Trust Aware Light Weight Secure Routing Protocol for Wireless Body Sensor Network using RCP Measures

Sangeethapriya Nachimuthu, Bharathi Lakshmanan, Dola Sanjay

Abstract: ***The growth of information technology and networking solutions encouraged the deployment of WBSN. It supports the monitoring and control of human conditions towards various issues. However, the security of data transmission and routing plays vital role and to achieve this, different algorithms has been identified. But, the earlier methods are does not produce expected QoS (Quality of Service) parameters. To improve the performance of routing, a novel trust aware light weight routing algorithm (RCP-TLSR (Reputation Completion Privacy Preservation-TLSR) has been proposed. The sensors of wireless body network discover the available routes between the source and destination. The selection of route and the sensor node has been identified according to the RCP measure which has been computed according to the reputation, completion and privacy preservation values. By choosing the routes according to the values of RCP, the method achieves higher performance in routing. On the other side, the data security has been enforced by block level encryption technique which is understandable for the concern sensor nodes. The method improves the performance in security and routing highly.***

Index Terms: WBSN, Secure Routing, Privacy Preservation, Data Security, TALWSR, RCP, QoS.

I. INTRODUCTION

The modern information technology and networking technology has introduced various solutions to support different domains. The sensor networks has
been used in different domains like data collection in war field networks, medical solutions, human monitoring and remote device controls and so on. The wireless body sensor networks are the collection sensor nodes which are attached to the human body in form of any device. In modern world, there is a huge requirement to track the location and conditions of human to achieve different aspects. For example, when a patient has been added to the monitoring and controlling system, it is required to monitor the blood pressure, temperature and more. In order to achieve this, the device attached to the human body comes with the sensor node which supports the transmission and reception of data packets through the network it located. Such combined sensor nodes forms the wireless body sensor networks.

Like any other network, the wireless body sensor network (WBSN) has been identified as dynamic network due to the mobility of human being.

Revised Manuscript Received on November 06, 2019.

SangeethaPriya Nachimuthu, Associate Professor Department of Electronics and Communication Engineering, Ramachandra College of Engineering, Eluru-534007, Andhra Pradesh, India.

Bharathi Lakshmanan, Professor Ramachandra College of Engineering, Eluru-534007, Andhra Pradesh, India.

Dola Sanjay S, Professor Department of Electronics and Communication Engineering,

Ramachandra College of Engineering, Eluru-534007, Andhra Pradesh, India. angeethariyaSP2005@gmail.com

The device attached to the human body gets moving all the time and in order to perform data transmission, they involve in cooperative transmission. Any sensor node cannot transmit directly to the destination which is restricted by the transmission range. The source node identifies the neighbor nodes and routes to reach the destination. From the routes identified, the method selects a single route to reach the destination. In terms of achieving higher QoS values, the routing plays vital role. The routing in WBSN has been performed in several ways, but the shortest path routing is always ultimate because it reduces the cost, energy, latency and so on. As the nodes of WSBN has limited power and have dynamic mobility conditions, it is necessary to consider the power conditions to improve the lifetime of the network. By considering different parameters of routing, an efficient routing algorithm can be adapted to meet higher QoS values.

On the other side, the security has higher importance in routing the packets towards various devices and humans. The data packets are travel through number of networks and it is not necessary that the continuity and the route should be available in all the locations and geographic areas. In most times, the packets should be travel through number of intermediate networks and number of IoT devices. The Internet of Things (IoT) devices are recently launched in different locations of any geographic area which supports the transmission and reception of data and to control various devices. The presence of IoT devices around the sensor nodes of WSBN can be used for successful routing of data packets. Also, the stable IoT devices support the higher performance in routing and reduce the frequency of retransmission.

The data security can be enforced in several ways, but the ultimate is data encryption. The data packets with more sensitive and medical information would travel through number of networks and different devices. So it is necessary to hide the sensitive information to meet the QoS requirements. Different encryption standards available towards data security and this paper present a block level data encryption algorithm to improve the data security. By performing block level encryption, the privacy preservation can be performed. The protocol enforced should be simpler and efficient. To achieve this, this paper presents the light weight scheme with RCP. The next section describe the working methodology in detail.

II. RELATED WORKS

There are number of methods available for the problem of secure routing in Wireless Body Sensor Networks. This section discusses different methods of routing in WSBN in detail.

In [1], Energy optimized Secure Routing (EOSR) algorithm is presented which works based on the trust measures. The trust measure is estimated in a distributed way. The method uses different factors in estimating the trust value for the nodes. According to the residual energy and route length in measuring the trust value.

In [2], to improve the security performance and coordination between nodes, an efficient trust based routing algorithm is presented. The method selects set of nodes to involve in data transmission based on the trust measure. The trust value is measured based on the energy available and resilience to attack.

In [3], a combined approach is presented to maximize the lifetime of the network. The clustering is performed using LEACH algorithm where the chain algorithm is used for route selection.

In [4], a privacy preservation technique is presented to support health care applications. The method uses multipath routing and hashing scheme has been used to enforce data security. The method generates hash value for each component and the same value has been used to detect the modifications.

In [5], reliability based routing protocol is presented for WSN. The method selects neighbors of source and destination according to their reliability. The markov chain model has been used to measure the reliability of nodes and improves the performance.

In [6], a Monarchy Butterfly Optimization based routing protocol is presented to support WBAN. The method is designed to support healthcare solutions and routing is performed according to the optimization of multiple factors.

In [7], a cluster-based routing algorithm is presented which uses Q-Learning technique. The QL-CLUSTER identifies the best fit route to reach the remote side health care station.

In [8], an Energy-Balanced Routing Protocol is presented which group the entire network region in to number of clusters. The clustering is performed using Kmeans and the cluster head is selected using fuzzy logic. The genetic algorithm has been used to select the fuzzy rule towards cluster head selection.

In [9], the author surveys various routing protocols to preserve energy of nodes. The method considers changing topology, power and computation power.

In [10], the author presents a thermal-aware, energy-efficient, and reliable routing protocol. The method consider the link quality and energy consumption in route selection.

In [11], a reliable energy efficient routing algorithm is presented. The method uses only limited nodes to become part of hopping and the rest to become forwarding. The method consider only the distance and energy of nodes in route selection.

In [12], a zone based routing protocol is presented to optimize the energy at higher traffic conditions. The method handles the redundant packets and reduces the retransmission and duplicate packets. The EEHRT technique works good on WSN.

In [13], the author present a fuzzy c means based Adaptive TDMA Scheduling (ECATS) algorithm. The method performs cluster head selection according to energy and scheduling is performed by time division multiple access.

In [14], an efficient adaptive routing algorithm is described to maximize the network lifetime. The method monitors the changes happening in the network and considers the user preferences. The routing is performed with tree based algorithm and consider the energy of nodes in identifying the routes.

In [15], an energy aware routing algorithm is presented on the basis of various techniques described earlier. The method extends the work of previous methods to optimize the energy of nodes in WSN.

In [16], the author proposed trust based cluster routing algorithm to improve security in WBSN. The method has each human body adapted with sensors which can transmit signals towards the healthcare systems. The cluster head selection is performed using PSO. The data transmission is performed using Self-Adaptive Greedy buffer allocation and scheduling algorithm (SGBAS).

All the methods discussed above suffer to achieve higher performance in security and introduces higher false ratio.

III. TRUST BASED LIGHT WEIGHT SECURE ROUTING WITH RCP:

The proposed trust based secure routing algorithm discovers the routes to reach sink. For each route identified, the reputation measure and privacy preservation support measures are estimated. Based on the values of all these measures, the method estimates the secure routing support (SRS) measure. According to the value of SRS, a single route has been selected. The working principle of the proposed algorithm is briefed clearly in this part.

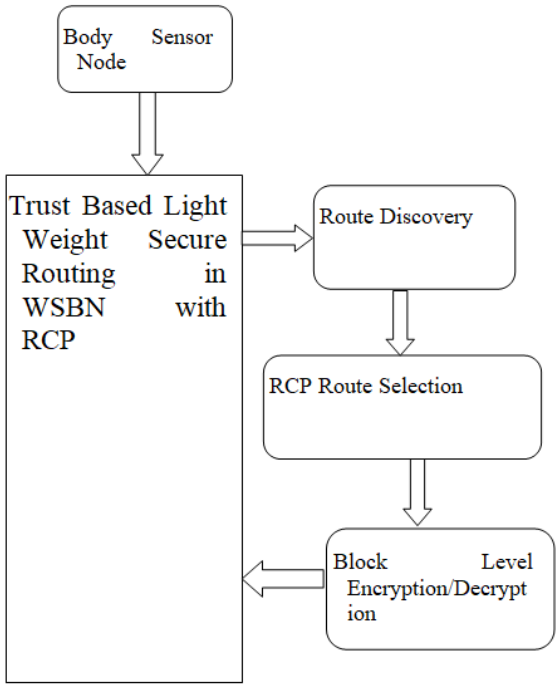

Figure 1: Architecture of proposed

a. TLSR-RCP System

The general architecture of proposed trust based light weight secure routing algorithm is presented in Figure 1. Each functional stage has been explained here.

b. Route Discovery:

The body sensor node generates a route request (WSBN-RREQ) and broadcast the packet in the network. The neighbor nodes present around the transmission range receives the packet and verifies the presence of route to reach the sink node. If there is a route then it generates the reply to the source. Otherwise, the request has been transmitted to the neighbors. This will be iterated till a route to be identified and generates the route reply. The source node receives the route reply and extracts the list of routes available. Identified routes are updated to the route table. Discovered routes are used to perform data transmission in the network. Each node generates the route reply by tagging the energy conditions and other information with the route reply.

Algorithm:

Input: packet p, Neighbor Table NT, Route Table RT

Output: Null

Start

Read packet p, NT, RT

Generate route request WSBN-RREQ = {SourceID,SinkID}

Broadcast WSBN-RREQ.

Neighbor receives route request packet WSBN-RREQ.

If $\int_{i=1}^{\text{size (RT (Neighbor))}} \text{RT(i)} \in \text{Route} \rightarrow \text{Sink}$ then

Generate route reply WSBN-RREP = {NodeID,Route,Source}

Send to source node.

Else

Add node id to request and forward to neighbors.

End

While true

Receive route reply WSBN-RREP.

Extract route R = $\int$ Route $\in$ WSBNRREP

Add route to Route Table RT= $\sum$(Routes $\in$ RT) $\cup$ R

End

Stop

The working principle of route discovery algorithm is presented above. The routes towards the sink and source have been identified. Identified routes have been added to the route table to support data transmission.

c. RCP Route Selection:

The routes selection is the process of choosing an optimal route from a set of routes available. Each route would have number of sensor nodes of WSBN and IoT devices and other static sensor nodes. By considering all these values, the method estimates reputation support measure (RSM), Completion Support Measure (CSM) and Privacy Preservation Support (PPS) measures. The reputation support is estimated according to the number of times the sensor node has been selected to participate in transmission, completion support is estimated according to the number of successful transmission among total number of transmission involved and the privacy preservation support is measured according to the number of tampered data received and number of un tampered packet received through the route. Using all these information and values, the method estimates the secure routing support (SRS) measure. Based on the value of SRS, a single route has been selected for data transmission.

Algorithm:

Input: Route Set Rs,Trace T

Output: Route R

Start

Read route set Rs and Trace T.

For each route r

Identify the traces Rt = $\int_{i=1}^{\text{size (T)}} \sum \text{T(i).Route} == \text{r}$

Compute number of times the route selected Nts = size(RT)

Compute reputation support measure RSM= $\frac{Nts}{\int_{i=1}^{size\ (T)} \sum T(i).sink == s \ \&\& \ T(i).Route\ != r}$

Compute completion support measure CSM. CSM = $\frac{\int_{i=1}^{size\ (T)} \sum T(i).route == r \ \&\& \ T(i).status == complete}{Nts}$

Compute privacy preservation support PPS. PPS = $\frac{\int_{i=1}^{size\ (T)} \sum T(i), route == r \ \&\& \ T(i).Tamper == false}{Nts}$

Compute SRS = $\frac{CSM}{RSM} \times \frac{PPS}{RSM}$

End

Choose route R with maximum SRS.

Stop

The working principle of route selection algorithm is presented which shows the procedure route selection. For each route, the algorithm estimates the reputation support, completion support and privacy support measures to compute the secure routing support measure. The route with maximum secure routing support measure has been selected for secure transmission.

d. Block Level Encryption/Decryption:

The data encryption is performed at each block and by splitting the data into number of blocks, the encryption is performed. The method split the data into number of blocks. For each block, the method encrypts the data with different keys which are provided initially to the body sensor node. Each block has been encrypted with concern key and the same has been used to decrypt the block to obtain the original information. This improves the security performance of the algorithm.

Algorithm:

Input: Data D, Key set Ks

Output: Encrypted / Decrypted data

Start

Read D,Ks.

Block set Bs = $\int$ Split(D, N)

N- denotes the block size.

For each block b

Encrypted data Ed = $\int_{i=1}^{\text{size (Bs)}} \text{Encrypt(Bs(i), Ks(i))}$

End

For each block b

Decrypted data Dd $= \int_{i=1}^{size\ (Bs)} Decrypt(Bs(i), Ks(i))$

End

Stop

The working principle of block level encryption and decryption is presented. It presents how the data has been encrypted or decrypted at block level. For each block, different key has been used for encryption and decryption.

e. Data Forwarding:

The method performs data forwarding according to the functions of route discovery, RCP route selection and data encryption/decryption algorithms. First the method performs route discovery and performs route selection using RCP route selection algorithm. With the selected route, the method performs encryption using block level encryption algorithm. Encrypted data has been sent through the selected route.

IV. RESULTS AND DISCUSSION:

The trust base light weight secure routing algorithm is hard coded and simulated under various circumstances. The NS2 (Network Simulator) is used for simulation. The performance is measured for many parameters at varying conditions.

Table 1: Simulation Details

Parameter name	Value
Total Nodes	200
Protocol Used	802.11
Simulated Area	1000×1000
Total Time	50secs

The Table 1, shows the parameters considered for the simulation of proposed trust based light weight secure routing algorithm.

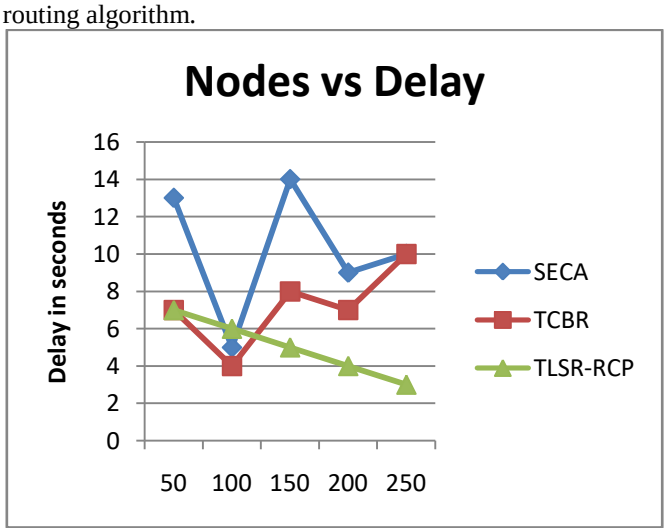

Figure 2: Performance on Delay

The delay introduced by the methods in data transmission according to number of nodes is counted and compared in Figure 2. The TLSR-RCP algorithm introduces only negligible delay at each condition which is less than previous TCBR and SECA algorithms.

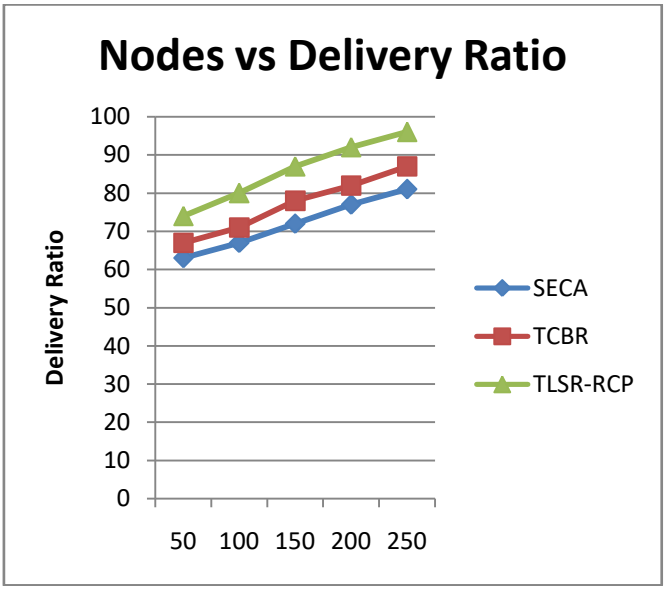

Figure 3: Performance on delivery ratio

The performance of the methods on delivery ratio is counted and matched with other methods value. The proposed TLSR-RCP algorithm has produced higher delivery ratio at the conditions of varying number of nodes than other SECA and TCBR algorithms.

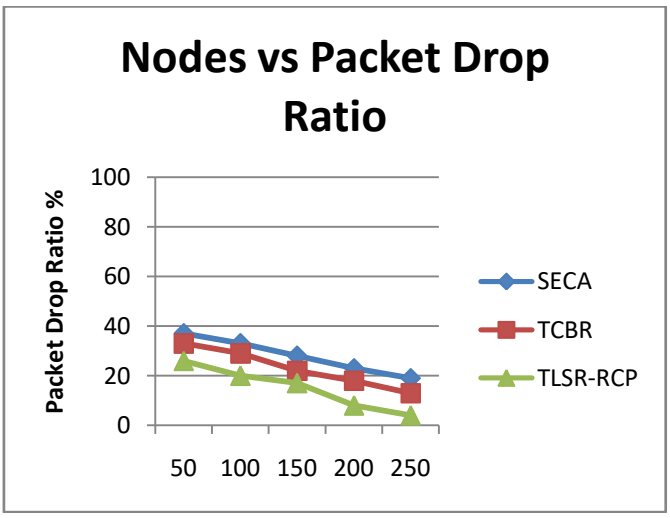

Figure 4: Performance on packet drop ratio

The packet drop ratio produced by different methods under varying number of nodes condition is measured and matched with other method values. The proposed TLSR-RCP algorithm introduces only negligible packet drop ratio at each condition which is less than SECA and TCBR algorithms.

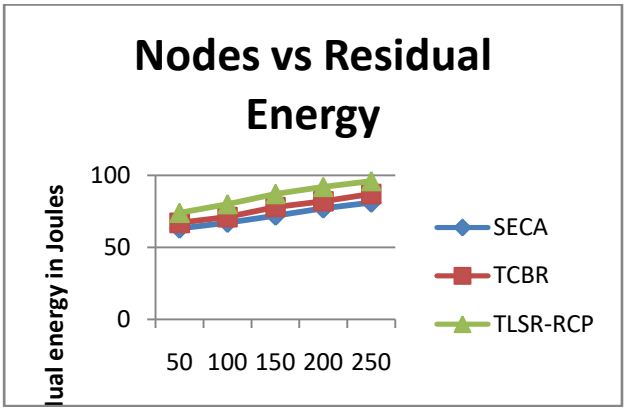

Figure 5: Performance on residual energy

The residual energy consumed by the methods at different conditions is measured and matched in Figure 5. The TLSR-RCP algorithm consumed less energy than other SECA and TCBR algorithms.

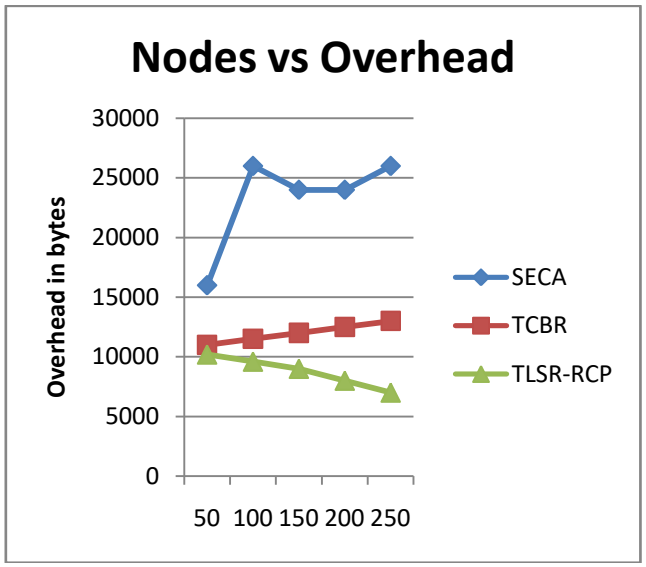

Figure 6: Performance on Overhead

The network overhead produced by different methods on varying number of nodes is measured and matched with the values of others. The TLSR-RCP approach introduces minimal overhead than SECA and TCBR algorithms.

V. CONCLUSION

An efficient trust based light weight secure routing algorithm for WSBN has been presented in this paper. The method performs routing according to the reputation of nodes in the route, completion support of the route and privacy preservation produced by the routes. Based on the above mentioned features, the computes the secure routing support measures for each route identified between the sensor and sink node. Finally, a route with higher security is elected. Similarly, the security at data level is achieved by adapting the block level encryption scheme. The TLSR-RCP method hikes the routing performance and security in WSBN.

REFERENCES:

1. Tao Yang, Xu Xiangyang, "A secure routing of wireless sensor networks based on trust evaluation model", Elsevier, Computer science, 131 (2018) 1156–1163, 2018.
2. Farruh Ishmanov , "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues", Hindawi, Journal of Sensors, 2017.
3. Hassan Oudani, "Energy Efficient in Wireless Sensor Networks Using Cluster-Based Approach Routing" , IJSSN, 5(1),6-12, 2017.
4. NidhiSharma ,"Privacy Preservation in WSN for Healthcare Application", Elsevier, Computer science, 132(2018), 1243-1252, 2018.
5. Mian Ahmad Jan ,"Moving Towards Highly Reliable and Effective Sensor Networks", Ad Hoc & Sensor Wireless Networks, 40, pp. 163–168, 2018.
6. Seyed Mahmood Hashemi, "Secure Routing of WBAN with Monarchy Butterfly Optimization", ACM, ICCIS, pages 155-158,2017.
7. Farzad Kiani , "Reinforcement Learning Based Routing Protocol for Wireless Body Sensor Networks", ISCSC, 2017.
8. Lin Li and Donghui Li , "An Energy-Balanced Routing Protocol for a Wireless Sensor Network", Hindawi, Journal of Sensors, 2018.
9. Yating Qu ,"A Survey of Routing Protocols in WBAN for Healthcare Applications, Sensors, 19(7), 2019.
10. Ghufran Ahmed , "Thermal and energy aware routing in wireless body area networks", IJDSN, 2019.
11. Rahat Ali Khan, "An energy efficient routing protocol for wireless body area sensor networks", JWPC, 99(4), 2018.
12. "EEHRT: Energy Efficient Technique for Handling Redundant Traffic in Zone-Based Routing for Wireless Sensor Networks", Hindawi, WCMC, 2019, 2019.
13. V.kavidha, S.anandakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink", Springer, Peer-to-Peer Networking and Applications, 2018.
14. Fouad El Hajji, "Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks", Springer, JCIN, 3(1), 67–83, 2018.
15. Sohail Jabbar, "Analysis of Factors Affecting Energy Aware Routing in Wireless Sensor Network", Hindawi, WCMC, 2018.