RESEARCH ARTICLE OPEN ACCESS

Performance Analysis Of An Improved Aodv Routing Protocol In Wireless Body Networks

Simhadri Lokesh[1], B jogeshwara Rao[2]
[1]*M.Tech (CSE), Dept. of Computer Science and Systems Engineering,*
[2]*Research Scholar, Dept. of Computer Science and Systems Engineering, Andhra University College of Engineering (A), Visakhapatnam, Andhra Pradesh, India.*
Corresponding Author: Simhadri lokesh

ABSTRACT
Over the past few years, there is an exponential growth in the wireless body area network (WBAN) for mobile patient monitoring system in areas of information processing and data transmission. WBAN provides low cost, wireless Body network technology that creates a system to monitor the patient remotely using an Internet or intranet, and it could be seen as a special-purpose wireless Body node network that provides the health monitoring to anyone, anytime and anywhere. As the position and speed of the remote mobile patient are continuously changing, that creates unpredictable topology and link instability. Therefore, routing is a very important task in WBAN. It is Difficult to select the suitable algorithm for desired network in the form data efficiency, end- to-end delay and the throughput. Many challenges, including a medical data transmission error and how to provide better healthcare services in underserved areas, are taken into account. To solve this problem we proposed a AODV routing algorithm to increase the network efficiency, data transmission, by measure the delay, throughput and improve the performance of Mobile Patient Network.
Keywords: WBAN, CSN, Network Architecture, Implementation Challenges, Data analysis, AODV.

Date Of Submission:16-11-2018 Date Of Acceptance:30-11-2018

I. INTRODUCTION

The concept of WBAN is nothing but the wireless sensor network which is consisting of various networks as well as wireless devices in order to enable the remote monitoring of person body functionalities and corresponding environment. Technological advancements in sensors, low-power integrated circuits, and wireless communications have enabled the design of economically viable miniaturized sensor nodes that can measure vital physiological parameters.The WBN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) Body's. Each such Body network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the Body's and an energy source, usually a battery or an embedded form of energy harvesting. A Body node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of Body nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual Body nodes. Size and cost constraints on Body nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WBNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.One major challenge in a WBN is to produce low cost and tiny Body nodes. There are an increasing number of small companies producing WBN hardware and the commercial situation can be compared to home computing in the 1970s. Many of the nodes are still in the research and development stage, particularly their software. Also inherent to Body network adoption is the use of very low power methods for data acquisition.In many applications, a WBN communicates with over a Local Area Network or Wide Area Network through a gateway. The Gateway acts as a bridge between the WBN and the other network. This enables data to be stored and processed by device with more resources, for example in a remotely located Server_ (computing).

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the simulator partly because of the range of features it provides and partly because it has an open source code that can be modified and extended. There are

different versions of NS and the latest version is ns-2.1b9a while ns-2.1b10 is under development

Network Simulator (Ns)

Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

NS is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast

quickly, is used for simulation configuration. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios. To simply use the simulator, it is sufficient to know

OTcl. On the other hand, one disadvantage is that modifying and extending the simulator requires programming and debugging in both languages.

II. RELATED WORK

In [6], the authors suggested an enhanced AODV to provide support to QoS, presuming the existence of some fixed connections in the network. The authors presented the concept of node consistency, founded on a node's history, which contained both a node's packet processing ratio and its mobility. Only consistent nodes were counted for routing. Still, the authors did not count the affect that indeterminable link failures would have on re-routing. In [7] authors have introduced a consistent, on-demand, weight-based routing protocol. The "weight" contained in the protocol messages used to choose stable routes which depends on three factors: Route Expiration Time (RET), which is the determined time of link failure among two nodes because of mobility, Error Count (EC), which catches the number of link breakage because of mobility, and Hop Count (HC). The authors have accepted that all nodes are moving in the same way and at the same time through a Global Positioning System (GPS), so that two neighboring nodes may determine the RET. Though the suggested scheme may fight against link failures because of mobility, link failures because of the less node energy is a component that also must be considered for when calculating weights for consistent routing. From the suggestions examined till now [8] it is clear that there is a requirement for a routing protocol that can give stability to the routes chosen for routing QoScapabledapplications, and also has process for fast re-routing to tackle indeterminable link failures. Moreover, the stability should come at minimum or no overhead for the system to be scalable. In what follows, we suggest enhancements to the AODV protocol that, give routes that are consistent for a session duration, with high probability, and that also contain a fast make-before- break process. In [10] QoS routing has recently got attention for giving QoS to wireless ad hoc networks and some work has been done to deal with this vital issue. Here, we give a short review of available work addressing the QoS routing effects in wireless ad hoc networks. Generally, QoS routing can be categorized into two basic types: hop-by-hop QoS routing and source QoS. In future, the term routing will relate to QoS routing if not specified. In source routing, the source node of a communication request locally calculates the whole constrained path to the aimed destination with the global state data that it locally holds. Collecting and holding global state information can insert unrestrained protocol overhead in dynamic networks and therefore have the scalability problem. Furthermore, the computation of constraint based routes would be computationally intensive for the computing nodes. The predictive location- based QoS routing protocol is mainly used to provide relief from the scalability problem in carrying out source routing with respect to communication overhead. Rather than broadcasting the status of every link network wide, every node broadcasts its node state (involving its velocity, current position, available resources and moving direction on each of its outgoing links) throughout the network at regular intervals of time or upon a substantial change. With this information, at any moment, each node can locally describe an instant perspective of the whole network. To hold a QoS request, the source node locally calculates a QoS fulfilled route (if available) and propagate data packets through the computed path. Furthermore, the source can determine route failure and predicatively calculate a new path before the old route failures by using the global state it holds. This routing protocol is appropriate or suitable for supplying soft QoS in small or medium-sized networks wherein mobile hosts are fitted with Global Positioning System (GPS) receivers and their moving behavior is determinable. The MANETs routing protocols may be generally categorized as on-demand driven protocols and table driven protocols. Table driven protocols require to hold the global routing information related to the network in each mobile

node for all the possible source-destination link and take to interchange routing information at the regular interval. This type of protocol has the characteristics of higher overload and lower latency.

III. WIRELESS BODY AREA NETWORK (WBAN)

The wireless body area networks (WBANs), are one of the low power sensor network [6], which provides efficient and reliable infrastructure for healthcare system including implanted, non-implanted and wearable sensor devices for human body. These sensor devices are used to capture various symptoms of a patient like heartbeat, body temperature, blood pressure, respiration and ECG etc. and send these symptoms to a Body Network Controller (BNC). BNC is an essential part of a WBAN which is capable to capture sensor data and after processing forwards to the centralized e-Health server. The eHealth server in turn saves this real time data from various patients that can be monitored by his clinician.

As shown in Figure 1, a BNC collects and processes data from the devices and forward it to a server using a wireless access network. The Wireless access network which is used in this scenario is IEEE 802.11ah. This standard is especially designed for IoT devices. There can be use of WLAN 802.11a/b/n standards but IEEE 802.11ah has some additional feature (like long range with low power consumption).

Figure 1. A typical WBAN in a smart healthcare system within the IoT network with its: things, network, and applications.

At other side e-Health server also use the public key algorithm for secure communication with remote users (sucah as, Doctors). Each user has its own private key and they will communicate with server by using a session key (session key is exchanged with the help of public key). By implementing this method confidentiality and security access of BNC and e-Health server can be achieved. The availability of system can be ensured by tracking the heartbeat of a patient, whereas the unavailability activates the emergency.

The main applications in wireless body area network (WBANs) is medial application where using in healthcare area. The example of this application illustrated in Figure 1. As shown in Figure 1, the plenty of sensor can be attached on body or may implemented under skin [6-8]. These sensor collect vital data from body where the patient is in different situation such as bed, running, working at office and so on [2, 9]. In addition, the safety domain is the other domain that we able to use WBAN to collect sensitive data and transfer collected data to the server for further services. As explained

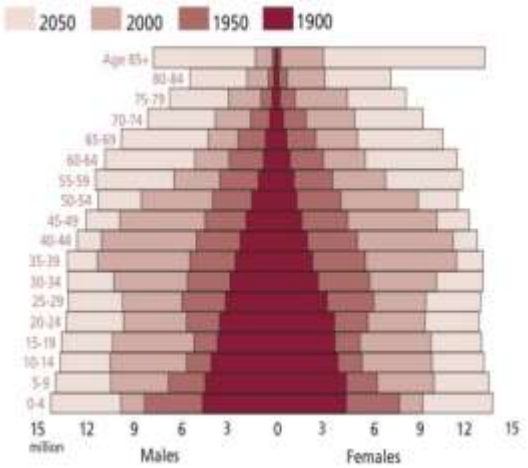

Figure 2: U.S. Age Pyramid [10]

in detail in [10], in the US the usage of healthcare service communications between and within WBANs in same and increase as shown in Figure 2. Different domain [11]. And finally is energy consumption

Type of device in WBANs

Sensor nodes: as we discussed earlier, there are plenty of sensor that used to collect vital data and then these data transfer to next node called PDA (Personal Digital Assistance).

Personal Digital Assistance (PDA): PDA or other exiting device such as smart phone aggregate medical data from body sensors and process it. The aggregated data will be transfer to next hop called base station.

Base Station (BS): there are plenty of device such as access point that working as a switch in the network. The data will be redirect from local place into cloud via the internet. As a result the medical data will be recorded in different server in cloud or any medical server in hospitals.

Number of node

The number of node using in WBANs is depends on some factors such as nature of network and the regulation of medical application.

Energy

Energy consumption is one main aspects in WBANs that must be consider before deployed it. The energy consumption must be consider in 3 way in WBAN. Firstly, energy consumption related to type of sensor using in WBANs. Secondly, energy consumption related to type of communications between and within WBANs in same and different domain [1]. And finally is energy consumption related to proceeding. There are several researcher focusing on type of sensors to reduce the energy consumption [10].

Usability

The other important issue in WBANs is usability that must be consider before deployed WBANs in small and big area. Regarding WBANs characteristics and plenty of device carry with which includes some variable sensors attached or implemented on/in body and also PDA that collected data from variable senor, we need to provide model to support them in small and large scale. Also, due to characteristics of WBANs, patent able to move from their place to another place or their domain to other domain very easy. As a result, there are plenty of interaction between their communications that need to consider before deployed WBANs. Figure 3 shown the position of WBAN.

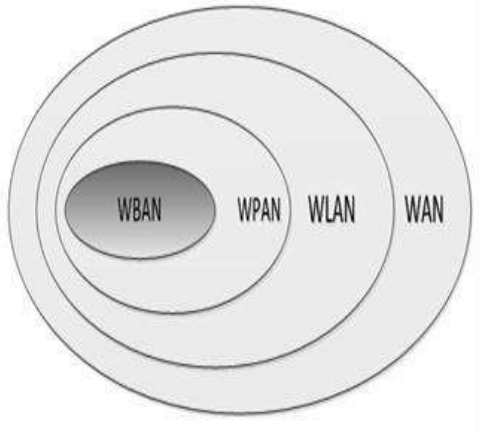

Figure 3: WBANs position

Security and Privacy

As we discussed earlier due to using plenty of devices such as variable sensors and PDAs and so on, the sensitive medical data will transfer over different type of wireless communication which possess several challenges in terms of security and privacy. Researchers need to consider the privacy in WBANs to protect the share data from untheorized users. And also, we need to provide some security mechanisms to secure communication between and within WBANs in same and different domain. There is a plenty of techniques proposed in terms of security and privacy in WBANs to address existing problem but we need to focus more to proposed efficient techniques to meet the requirements of WBANs as well [8]. Figure 4 shown the overall wireless communications between WVBAs and their service providers.

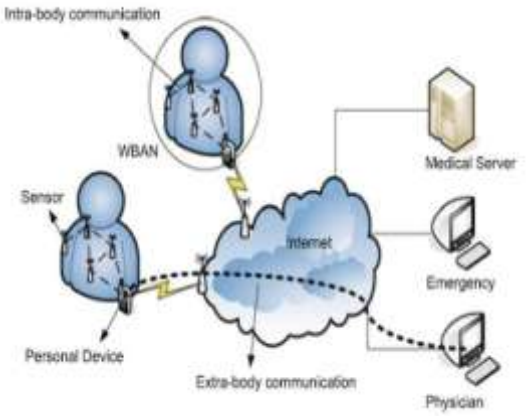

Figure 4: WBANs communication

IV. AODV ROUTING PROTOCOL

AODV [2] is an on-demand routing protocol that constructs routes only when needed. It uses sequence numbers to assure the originality of routes. To discover a route to a destination, a source node using AODV disseminates a route request (RREQ) packet based on constant Time to Live (TTL) value. The RREQ packets consists the current sequence number, node's IP address, broadcast ID and recent sequence number for the destination node which is known to the source node. The destination node on reception of RREQ, sends a unique route reply (RREP) packet with the reverse route constructed at the mediator nodes on the route discovery process. In situation of link breakage or invalid TTL value a route error packet (RERR) is delivered to the destination and source nodes. Because of use of sequence numbers, the source nodes are all time able to discover new valid routes.

V. PROPOSED METHODOLOGY

We are presenting the improved method for WBAN routing protocol with aim of improving energy efficiency of WBAN network as compared to existing routing protocols. Here we added the new energy efficient function in existing AODV routing protocol. Here we have taken two routing protocols under investigation such as AODV, DSR and the modified AODV routing protocol.

Following is the algorithm which is added to this AODV routing protocol for the improvement of energy and hence the other parameters. For a packet P, we use hc(P) and lvl(P) to represent the two additional fields of the packet, respectively. The algorithm needs to access other fields in a packet, such as the source, destination, sender and sequence number. Similarly, in the algorithm, they are represented by s(P), d(P), nid(P) and seq(P). We use s-d (P) to represent the source-destination pair of the flow that the packet belongs to. An "overhear table" is maintained at each node.

Algorithm: When node i overhears packet P,BEGIN

Step 1: Lookup s-d (P) in overhear table;

Step 2: IF no match, add entry e': s-d(e')=s-d(P), seq(e')=seq(P),ov-list(e') initialized with first entry <hc(P),lvl(P),nid(P)>. GOTO END;

Step 3: (Assume a match is found at entry e.) IF seq(P)<seq(e),ignore P. GOTO END;

Step 4: IF seq(P)>seq(e), update e as the following:seq(e)=seq(P), ovlist(e) reset as having only one entry <hc(P),lvl(P),nid(P)>. GOTO END;

Step 5: IF seq(P)==seq(e), do the following:

Step 5.1: Add entry <hc(P),lvl(P),nid(P)> into ovlist(e);

Step 5.2: IF ovlist(e) has three entries A, B, C satisfying thefollowing conditions, a better sub-path is found. 1)hc(C)==hc(B)+1==hc(A)+2;
2)lvl(node i)≥MAX(lvl(A),lvl(C));
3) (lvl(node i) -lvl(B))≥2. Activate this new subpath. Delete entry e from overhear table. GOTO END;

Step 5.3: IF ovlist(e) has two entries A and B, such thathc(B)==hc(A)+1 and lvl(node i) ≥ MAX(lvl(A),lvl(B)+2), add this indicator I in the WaitingIndicator list: candidate(I)=B, seq(I)=seq(e), s-d(I)=s-d(e). GOTO END;

Step 5.4: IF ovlist(e) has two entries B and C, such thathc(C)==hc(B)+1 and lvl(node i) ≤ MAX(lvl(B)+2,lvl(C)), node i broadcast one SHORT informing packet Q as follows: candidate(Q)=B, seq(Q)=seq(e) s-d(Q)=s-d(e); When node i receives a SHORT informing packet Q, BEGIN

1. Compare fields of Q with any valid entry in Waiting Indicator list;

IF there is no match, ignore packet Q; ELSE a better subpath is found

VI. CONCLUSION

Due to the limited resources of Body nodes in terms of computation, memory and battery power, secure and energy-save data aggregation methods should be designed in WBNs to reduce the energy cost of data collection, data processing anddata transmission. In this paper, we present an ID-based aggre-gate signature scheme for WBNs, which can compress many signatures generated by Body nodes into a short one, i.e., it can reduce the communication and storage cost. Moreover, we have proved that our IBAS scheme is secure in random oracle model based on the CDH assumption, and we also have proved that our aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid. In our future work, we will focus on designing more efficient data aggregation schemes.

REFERENCES

[1]. I. Paik, T. Tanaka, H. Ohashi and W. Chen, "Big Data Infrastructure for Active Situation Awareness on Social Network Services," Big Data (BigData Congress), 2013 IEEE International Congress on. IEEE, pp. 411-412, 2013.

[2]. E. Hargittai, "Is Bigger Always Better? Potential Biases of Big Data Derived from Social Network Sites," Annals of the American Academy of Political & Social Science, vol. 659, no. 1, pp. 63-76, 2015.

[3]. Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Sup-porting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.

[4]. I. Hashem, I. Yaqoob, N. Anuar, et al., "The rise of "big data" on cloud computing: Review and open research issues," Information Systems, vol. 47, no. 47, pp. 98-115, 2015.

[5]. H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou and X. Shen, "Enabling Fine grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, DOI10.1109/TDSC.2015.2406704, 2015.

[6]. H. Li, D. Liu, Y. Dai and T. Luan, "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP," IEEE WirelessCommunications, vol. 22, no. 4, pp. 74-80, 2015.

[7]. X. Liu, B. Qin, R. Deng, Y. Li, "An Efficient Privacy-Preserving Out-sourced Computation over Public Data," IEEE Transactions on Services Computing, 2015, doi: 10.1109/TSC.2015.2511008

[8]. X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving out-sourced calculation of rational numbers," IEEE Transactions on Depend-able and Secure

Computing,2016,doi:10.1109/TDSC.2016.2536601.

[9]. H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.8, pp. 2053-2064, 2014.

[10]. H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, "An Efficient Merkle Tree Based Authentication Scheme for Smart Grid," IEEE SYSTEMS Journal, vol. 8, no.2, pp. 655-663, 2014.

Simhadri lokesh "Performance Analysis Of An Improved Aodv Routing Protocol In Wireless Body Networks "International Journal of Engineering Research and Applications (IJERA) , vol. 8, no.11, 2018, pp 41-46