# Improved Audit-based malevolent Node Detection and Energy Efficiency for Healthcare Applications

**Deepa[1], M. Manju[1], Sathyaraj[1]**

*[1]Assistant Professor, RMK College of Engineering and Technology, Chennai, India*

## Abstract

Recently Wireless Body Area Sensor Networks (WBANs) are going more democratic and have revealed great possible in real time supervising of the human body. WBANs have involved a wide range of supervising applications for example sports activity, healthcare, and psychotherapy systems. However, WBANs contains more challenging issues should be resolved such as Quality of Service (QoS), energy efficiency and security and privacy issues are the most significant concerns. Because these systems manage life-critical data, they must be secure. To overcome the above issues, Improved Audit-based Malevolent Node Detection for Healthcare Applications is proposed. Audit-based malevolent Detection (AMD) is proposed for discovering and separating malevolent nodes in WBANs. The AMD system incorporates reputation management, trustworthy route discovery, and recognition of malevolent nodes based on behavioral audits. It integrates three critical functions: reputation management, route discovery, and identification of malevolent nodes via behavioral audits. An AMD can build paths consisting of highly entrusted nodes, subject to a desired path length constraint. In addition, the node fitness function is utilized for improving the energy efficiency in WBAN. The simulation result shows that AMD_EE successfully avoids malevolent nodes, even when a large portion of the network drops to forward packets and enhance the lifetime.

***Keywords:*** *Malevolent node detection, trustable routing, Reputation System, Energy Efficiency, Wireless Body Area Network.*

## Introduction

As wireless devices and sensors are growingly distributed on people, researchers have begun to focus on WBANs. The WBAN application areas are widely increasing day by day. Applications of WBAN contain sport activity, hobby, healthcare, and personal help, in which sensors gather data from people, physiological and their surrounds. WBAN system architecture has been shown in Figure 1. It contains sensors, actuators and control units. Wireless channels are used to communicate from sensor to user via internet.

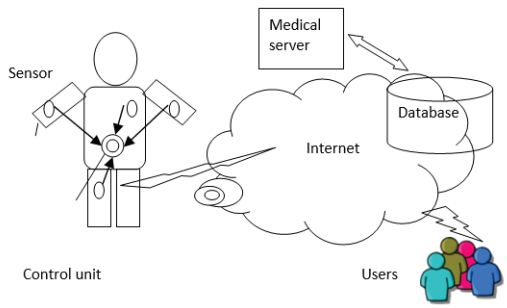


**Fig. 1: WBAN System Architecture**

The common benefits of WBAN health supervising systems for example unobtrusive, cost effective, and unobtrusive, they provide patients with continuous supervising of physiological signals that is useful particularly for the old peoples. WBAN enables patients to be supervised incessantly, and assisted rapidly by portable health teams while physiological signals illustrate that is required. Uninterrupted supervising of patients speeds up the patient retrieval progression, and minimizes death rate particularly in diabetic patients and cardiovascular.

Deficiency of security in WBANs may hamper the wide public acceptance of this technology, and more significantly can cause life-critical results and even death of patients. However, allowing for severe and scalable security system to prevent malevolent communications with WBANs is complex. Open wireless medium, makes the patient's information prostrate to being modified, eavesdropped, loss and injected. In addition, channel characteristics in WBANs such as very low Signal-to-Noise-Ratio situation and restriction of sensors in terms

of energy shortage, limited memory capacity, lacking computational and communication capability to create the opportunity of security attacks in WBANs. Hence, in WBANs, improving system performance and malevolent node detection is an important factor. Thus in this paper, Improved Audit-based malevolent Node Detection and Energy Efficiency is proposed.

The rest of this work is structured as follows. Section 2 presents a related work. In section 3 explains Improved Audit-based malevolent Node Detection and Energy Efficiency for Healthcare Applications. Section 4 discusses the simulation results and analysis. The final section is a conclusion.

**Related Work**

The WBAN is broadly predictable that a high stage privacy and system security meet a fundamental task in defending information while being utilized by the healthcare and during storage to make sure that patient's account are maintained secure from intruder's [1].The conventional security scheme that required inexhaustible resources, thus they cannot useful to the enormously resource restrained sensors. In addition, the WBAN security necessities like authentication, confidentiality, availability, data freshness, integrity, and non-repudiations. These are important security issues in healthcare applications in WBAN [2].Securing while Sampling in WBAN [3], rejects the requirement for a part encryption algorithm and the pre key distributed function thus it reduces the usage of sensor memory and other resources. This scheme provides a physical layer security. Also it isolates the eavesdropper present in the network.

Clique-Based WBAN Scheduling algorithm [4] is used to avoid interference. This scheduling method to schedule the sensors for working in a time slots manner. In this scheme, each node works by sleep or awake schedule during its own time slots thus extend the lifespan. Anonymous Authentication scheme [5] is used for reducing the computation burden of the client. This scheme provides the security against impersonation attack in WBAN.A Hybrid Key Management System (HKMS) [6] that introduced lightweight and scalable key management scheme for making resource-efficient WBAN. In this scheme, the one-way hash function builds a Merkle Tree for authentication purpose. This scheme addresses the compromised node also it reduces the network overhead. However, this scheme cannot handle the energy efficiency and QoS improvement in WBAN.

A secure cloud-based mobile healthcare system [7] is used to secure the among sensor communication by multi-biometric key design in WBANs. The e-medical reports are securely stored in the hospital society cloud and isolation of the patients' information is maintained. This scheme offers security resolution for omnipresent mobile healthcare applications.ECC with signature Hash Function scheme [8] is introduced for improving sensor authentication in WBAN. In this scheme, the hash-chain based key signature technique to secure information passing from sensor to user in WBAN. Also, Elliptical Curve Cryptography (ECC) algorithm is used to verifies the authenticate sensor. It extensively formulated to reduce the eavesdropping attack and get the patient information from the legitimate sensor. Secure Sensor Association and Key Management [9] is used to associate the sensor groups and offer a data integrity and confidentiality in WBAN. This scheme provides the data integrity by ECC algorithm. The authentication procedure and group key generation are very simple and efficient.

Revocable and Scalable Certificate less Remote Authentication Protocol [10] featured with client anonymity, key escrow resistance, non-repudiation, and revocability for WBANs. In this scheme, the certificate less encryption and a signature with proficient annulment against short-term key exposure, that considers independent interest. Also, a certificate less anonymous remote authentication with annulment is constructed by integrating the encryption scheme and signature scheme. This scheme is particularly suitable for the large-scale WBANs. However, this scheme creates complexity. Secure and efficient data communication protocol [11] is used to protect the information transmissions among sensors and the users by applying Ciphertext-Policy Attribute Based Encryption method. In this scheme, the sensor signature and patient information's are stored by the ciphertext format at user, thus assuring data security. However, this scheme increases the computational cost.

Improved Audit-based malevolent Node Detection and Energy Efficiency for Healthcare Applications

This AMD-EE provides a complete malevolent node isolation system for rejecting malevolent in WBAN. In this scheme, the AMD contains three phases such as a reputation module, a route discovery module,

and an audit module. Then isolate the malevolent nodes finally, the source transmit the data through the energy efficiency path without malevolent node in WBAN.

**Reputation Phase:**

In reputation module, the malevolent node is detected by direct trust and indirect trust. Here, every node direct trust is measured by reputation value. The node reputation value is calculated by the equation (1) given below.

$$RV_i^{\mathrm{j}}(\mathrm{t}) = \begin{cases} \beta * RV_i^{\mathrm{j}}(\mathrm{t}-1) \\ \min\{RV_i^{\mathrm{j}}(\mathrm{t}-1) + \beta, 1.0\} \end{cases} \quad (1)$$

Here, the trust factor $\beta$ is present between $0 < \beta < 1$, t represent the time, i represents the source node and j represent the behavior checking node. If the node has a reputation value is above threshold value that node is a good behavior node. A node with a reputation value is below threshold factor in many time that node is chances for acting malevolent node.

The indirect trust information is used while the direct trust information becomes stale, otherwise is not accessible owing to the deficiency of prior communication among two nodes. The indirect trust is computed based on reputation value is given below.

$$RV_i^{\mathrm{j}}(\mathrm{t}) = \frac{\sum_{k \in \tau_i} RV_k{}^{j}(\mathrm{t})}{|\tau_i(\mathrm{t})|} \quad (2)$$

The direct trust information is failed when the source i collect the opinion of node j from k neighbor nodes. Assume $\tau_i$ represents the neighbor nodes report the information about node j to source node i.

**Route Detection Phase:**

In route detection phase, the source finds out reliable routes from a source to a destination. The trustworthiness of a path based on the reputation value from source to destination is given below.

$$RV_{S \to D} = \sqrt[m+1]{\prod_{i=1}^{m} (\mathrm{RV_s}^{\mathrm{i}} * \mathrm{RV_D}^{\mathrm{i}} * \prod_{j=1, j \neq i}^{m} RV_i^j)} \quad (3)$$

Here, calculate the path reputation value by multiplying individual intermediate node reputation value. Suppose malevolent node present, the path reputation value is cannot increase superior than its own reputation. Then the isolates the accused node and verified it is a malevolent node or not in audit phase.

**Audit Phase:**

In this phase, the accused node is confirmed by malevolent or authenticated by using the Renyi-Ulam Games. This game engages two players such as a questioner and a responder. Here, the questioner is a source or destination and the responder is a routing nodes. The questions stated by the questioner represent to the audits executed by the source to nodes in the path from source to destination. While replying to an audit, nodes state the set of packets sends to the next hop.

The source aggregates more audits to make cut or membership questions. The responder dishonesty when a malevolent node lies with regard to the packets forward to the next hop. Such as, node dishonesty by either taking to forward all packets established when in actuality it falls them, or not forward the data packets. Then, the source confirms that node is a malevolent node and then send notification message to the network.

Finally, the source transmits the data through the energy efficiency path. The energy efficiency path is selected based on the highest residual energy, minimum distance and minimum hop count. Thus, avoids the frequently utilization of energy in the network.

**Simulation Analysis**

The simulation analysis is done using the Network Simulator (NS-2). The existing scheme HKMS and the proposed AMD-EE scheme are analysed and compared with the simulation results. The network traffic in the simulation prototype is handled using traffic model Constant Bit Rate (CBR).The parameters used for the simulation of the proposed scheme are tabulated below. The performance of the proposed scheme is evaluated by the metrics packet delivery rate, delay, packet loss rate and throughput.

**Packet Delivery Rate (PDR)**

PDR is defined as the rate of packets delivered to the destination node. PDR is calculated by the Equation 4.

$$PDR = \sum_{0}^{n} \frac{PacketsDelv}{Time} \quad (4)$$

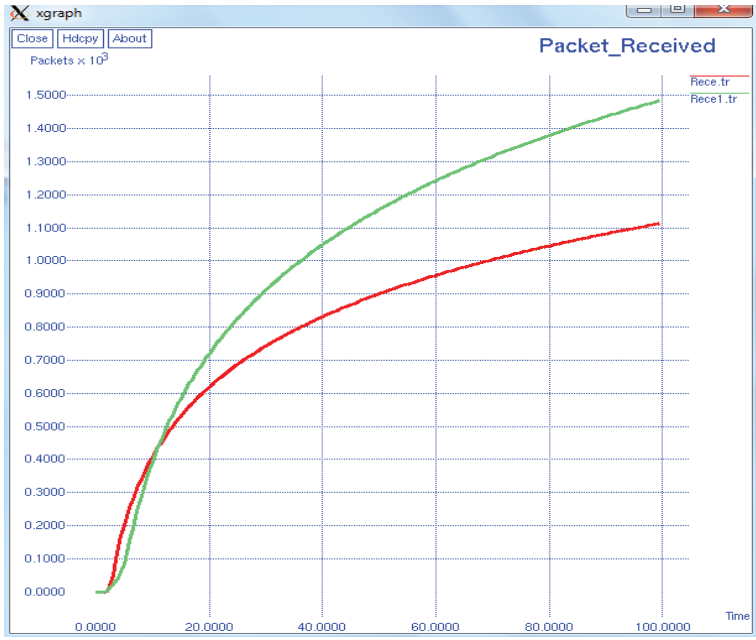


**Fig.2 Packet Delivery Rate**

Where n = number of nodes, green color line represents the AMD-EE mechanism and red color line represents the HKMS mechanism. The packet delivery rate of the proposed mechanism AMD-EE is higher than the packet delivery HKMS mechanism that is demonstrated in Figure 2. The more prominent estimation of packet delivery rate implies the better execution of the protocol.

**Packet Loss Rate (PLR)**

PLR is defined as the number of packets lost per unit time. PLR is measured by the Equation 5.

$$PLR = \sum_{0}^{n} \frac{PacketsLost}{Time} \qquad (5)$$

The packet loss rate of the proposed mechanism AMD-EE is lower than the HKMS mechanism that is explained in Figure 3. Lower the packet loss proportion demonstrates that higher execution of the network.


**Fig. 3 Packet Loss Rate**

**Average Delay**

Average Delay is defined as the time difference between the received and sent packets to the total number of nodes. It is measured by the Equation 6.

$$\text{Average Delay} = \frac{\sum_0^n \text{Pkt Recvd Time} - \text{Pkt Sent Time}}{n} \quad (6)$$

The delay value is low for the proposed scheme AMD-EE than the existing method HKMS is revealed in Figure 4. The base estimation of delay implies that higher estimation of the throughput of the system.


**Fig. 4: Average Delay**

Throughput

Throughput is defined as the average packets delivered to the destination successfully. The average throughput is estimated using Equation 7.

$$Throughput = \frac{\sum_0^n Pkts\ Received\ (n) * Pkt\ Size * 8}{1000} \quad (7)$$

The proposed scheme AMD-EE has higher average throughput when compared to the existing scheme HKMS is shown in Figure 5. It can be observed from the graph explains that the number of packets received successfully for every 1000 packets for AMD-EE is greater compared to that of the HKMS mechanism.


**Fig.5: Throughput**

## Conclusion

In this scheme, we have proposed Improved Audit-based malevolent Node Detection and Energy Efficiency for Healthcare Applications. Audit-based Misbehavior Detection technique for identifying and isolating malevolent nodes that drops to forward packets in WBANs. The AMD_EE system integrates reputation management, trustworthy and Energy Efficiency route discovery, and identification of misbehaving nodes based on behavioral audits. The simulation result shows that AMD successfully avoids malevolent nodes, even when a large portion of the network drops to forward packets. Also it detects the selective dropping attacks over end-to-end traffic streams in WBAN. The simulation results indicates that our scheme to improve both the energy efficiency and network performance in the WBAN.

**Ethical Clearance:** RMK College of Engineering and Technology

**Source of Funding:** Self

**Conflict of Interest:** NA

## References

1. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt Inform J. 2017; 18(2):113-122, 2017.
2. Kumar P, Lee HJ. Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors. 2012; 12(1): 55-91.
3. Dautov R, Tsouri, G R. Securing while sampling in wireless body area networks with application to electrocardiography. J biomedical & health inform, 2016; 20(1):135-142.
4. Xie Z, Huang G, He J, Zhang Y. A clique-based WBAN scheduling for mobile wireless body area networks. Procedia computer science, 2014; 31: 1092-1101.
5. He, D, Zeadally S, Kumar N, Lee, J H. Anonymous authentication for wireless body area networks with provable security. IEEE Syst J. 2017;11(4): 2590-2601.
6. Meharia P, Agrawal D P. A hybrid key management scheme for healthcare sensor networks. IEEE Int Conf on Commun. 2016; p. 1-6, 2016.

7. Khan FA, Ali A, Abbas H, Haldar, NAH. A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. Procedia Comp Science. 2014; 34: 511-517.
8. Devasena GS, Kanmani, S. Robust Security for Health Information by ECC with Signature Hash Function in WBAN. Indonesian J of Elect Engg and Comp Science, 2018;11(1): 256-262.
9. 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 of Commun and Net, 2015; 17(5): 453-462.
10. Xiong H, Qin, Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE trans on inform forensics & sec, 2015;10(7): 1442-1455.
11. Hu C, Li H, Huo Y, Xiang T, Liao X. Secure and efficient data communication protocol for wireless body area networks. IEEE Trans on Multi-Scale Comp Syst. 2016; 2(2): 94-107.