metrics

Packet Delivery Ratio:

Packet Delivery Ratio is the ratio of the packed delivered successfully to the packets generated at the source. The packet loss rate is low if the Packet Delivery Ratio is high, which in turn leads to the more efficient routing protocol. But in real time communications, the routing protocol which has high Packet Delivery Ratio may not be better than the one with lower Packet Delivery Ratio, since the packets which are arrived late may be useless even though these packets are delivered successfully to the destination. Also, the traffic in Real time systems is sensitive to the delay.

EXISTING SYSTEM : TSEOAP (green)

PROPOSED SYSTEM: OLSR (red)

Throughput Ratio:



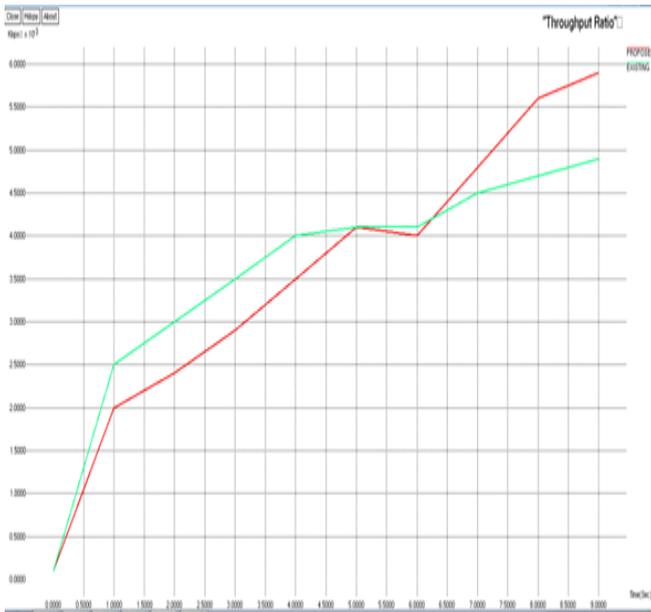


Figure 18 Throughput Ratio

VI CONCLUSION AND FUTURE ENHANCEMENT

To have a better transmission process with low latency, OLSR performs better than the TSEOAP. As it is a proactive protocol the route is already known when the packet needs to be forwarded so there will be little delay. The main advantage of the proposed system are the life time of the network is maximized and has achieved better security level. For the detection of malicious nodes Intrusion Detection System (IDS) is used whose active time is reduced as much as possible without compromising on its effectiveness. The performance is very high due to its frequent route updates. The main drawback in TSEOAP is, it did not concentrate on insider attacks. So it was concluded that by using proactive protocol there will be no insider attackers in the network.

In the proposed system STOLSR, there is a need to transmit the updated topology throughout the network periodically by each host. Thus, in future enhancement, the proposed system can be extended on updation of information periodically by the host.

REFERENCES

- Z. Liu, B. Liu, C. Chen, and C. W. Chen, "Energy-efficient resource allocation with QoS support in wireless body area networks," in 2015 IEEE Global Communications Conference (GLOBECOM), IEEE, pp. 1–6, 2015.
- S. Manfredi, "Congestion control for differentiated healthcare service delivery in emerging heterogeneous wireless body area networks," *Wireless Communications, IEEE*, vol. 21, no. 2, pp. 81–90, 2014.
- Y. He, W. Zhu, and L. Guan, "Optimal resource allocation for pervasive health monitoring systems with body sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 11, pp. 1558–1575, 2011.
- Khan Shafiullah, Nour Mast, Jonathan Kok-Keong, Ayesha Salahuddin, "Passive security threats and consequences in IEEE 802.11 wireless mesh networks." Volume 2; No. 3. January 2008.
- S.Veena, K.Ramyadevi, K.Elavarasi and P.Janshi, "A survey on detection of attacks and prevention model in wireless sensor network", *Journal of Advanced Research in Dynamical and Control systems*, Vol 10, 03- Special Issue, 2018.
- G. V. Crosby, C. A. Chin, T. Ghosh, and R. Murimi, "Wireless body area networks in mhealth," in *Mobile Health*. Springer, pp. 873–915, 2015.
- S.Veena, P.Janshi, D.John Aravindhar, "A Trust with an energy optimized model in WSN", *Taga Journal of Graphic Technology*, Vol 14, 2018.

- C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, pp. 1–15, 2016.
- B. Liu, Z. Yan, and C. W. Chen, "Medium access control for wireless body area networks with QoS provisioning and energy efficient design," *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1–1, 2016.
- G. Fortino, R. Giannantonio, R. Gravina, P. Kuryloski, and R. Jafari, "Enabling effective programming and flexible management of efficient body sensor network applications," *IEEE Transactions on Human-Machine Systems*, vol. 43, no. 1, pp. 115–133, 2013.
- R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: technologies and design challenges," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1635–1657, 2014.
- H. Moosavi and F. Bui, "Optimal relay selection and power control with quality-of-service provisioning in wireless body area networks," *IEEE Transactions on Wireless Communications*, vol. PP, no. 99, pp. 1–1, 2016.
- Ali Moussaoui a,n, Fouzi Semchedine b, Abdallah Boukerrama "A link state QoS routing protocol based on link stability for Mobile Adhoc Networks" *A. Moussaoui et al. / Journal of Network and Computer Applications* 39(2014)117–125.
- De-gan Zhang a,b,c, Ting Zhang a,b, Yue Dong a,b,* Xiao-huan Liu a,b, Yu-ya Cui a,b, De-xin Zhao a,b, "Novel optimized link state routing protocol based on quantum genetic strategy for mobile learning" *Journal of Network and Computer Applications* 122 (2018) 37–49.

AUTHORS PROFILE



S.Veena, is working in S.A.Engineering College and has a total teaching experience of 18 years. She is a Life member of ISTE. She has published and presented a total of 40 papers in Conferences and Journals and she has also published 1 Book. Her areas of interest are Data Science, Artificial Intelligence, Data Mining, Bioinformatics, Network Security and Cloud Computing. She has acted as one of the Coordinator for organizing a National Workshop on Quantum Computation and Cryptography sponsored by DST-SERB and FDP on Adhoc and Sensor Network approved by Anna University.



D. John Aravindhar is working in Hindustan Institute of Technology and Science. He has a total teaching experience of 18.6 years. He is a member of ACM Professional Society. He has published and presented a total of 35 papers in Conferences and Journals and he has also published 1 Book. His areas of interest are Cloud Computing, Data Mining and Data Analytics. He and his Colleague have received a grant from TNSCST for organizing International Conference in the year 2018.



K.B. Aruna, is working in S.A.Engineering College and has a total teaching experience of 6.6 years. She is a Life member of ISTE. She has published and presented a total of 10 papers in Conferences and Journals and she has also published 1 Book. Her areas of interest are Data Structures, Network Security and Cloud Computing.



L. Sudha, is working in S.A.Engineering College and has a total teaching experience of 7.8 years. She is a Life member of ISTE. She has published and presented a total of 10 papers in Conferences and Journals and she has also published 1 Book. Her areas of interest are Data Structures, Network Security and Cloud Computing.