International Journal of Science Academic Research
Vol. 04, Issue 04, pp.5467-5471, April, 2023
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

SECURE PRIVACY PRESERVING ROUTING MODEL TO ENABLE LOCATION PRIVACY IN WBAN

***Sathya, G. and Evanjaline, D.J.**

Department of Computer Science, Rajah Serfogi College (Autonomous), Affiliated to Bharathidasan University, Thanjavur, Tamil Nadu, India

Received 20th February 2023; **Accepted** 15th March 2023; **Published online** 27th April 2023

Abstract

Wireless Body Area Networks (WBAN) provide the much needed transition from traditional healthcare systems to E- healthcare models. They enable the patient to perform their daily functionalities without frequent disruptions in their schedules by continuous collection of data automatically. These information are transmitted to the health care provider automatically for analysis. However, ensuring security and privacy in this process is of critical importance due to the highly sensitive nature of the information being transmitted. This work presents the Privacy Preserving Routing (PPR) model that includes elements to improve the security levels during transmission and also enhances the lifetime of the network by providing effective load balancing. The process of fine grained reactive routing included in the routing model ensures selection of the appropriate node to ensure high probability of packet delivery. Experiments were performed and comparisons with existing standard models indicate that the PPR model exhibits high stability levels which shows that the model is highly capable of handling sniffing attacks Ensuring high security in the delivery process.

Keywords: Wireless Body Area Networks, Secure Routing, Privacy Preserved Routing, Firefly Algorithm; Network Lifetime, Load Balancing.

INTRODUCTION

Increase in the Internet of Things (iot) based devices has been revolutionary in the healthcare domain by providing scope for next generation E-health systems. Utilizing electronic health systems can aid in providing improved quality health care to patients [1]. Current lifestyle has resulted in increased chronic diseases like cardiovascular problems, hypertension, diabetes etc. Preventing these disease by providing early detection is possible by continuously observing the data using medical devices. Improvement in wireless technologies effectively aid in building devices that can help in measuring the medical parameters [2]. This opens possibility for building industry healthcare applications. Wireless Body Area Networks (WBAN) are specialized type of wireless sensor networks that are widely used in healthcare applications [3, 4]. These devices are lightweight in nature and use wireless based transmissions. They are usually designed to perform specific functionalities. These devices have huge applications in the biomedical domain [5]. They can effectively aid in measuring biomedical data like heart rate, sugar levels, blood pressure, pulse rate, oxygen levels etc [6]. The devices are also capable of sending the measurements outside the network to devices for analysis by medical practitioners. Collecting measurements using these devices can be performed automatically without any interference to the normal life of the patient [7]. Automatic collection period Levels can be specified to ensure continuous monitoring by medical practitioners. Such effective monitoring can result in accurate and prompt analysis of any inherent issues [8]. WBAN devices are designed to be wearable and also implantable. They can perform intrabody communication and also extra body communication. Intra body communication is the process of communicating between the sensor and nodes that are implanted or placed on a single patient forming a network.

Corresponding Author:** ***Sathya, G
Department of Computer Science, Rajah Serfogi College (Autonomous), Affiliated to Bharathidasan University, Thanjavur, Tamil Nadu, India

Extra body communication is the process of communicating data to a device outside the network. Most critical measurements are obtained from implanted sensors, rather than sensors placed externally [9]. Major challenge in using wireless body area devices is the fact that the implanted devices are battery operated and battery replacement is not an option for these devices [10]. Routing is considered to be one of the major sources of charge depletion. Effective routing can aid in extending the lifetime of these networks [11]. Further, improving security during transmissions also play a vital role due to the highly sensitive nature of the information being transmitted. Sniffing attacks is one of the major attacks encountered in WBAN. Sniffing is the process of obtaining information from intermediate nodes. Identifying the source node can aid in easy interpretation of information. Hence, improving source node privacy can improve the security levels of the network. Developing routing techniques that cannot backtrack the source node is highly essential. This work presents a secure privacy preserving routing technique that aids in improving the security of transmission and also extending the lifetime of the network.

Related works

Security, privacy and extending network lifetime are some of the major requirements in WBAN. This section discusses some of the recent works that are based on satisfying the above mentioned requirements. A privacy preserving model for WSN has been proposed by Li *et al.* [12]. This work presents a mutual authentication scheme that also includes key agreement components to ensure security in WBAN. The model however was identified to be vulnerable towards intermediate node capture attack. It was identified to be effective towards replay and eavesdropping attacks. A secure RFID authentication based model for WBAN has been proposed by Izza et al [13]. The model aims to provide improved data security during transmissions and has also been identified to be resistant towards various attacks. It uses Elliptic Curve Cryptography

(ECC) mechanism and Elliptic Curve Digital Signature with Message Recovery (ECDSMR) to provide security to the transmitted message. An ID Verification scheme using ECC has been proposed by Liao *et al.* [14]. This work mainly focuses on improving the authentication levels based on the ID-verifier transfer protocol. A health care model using RFID for authentication has been proposed by Zhao [15]. This work is also based on ECC to improve the authentication process. A similar work using two way security authentication for RFID has been proposed by Liu *et al.* [16]. A privacy preserving model for health applications in WBAN was proposed by Odelu *et al.* [17]. This model mainly focuses on providing privacy for user credentials. The model provides robust security and also avoids large number of public keys to ensure low computation. Other similar key based authentication schemes for WBAN where proposed by Das *et al.* [18], Omala *et al.* [19] and Shen *et al.* [20]. A model explicitly designed to maintain anonymity based on mutual authentication schemes has been proposed by Gupta *et al.* [21]. The model aims to handle the resource constraint nature of WBAN devices to propose a lightweight protocol that provides improved security for the information being transmitted in the network. The work uses basic symmetric cryptosystems to improve the privacy levels and also maintain the lightweight nature of the protocol. Improving security in medical data transmissions is one of the significant requirements in a military environment. Wireless sensors aid in instant notification during emergency periods for the rescue team. The work proposed by Saravanakumar *et al.* [22] presents a Disturbance Resistant Network (DRN) which can effectively transmit data and are specifically designed for terrestrial environment. They use group based registration schemes to improve privacy. A machine learning based model so fault prediction in WBAN has been proposed by Awad *et al.* [23]. This work creates an ensemble of multiple machine learning models for the fault prediction process. A lightweight security model for WBAN has been proposed by Ullah *et al.* [24]. This work uses certificateless signcryption To improve the security levels during data transmission. An energy harvesting based technique for effective routing in WBAN has been proposed by Ullah *et al.* [25]. An extension to this approach using the clustering model has been proposed by Ullah *et al.* [26].

Privacy Preserving Routing (PPR)

Preserving privacy of the transmitted message is highly significant in any routing system. Packet sniffing is one of the most common attacks that can be encountered in any wireless network. A Wireless Body Area Network (WBAN) is a specialized type of wireless network that is used to measure the physiological parameters of a human patient by deploying wireless sensors in or on the body of the patient. The major work of sensors in WBAN is to collect information and aid the other sensors during the transmission process. Unlike WSN models, sensors in WBAN are different from each other due to the varied types of information collected by them. In general, sensors collect information like temperature, heart rate, blood glucose levels, uric acid levels etc. Data when paired with sensor identifiers will aid in determining the type of measurement. Sensors are primitive in nature and are specialised in collecting data accurately. Additional functionalities like incorporating cryptographic techniques will result in rapid reduction of battery life. Hence, it is always recommended to incorporate privacy preserving routing mechanisms to provide source privacy. This work presents a secure privacy preserving routing mechanism to aid in secure and faster routing, and improved privacy. The proposed architecture is composed of the network configuration and search space initialization phase, reactive routing phase and privacy preserving route identification phase. Algorithm for the PPR model is provided below.

Input: Node Coordinates, Start Node, End Node

Output: Route between start and end nodes

- Network configuration and search space creation
- Transmission Initiation and source and destination node determination
- If source node is directly connected to destination
- Perform direct transmission
- Set source node as the current node
- If source node is not directly connected
- Random firefly distribution in the search space
- Identify intensity levels of fireflies based on modified fitness function from the current node
- For every firefly f
- Determine and move towards the firefly with most optimal solution
- Goto step b until the search space has not converged
- Identify the node with maximum number of fireflies
- Use the node as the next hop and set it as the current node
- Verify if the current node is the destination node
- If so terminate routing process, else goto step b with the new node as the current node

Network Configuration and Search Space Initialization

The WBAN model constructed for this application is composed of 16 nodes (14 sensors and 2 sink nodes). The nodes are deployed in varied locations. Each node is specialized in collecting a different physiological parameter from the patient. Two nodes are designated as sink nodes. The responsibility of a sink node is to collect information from all the other nodes and to transmit it to the device outside the network for further analysis of the collected details. All the nodes are wirelessly connected and all the nodes transfer data to the sink node. The nodes that are directly connected to the sink node does not require any routing mechanism for the transmission. However, there are several other nodes that do not fall under the range of the sink node. This is due to the limit of the wireless signal range. Hence, these nodes require routing mechanisms for transmission of data. Sensors that are far from the sync node transmits information through neighboring sensors based on the routing mechanism applied in the network. Routing is performed using the modified Firefly algorithm. Hence, after the deployment of nodes, search space for the Firefly model is created based on the location of deployment of nodes and their connectivity status.

Transmission Initiation and Reactive Routing

When a transmission is initiated, the source and destination nodes are determined. In this case the destination node is the sink node. An additional verification mechanism is employed to determine if the source node is directly connected to the sink node. If so, the transmission is directly performed. Since there is no intermediary involved in this transmission, the transmission is intrinsically secure. However, considering the

nodes that are not directly connected to the sink node, their transmissions are usually performed with the aid from other intermediate nodes. Such transmissions are vulnerable in nature, and it's vulnerability level increases with the increase in number of nodes. Such transmissions are prone to sniffing attacks. To ensure security of the transmitted packet, it becomes mandatory to employ a routing algorithm that provides high degree of safety for the transmitted packet. This work proposes a modified Firefly algorithm to enable secure routing. The route identification mechanism employed in this work is reactive in nature. Reactive routing triggers the route identification process only after the transmission is initiated. This work performs fine grained reactive routing which identifies the next hop for transmission only when the requirement arises. The entire route is not identified beforehand. This process has two advantages namely; reduced retransmission and Privacy preservation. As every hop node is determined just prior to the transmission, node failure, no depletion and probability of the packet being sniffed are avoided. Every need for transmission triggers the modified Firefly algorithm to determine the next best hop for transmission. After the transmission to the next hop, a verification mechanism is triggered to check if it is the sink node. If the node is not the sink node, the next optimal node for transmission is determined. This improves the privacy levels to a large extent and aids in avoiding packet sniffing.

Privacy Preserving Route Identification using Modified Firefly Algorithm

The search space for the Firefly algorithm is composed of nodes depicting sensors and connectivity details of the nodes based on their wireless transmission levels. Source node is the transmission initiator, sync node with the Terminator node. Fireflies Are used as the agents to determine the most optimal solution. Fireflies are dispersed in the search space in random to all the nodes that are directly connected to the source node. Movement of fireflies is based on their light intensity which provides the fitness of a Firefly. General Firefly algorithm assumes that all the nodes are connected to each other, and uses the distance factor to determine the light intensity of The fireflies. The proposed modified Firefly algorithm is constrained based on the connectivity factors, and the intensity level which determines the fitness of fireflies is modified by integrating the charge of nodes, temperature levels and the distance factors. These factors ensure that the modified algorithm determines the optimal solution based on the current status of nodes rather than the distance factor alone.

The intensity of a firefly f is given by,

$$I_{f,s} = \frac{f_{ch}}{d_{f,s} \times f_{temp}}$$

Where f_{ch} is the charge of the firefly f, $d_{f,s}$ is the distance between the firefly f and the source node s and f_{temp} is the temperature of the firefly f. After the determination of the light intensity, All the fireflies move towards the Firefly that exhibits the highest light intensity level. This process of intensity identification and movement is repeated until convergence is reached. Convergence is achieved when all the distributed fireflies in the search space are accumulated on a single node. However, this process might be time consuming. Hence, a predefined level 4 maximum number of iterations is set by the domain expert. When this threshold is reached, the fireflies are considered to have converged. Since, the actual convergence has not been achieved, some fireflies might occupy different nodes. Hence the optimal node is identified by determining the node containing maximum number of fireflies. The process of identifying the optimal next hop node is given by,

$$optima = argmax_{j\in(0,n)}(posVector_j)$$

$$posVector_i = \sum_{j=0}^{n} count_{ij} \ \forall i = 0,1 \dots n$$

$$count_{ij} = \begin{cases} 1 & if pos_i = pos_j \\ 0 & Otherwise \end{cases}$$

Where pos_i *and* pos_j are the coordinate positions of fireflies *i* and *j* respectively and *n* is the number of fireflies.

The selected optimal node is considered as the next hop and the package is transmitted to this node. This node is set as the source node and the process of identifying the next node is iteratively performed until the sink node is reached.

RESULTS AND DISCUSSION

The node deployment coordinates, and the simulation parameters employed in the E-HARP model have been adopted in this work to enable comparison. Comparisons of results from the proposed PPR model is performed with the E-HARP model proposed by Ullah *et al.* [25], and its extension, the EH-RCP model [26]. The transmissions are initiated, and the network is monitored for 18000 transmissions from random nodes at random time. The network parameters have been recorded for every 2000 iterations for analysis. The transmission time requirements for the proposed PPR model is shown in figure 1. Time requirements for every 2000 transmission has been recorded. It could be observed from the figure that the range of transmission times varies between 9 seconds and 11 seconds. The average time requirement for the entire transmission has been observed to be 10 seconds. Such low transmission times exhibit the load time requirements in the routing process. This validates that the proposed PPR model identifies the next hop nodes faster and more effectively, hence reducing the transmission latency to a large extent.

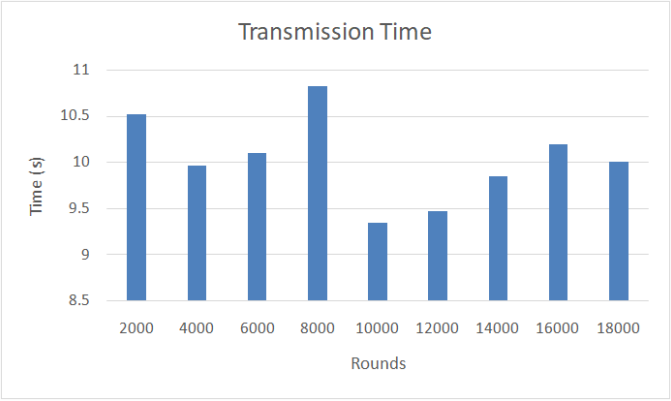

Figure 1. Transmission Time of PPR

Table 1. Network Lifetime Analysis of PPR

	0	2000	4000	6000	8000	10000	12000	14000	16000	18000
PPR	0	0	0	0	1	1	2	3	6	10
E-HARP	0	0	0	0	1	3	5	10	14	14
EH-RCP	0	0	0	1	3	4	5	10	14	14

Table 2. Stability Analysis of PPR

	0	2000	4000	6000	8000	10000	12000	14000	16000	18000
PPR	14	14	14	14	13	13	12	11	8	4
E-HARP	14	14	14	14	13	11	9	4	0	0
EH-RCP	14	14	14	13	11	10	9	4	0	0

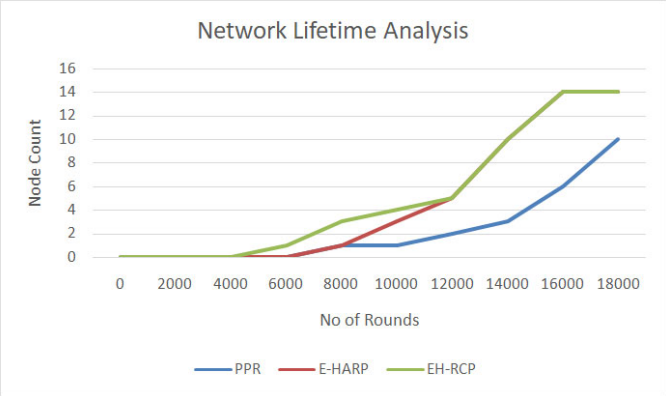

Figure 2. Comparison of Network Lifetime of PPR

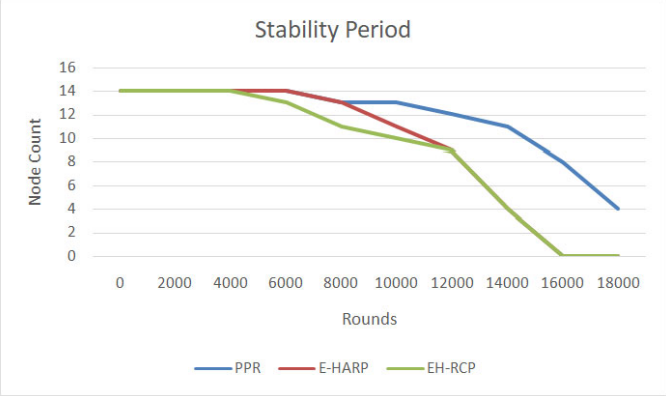

Figure 3. Comparison of Stability Levels of PPR

Comparative study

A comparative analysis of the PPR model has been performed with E-HARP and EH-RCP models. Comparisons were performed in terms of network lifetime analysis and stability analysis. A comparison of the network lifetime analysis is shown in figure 2. Network lifetime refers to the number of depleted nodes in the network at a particular Time period. It could be observed that the network deterioration levels begins at iteration 6000 for the EH-RCP model, while the deterioration levels for PPR and E-HARP begins at iteration 8000. The deterioration levels are quite rapid in E-HARP and EH-RCP models, and the network fails at iteration 16000. However, the PPR model exhibits lower deterioration levels and even after the iteration 18000 the model can still be observed to contain live nodes. These results depict the effective load balancing scheme employed by the PPR model. Further, the randomization included in the load balancing process aids in secure transmissions resulting in reduce the need for retransmission scenarios. A tabulated view of the network lifetime analysis is shown in table 1. The results indicate high failure levels in the E-HARP and EH-RCP models. After every 2000th iteration the node failure levels increase considerably and the entire network failure with 14 failed nodes occurs at iteration 16000. However, the PPR model exhibits slow failure rates and even after the iteration 18000 the network is live with four active nodes and two sink nodes. Stability period Indicates the number of live nodes existing in the network. High stability levels indicate secure and reliable networks. Frequent retransmissions results in rapid reduction of stability levels in the network. A comparison of the Stability levels is shown in figure 3. Although the network remains stable till the 4000th iteration, the stability levels of EH-RCP and E-HARP starts reducing rapidly after the initial failure. However, the PPR model shows higher stability levels indicating low retransmission and effective routing process. A tabulated view of the stability levels is shown in table 2.

The rapid reduction of stability after the initial failure at 6000th iteration in EH-RCP and 8000th iteration indicates the model is prone to retransmissions due to node failure and attacks. However, the PPR model indicates high stability depicting low retransmissions and high resilience towards attacks. This shows the enhanced security levels brought into the routing mechanism with the inclusion of privacy preserving techniques in the PPR model.

Conclusion

Wireless Body Area Networks (WBAN) are especially case of Wireless Sensor Networks (WSN). These networks are specifically used for healthcare purposes, wide deploying the sensor nodes in order on human body for continuous measurement of physiological parameters of the patient. Battery, size and functionality of the node apart from collecting the required information provides ample challenges in designing a secure and privacy preserving routing protocol. This work presents a security enhanced privacy preserving model PPR, based on the modified Firefly algorithm to ensure high efficiency during the routing process. Reactive routing technique is employed in a fine grained manner to ensure privacy. The model has been identified To reduce retransmission levels to a large extent and also provides safety from sniffing attacks by selecting different routes during the transmission process. The model has been identified to reduce transmission time to a large extent and also extends the lifetime of the network. Future enhancements of the model can be in the form of including cryptography based techniques to encrypt the transmitting information for better protection.

REFERENCES

1. Hossain MS, Muhammad G . Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. *Comput Netw,* 2016;101:192–202 .

2. Patel M, Wang J. Applications, challenges, and prospective in emerging body area networking technologies. IEEE *Wirel Commun Mag.,* 2010;17(1):80–8 .
3. Shen J, Chang S, Shen J, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. *Futur Gener Comput Syst.,* 2018;78:956–63 .

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, *IEEE Communications Surveys Tutorials* 17 (4) (2015) 2347–2376.doi:10.1109/COMST.2015.2444095.

4. Kumar, A. A. Rahmani Hosseinabadi, M. Shareh, A. Zolfagharian, N. Chilamkurti, S. Rad, Iot resource allocation and optimization based on heuristic algorithm, Sensors (2020) 539.
5. Sangaiah, K., M. Sadeghilalimi, A. A. R. Hosseinabadi, W. Zhang, Energy consumption in point-coverage wireless sensor networks via bat algorithm, *IEEE Access,* 7 (2019) 180258– 180269.
6. Sangaiah K., D. V. Medhane, T. Han, M. S. Hossain, G. Muhammad, Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics, *IEEE Transactions on Industrial Informatics,* 15 (7) (2019) 4189–4196.
7. A Survey on Security and Authentication in Wireless Body Area Networks
8. A survey on wireless body area networks: architecture, security challenges and research opportunities
9. Salayma, M., Al-Dubai, A., Romdhani, I., & Nasser, Y. (2017). Wireless Body Area Network (WBAN) A Survey on Reliability, Fault Tolerance, and Technologies Coexistence. *ACM Computing Surveys (CSUR),* 50(1), 1-38.
10. Abidi, B., Jilbab, A., & Mohamed, E. H. (2020). Wireless body area networks: a comprehensive survey. *Journal of Medical Engineering & Technology,* 1-11.
11. X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, K.-K. R. Choo, Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks, *Computer Networks,* 129 (P2) (2017) 429–443. Doi:https://doi.org/10.1016/j.comnet.2017.03.013
12. An enhanced scalable and secure RFID authentication protocol for WBAN within an iot environment
13. Liao YP, Hsiao CM. A secure ecc-based rfid authentication scheme integrated with id-verifier transfer protocol. *Ad Hoc Netw*., 2014; 18:133–46. Http://dx.doi. Org/10.1016/ j.adhoc.2013.02.004.
14. Zhao Z. A secure rfid authentication protocol for healthcare environments using elliptic curve cryptosystem. *J Med Syst.,* 2014b; 38:46. Http://dx.doi.org/10.1007/ s10916-014-0046-9.
15. Liu B, Yang B, Su X. An improved two-way security authentication protocol for rfid system. Information 2018; 9(86). Http://dx.doi.org/10.3390/info9040086.
16. Efficient privacy preserving device authentication in wbans for industrial e-health applications
17. Das AK, Chatterjee S, Sing JK . A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks. *Adhoc Sens Wirel Netw.,* 2015;28(3/4):221–56 .
18. Omala AA, Kibiwott KP, Li F . An efficient remote authentication scheme for wireless body area network. *J Med Syst.,* 2017;41(2):25
19. Shen J, Tan H, Moh S, Chung I, Liu Q, Sun X . Enhanced secure sensor association and key management in wireless body area networks. *J Commun Netw.,* 2015;17(5):453–62 .
20. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN
21. Efficient privacy preserving device authentication in wbans for industrial e-health applications
22. Das AK, Chatterjee S, Sing JK . A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks. *Adhoc Sens Wirel Netw.,* 2015;28(3/4):221–56 .
23. Omala AA, Kibiwott KP, Li F . An efficient remote authentication scheme for wireless body area network. *J Med Syst.,* 2017;41(2):25
24. Shen J, Tan H, Moh S, Chung I, Liu Q, Sun X . Enhanced secure sensor association and key management in wireless body area networks. *J Commun Netw.,* 2015;17(5):453–62 .
25. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN.

****