International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Better Security Aware D2D Transmission Protocol with Optimal Relay Assignment Algorithm (ORAA)

V.Nandalal, M.S.Sumalatha, V.Anand Kumar, T.Manikandan

ABSTRACT--- The systems which deals with healthcare are rapidly untouched and a widespread area, where both opportunities & challenges are plenty. The increase of smart mobile phones and advancement in sensors which are used for medical purpose, these devices enhance Wireless Body Area Networks (WBAN). Which is used for patient monitoring remotely called as M-health also called as Mobile-health. It increases the quality and health care by providing a reliable and cost effective. In this system, a protocol called LSAP (Lightweight and Security Aware protocol). LSAP is proposed to assist Device to Device transmission of data for Mobile health systems by means of ORA (Optimal Relay Assignment) algorithm. Linear marking Mechanism was a general idea behind ORAA algorithm. To realize polynomial time complexity at the end of every iteration; are offered by linear marking. To increase the objective function during iteration process, ORA regulate the assignment which is the preliminary assignment. Source node of minimum capacity was identified by ORA at the time of iteration process, which results in designing an efficient system.

Keyword - WBAN, LSAP, ORA, M-Health

I. INTRODUCTION

A system which performs M-Health is visualized as a positive enhancement to improve health care feature and saves lives in the aging society. In Health systems, the PHI - Personal Health Information is collected by BAN - Body Area Network and collected by smart phone. Heath care centre receive data sent via cellular network. To the escalating popularity of healthcare, the health check information send to base stations may exasperate the previously overload cellular networks. Luckily, D to D communications be suggest to be an most beneficial answer to meet up with the inflammable trying of spectrum since they could be used on the same resources over shorter distances. Accordingly, this paper proposes to broadcast the Personal heath information through Device to Device exchanges in Medical-health systems. Device-to-Device interactions are unsafe to safety attacks likes eave dropping, false messages, confidentiality contravention, etc. Nowadays, safety of systems deals with M-health has paying huge attentions. The majority of these mechanisms largely center of attention on any unknown verification or confidentiality concern even as rejecting the precautions at some stage in information communication. By taking into consideration, this trouble of maintaining high privacy scheme in opposition to worldwide eaves dropping for M-health system. These are settler mechanism on safety measures on information communication for M-health system at the same time as they won't take into account the Device to Device assist data transmission layout.

The new certificate less generalized Signcryption algorithm be able to work on three modes: Signcryption mode, signature mode, or encryption mode flexibly. We use Certificate Less Generalized Signcryption to design a Light weight and Security Aware protocol D 2 D assist information communication procedure for M-health system. At first the Personal Health Information is sum up with Signcryption mode and then the source's uniqueness is encrypted with the encryption mode by the source client, thus it achieving data confidentiality and data integrity, mutual authentication and contextual privacy. In inclusion, a session key is introduced in the Signcryption algorithm to increase the security strength. At the end of each transmission session, the session key is modernized updated by a secure hash function to attain promote protection. Furthermore, the source client and all the relays sign on the encrypted information to promise information reliability. Particularly, the projected Light-weight and Security-Aware protocol can to attain obscurity and unlink facility by using the pseudo uniqueness and a random number in the code manuscript of the distinctiveness.

To provide better connectivity wireless networks are fast changing mobile technology. The demands of new applications in multimedia are increased and the requirements are enhanced capacity and data rate should be high. To meet the above mentioned requirements in wireless channel, new generation wireless communication should be deploy. To overcome the wireless channel problem one important technique is Multi Input Multi Output (MIMO).

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Dr.V.Nandalal, Associate Professor, Sri Krishna College of Engineering and Technology, Coimbatore, T.N, India. (E-mail: nandalal@skcet.ac.in)
M.S.Sumalatha, Research Scholar, Sri Krishna college of Engineering and Technology, Coimbatore, T.N, India. (E-mail: mysansuma@gmail.com)
V.Anand Kumar, Assistant Professor, Sri Eshwar College of Engineering, Coimbatore, T.N, India. (E-mail: anand.kkr@gmail.com)
Dr.T.Manikandan, Professor, Department of ECE, Rajalakshmi Engineering College, Chennai, T.N, India. (E-mail: Manikandan.t@rajalakshmi.edu.in)

In wireless network for obtaining the spiral diversity, multiple antennas in transmission and reception are installed. This was wide accepted solution, which results to outcome fading in wireless channel. Cooperative communication is new distributed spatial diversity, based on the coordination between terminals in wireless technology. To improve the wireless cooperative network, a new technique called wireless relay networking is used. It reduces the use of multiple antennas per terminal. Antenna array can be provided by relay network which allow terminals to collaborate. It provides a better cooperative in practical use, because every node desires only single antenna as a relay node. This forms a virtual antenna array.

II. LITERATURE SURVEY

Rongxing Lu et al presented a paper "A Secured Privacy-Preserving Opportunistic Computing Framework for the Mobile-Healthcare Emergency" explains penetrating of smart mobile phones and the benefits of BSN, m-healthcare, which broaden the process of Healthcare provider into a common environment for enhanced health check up, that has paying attention substantial attention in recent times. However, extend of M-healthcare still have a lot of dispute together with data precautions and confidentiality maintenance. In this manuscript, we present a protected and confidentiality preserving opportunistic computing framework, called Secure Privacy and Opportunistic Communication, for mobile- healthcare crisis. By means of SPOC, Mobile phones property which includes energy and power of computing that can be opportunistically jointly to development the computing intensive PHI through M-healthcare crisis by means of negligible confidentiality exposure. In exact, to influence the Personal Health Information confidentiality leak and the efficient consistency of Personal Health Information method and communication in mobile-healthcare crisis, we initiate an well organized user friendly confidentiality controlled access in Secure Privacy and Opportunistic Communication framework, which is based on attribute based controlled access and a latest Privacy Maintaining Scalar Product Computation (PPSPC) system, and allows a client to make a decision who know how to take part in the opportunistic computing to assist in dealing out information. The concluded safety study illustrates that the projected Secure Privacy and Opportunistic Communication framework be able to proficiently attain user centric privacy access control in M-healthcare crisis

Linke Guo et al presented a paper“ A Secured Attribute-Based Authentication Systems for the Mobile Health Networks”, explains how healthcare system based on electronics comprise paper based health care system owed to the smart feature such as worldwide ease to access, efficient accuracy level, and cost efficient. since a most important section of Electronic health system, m-healthcare concern to smart phones on the way to facilitate patient to physician and patient to patient interactions meant for improved health care and excellence of life. Unfortunately, patient’s examination on possible leak of individual healthiness data is the leading elegant block. In present Electronic networks, medical data of patients are usually related through a set of features like living indications and present treatment based on the data collected from portable systems. Personal Health Records must be provable for assurance the accuracy of those features. Conversely, owing to the tie facility among distinctiveness and Personal Health Records, existing M-health system falls to preserve patient identity confidentiality though contributing health services. To resolve this difficulty, we put forward a decentralized arrangement that leverages user’s confirmable features to verify each other [2]. X.Liang et al presented a paper “PEC: A Privacy – Preserving Emergency call scheme for mobile healthcare Social networks”, proposes a PEC, facilitates patients in urgent situations to speedy and precisely pass on crisis information to the close by assistants by means of MHSNs- Mobile Healthcare Social Network. On one occasion an urgent situation occurs, the PDA-Personal Digital Emergency Assistant of the patient run the Privacy Emergency call to gather the urgent situation information which includes locality of patients, his/her healthiness record and also physiological patient conditions. The Privacy Emergency call makes sure the instant to inform the medical doctor of the urgent situation is the shorter distance. We show via hypothetical investigation that the Privacy Emergency Call is able to offer fine grained access control on the urgent situation information, wherever the accurate to employ strategy is situate by patients. In addition, we exhibit via simulation that the privacy Emergency call can be to decrease the reply time of situation under emergency care in Mobile Healthcare Social Networks [5]

J.Liu et al presented a paper “Certificate Less Remote Anonymous Authentication Scheme For Wireless Body Area Networks” explains how WBAN have been known as a one of the most capable wireless sensor technologies for efficient healthcare examine gratitude to its potential of faultlessly and endlessly exchanging medicinal data in real time. Conversely, they not have an understandable in depth resistance line in such a latest networking models would make its probable users be anxious about the leak of their classified information, particularly to the individuals unauthenticated. In this manuscript, we present a pair of well-organized and less weight verification protocols to facilitate distant Wireless Body Area Network users to secretly enjoy health care services. In particular, our verification protocols are deep-rooted with a tale CLS-certificate less signature scheme, which is computational resourceful and provably protected adjacent to existential falsification on adaptively chosen message attack in the random oracle model. Also, our design makes sure that request or service provider have no license to reveal the actual individuality of users. Even network manager, provides a confidential key generator in verification protocols, and is prohibited from imitating legal users. The performance of our designs are assessed from end to end both theoretic investigation and experimental replication, and a comparative study reveals that they are better than existing scheme in terms of improved tradeoff between enviable security properties and computational overheads, nicely meeting the needs of Wireless Body Area Network [7].

III. LIGHT WEIGHT AND ROBUST SECURITY AWARE(LRSA ALGORITHM)

A light weight and security aware Protocol, device to device assist data communication protocol for system performing M-health by means of certificate less generalized Signcryption method. Particularly, we initially proposed a latest well organized certificate less generalized Signcryption scheme which can lithely work as one of the three cryptographic primitives:

1. Signcryption algorithm
2. Signature algorithm
3. Encryption algorithm

By using the proposed certificate less generalization Signcryption scheme, light weight and security aware protocol attains information privacy and reliability, shares verification and background confidentiality. Moreover, obscenity and uplink capability are along with noticed by using the pseudo identity and selecting different random number at dissimilar sessions. In addition, light weight and security aware protocol has a uniqueness of promote security with hash chain of sectional key. The proposed light weight and security aware protocol is collected by the following four phases:

1. System initialization
2. Data formulation
3. Data transmission
4. Data receiving

By using this proposed certificate less generalized Signcryption scheme, Light Weight and Security Aware protocol attains information privacy and reliability, shared verification and background confidentiality. As the personal health information is protected twice by both session and complete confidential key of the deliberate doctor. Revelation of one key will not influence the privacy of the user information. Both the Signcryption of the PHI-personal heath information by the client and the signature conducted by the relays guarantee reliable information. The drawbacks of efficient entire will pretentious, if the number of relay nodes is dynamic in nature. Effectiveness of the overall system will be increased.

IV. OPTIMAL RELAY ASSIGNMENT

A major difficulty of relay node assignment in the co-operative communication in wireless network is resolve up to the greater level by the algorithm called ORAA- Optimal Relay Assignment Algorithm. The essential design of this algorithm is a “Linear Marking” mechanism. This Linear Marking mechanism proposes a linear difficulty at every iteration results in attaining polynomial time difficulty. This algorithm work despite of consequences the number of relay nodes at the source or destination. Preliminary with this initial assignment, ORAA regulate the task during iteration, with the objective of raising the objection function. Particularly, for the period of iteration, ORRA classify the source node that corresponds to smallest amount capacity.

Algorithm as projected here is based on the extensively used purposed for the mutual communication which is capacity. Each node in the destination and source pair will display the dissimilar capacity subsequent to applied algorithm. The effort in anyway supposed to be maximization of the capacity of the meticulous pair along with all pairs of destination and source. It is not essential that in each network there should be sufficient relay nodes accessible. Capacity improvement of the pair in source and destination should be the eventual effect of the relay node assignment. Yet again a vital thing is that, an algorithm does not always allot the relay node to the pair in source and destination. If the assignment of the relay node demonstrates the slighter capacity as compared to the direct communication, there will be no relay assignment in pairs.

Making straightforward operation of the algorithm, it is constantly interested in maximizing the least capacity of the pairs of source and destination. Which means, the capacity with scrupulous pair of source and destination is performing the communication will always been tired to be exploit by conveying the appropriate relay node, but if that relay node is unproductive that is not able to maximize the capacity up to attractive level, then the relay will not be assigned to that pairs in source and destination and the direct communication will be carried out. The compensation of algorithm works apart from the number of relay nodes is less or more than the number of source and destination nodes. Effective of the overall systems will be increased.

V. BLOCK DIAGRAM

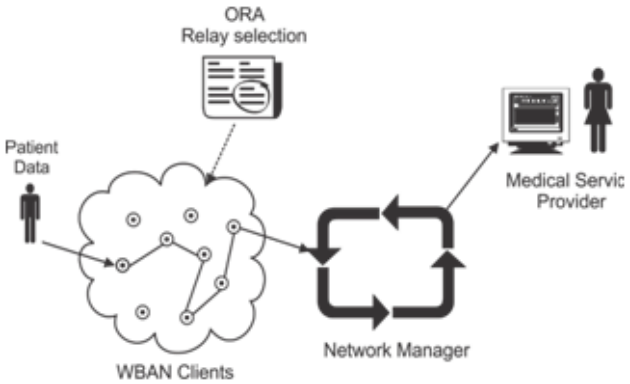

Fig.1. System Architecture

The three major blocks in the system architecture of Mobile-health are

1. Network Manager (NM)
2. Wireless Body Area Network (WBAN) Client
3. Medical Services Providers

Network manager (NM): NM will be a commanding body which is the incharge of the entire architecture. The functions like patient managing and initializing the system are done here. In the proposed scheme, it is a generation center. Network manager can’t be completely trusted, as it might be operate by the business organization or M-Heath center. Accordingly, the NM only provides a partial private key to keep away from the key escrow difficulties and also it is banned the right to use patient physical condition data base. WBAN Client: It is a medicinal client prepared with a mobile phone plus personal WBAN. The WBAN contains various body sensors like blood pressure sensor, oxygen saturation sensor, body temperature sensor and so on,.

All the information sensed by these sensors will prepare the client personal health information, which is sent to the smart phone which is important component in the M-health. As it process PHI and the mail information to the network manager for getting the related doctor. Unlike from the in-bed patient, the wireless body area network clients are smart phone users in our architectural model of M-health. Customer has to register to the network manager for joining the Mobile Health systems.

Medical Service Providers: They are doctors, clinic or hospitals. They offer consulting service or medical services to the Patients or customers. They also required preloading restrictions and registering to the network manager earlier they provide to customers. In our system architecture, we believe that the doctors get the liability of Medical Service Provider.

Time domain, frequency domain, hybrid frequency/time domain and cooperative relaying techniques are some of the conventional methods of relaying.

Frequency domain relaying:

Relays are working on channels with dissimilar frequency. The major benefits of this relaying are relays can broadcast and accept information at the same time.

Hybrid frequency/ time domain relaying:

It operates occasionally on dissimilar frequency channels to send information. The scheme here is to change frequencies between the base stations. Where the base station broadcast the information to its customer at the same time relay is transmitting information on different frequency.

Co- Operative relaying method:

This method considerably improves the features of relay based architecture by numerous RSs considerately broadcast the similar information to a Service station or the Base Station. This situation forms the similarity with MIMO method with broadcast/accept assortment and spatial multiplexing.

Path management:

IEEE 802.16j network encompass multi-hop paths between the Base Station and Master Station, the desires a controlled path management mechanism. There classify two approaches, embedded path management and explicit path management.

Relay path routing:

The method of formative most appropriate route to Base Station from source Master Station by taking into consideration of limits such as availability of, radio resource, bandwidth, interference etc,. In central routing path information is saved in the Base Station, but in distributed path routing path information is occupied. For dropping the right of entry and latency and in addition by means of the radio resource efficiently, the distributed path routing is chosen in excess of the centralized one. Whole networks can't be controlled by centralized path routing. Throughput of a wireless link depends on both the bandwidth of the link and the Physical layer loss rate.

VI. RESULT

From the analysis it is proved that the new scheme ORAA maintains a consistent improvement in the efficiency irrespective of the number of datasets. Table I shows the complete analysis of two methods with corresponding data sets.

Table I: Comparison table

Datasets	300	500	900
LRSA	87.34	86.34	81.45
ORAA	93.24	94.34	94.78

CONCLUSION:

In this system Light weight and Robust Security Aware (LRSA) is a proposed M-Health system by using certificate less generalized Signcryption method along with a powerful relay selection strategy called Optimal Relay Assignment Algorithm (ORAA). The Relay selection act as a very important position in exploiting the variety of gain achieved in wireless cooperative communication systems, and therefore relay selection has appropriately paying attention. The experiments result shows that the efficiency of the Certificate Less Generalized Signcryption system is increased with ORAA.

EXPERIMENTAL EVALUATION:

The experimental evaluation is done to prove the performance of the proposed system ORAA which is evaluated with the existing LRSA scheme.

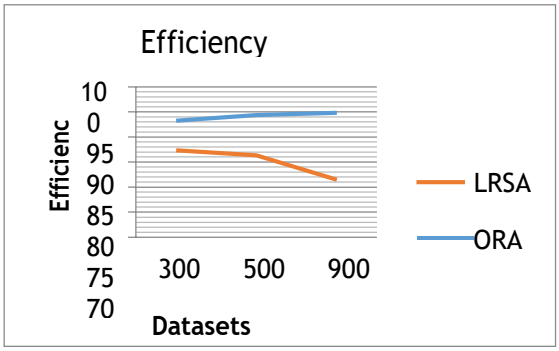

Fig.2. Efficiency Evaluation

The above comparison table is used for performance evaluation between LRSA and ORAA with dataset 300, 500 and 900 processed by same number of WBAN clients.

REFERENCES

1. Rongxing Lu, Xiaodong Lin, Xuemin Shen "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, Issue: 3, March 2013.
2. Linke Guo,Chi Zhang, Jinyuan Sun and Yuguang Fang "A Privacy- Preserving Attribute - Based Authentication System for Mobile Health Networks", IEEE Transactions On Mobile Computing,Vol.13,No. 9, September 2014.

3. Dr. V.Nandalal and N.Sathish Kumar,"A Detailed Study on Reconfigurable Circular Patch Antenna", International Journal of Pure and Applied Mathematics, Volume-119, Issue-12,pp-1545 – 1553, 2018.
4. Dr. V.Nandalal and N.Sathish Kumar,"Performance Evaluation of Reconfigurable Circular Patch Antenna", International Journal of Advance Research Trends in Engineering and Technology, Volume 4, Issue 7, pp-55 – 59
5. Xiaohui Liang, Rongxing Lu, Le Chen, Xiaodong Lin, and Xuemin (Sherman) Shen "PEC: A Privacy-Preserving Emergency Call Scheme for Mobile Healthcare Social Networks". Journal of Communications and Networks, Vol. 13, No. 2, April 2011.
6. Dr. V.Nandalal and V.Anand Kumar, "A Comprehensive Study on Encoding Techniques in Low Density Parity Check Codes", Journal of Advance Research in Dynamical and Control Systems, Volume 10, Issue 12(Special Issue), 2018.
7. Jingwei Liu, Zonghua Zhang, Xiaofeng Chen, Kyung Sup Kwak, "Certificate less Remote Anonymous Authentication Schemes for Wireless Body Area Networks". IEEE Transactions on Parallel and Distributed Systems Volume: 25, Issue: 2, Feb. 2014
8. A. Bletsas, A. Khisti, D. Reed, A. Lippman, "A simple cooperative diversity method based on network path selection", IEEE J. Sel. Areas Commun., vol. 24, no. 3, pp. 659-672, Mar. 2006.
9. T. Clause, P. Jacquet, Optimized link state routing protocol, Oct. 2003.
10. K. Mandke, R. C. Daniels, S. Choi, S. M. Nettles, R. W. Heath, "Physical concerns for cross-layer prototyping and wireless network experimentation", Proc. ACM Int. Workshop Wireless Netw. Test beds Exper. Eval. Charac. & MobiCom, pp. 11-18, 2007-Sep.-10.
11. K. Azarian, H. E. Gamal, P. Schniter, "On the achievable diversity-vs-multiplexing tradeoff in cooperative channels", IEEE Trans. Inf. Theory, vol. 51, pp. 4152-4172, Dec. 2005.
12. A. Bletsas, Intelligent antenna sharing in cooperative diversity wireless networks, 2005.
13. Jingwei Liu , Zonghua Zhang, Xiaofeng Chen and Kyung Sup Kwak "Certificate less Remote Anonymous Authentication Schemes for Wireless Body Area Networks", 2013 IEEE.