IMPROVED AUDIT-BASED MALEVOLENT NODE DETECTION AND ENERGY EFFICIENCY FOR HEALTHCARE APPLICATIONS

D. Deepa[1], M. Manju[2], MR. Sathyaraj[3]

[1,2,3]Assistant Professor, Department of Electronics and Communication Engineering,

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. Developing technologies quickly alteration the vital qualities of recent societies in terms of smart surroundings [1]. To exploit the contiguous situation data, small detecting devices as well as smart entries are extremely demanded. 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. The safety defenses as well as confidentiality of medical data are a disputing concern. 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. As a result, the users access the data without modifying or interrupting the malevolent nodes in the network. 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.

Index Terms—Malevolent node detection, trustable routing, Reputation System, Energy Efficiency, Wireless Body Area Network.

1 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 [10]. 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.

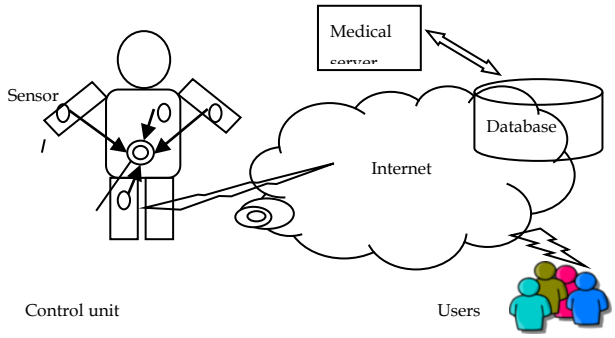


Figure. 1 WBAN System Architecture

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 [11].

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.

2 RELATED WORKS

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 [2].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 [3].Securing while Sampling in WBAN [4], 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 [5] 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 [6] 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) [7] 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 healthcare system [8] is used to protected the among node transaction via multi-biometric factor design in the networks. The e- checkup reports are steadily kept in the clinic society mist as well as isolation of the patients' information is maintained. This scheme offers security resolution for omnipresent mobile healthcare applications. Elliptic Curve Cryptography (ECC) with signature Hash Function scheme [9] is introduced for improving sensor authentication in WBAN. In this scheme, the hash-chain depend key sign algorithm to ensure information transaction. Also, this method is utilized for checking the authority. Association as well as Key Management [10] 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 authority process as well as group key creation is very basic and effective.

Revocable as well as Scalable Certificate less scheme [11] had node namelessness, identify escrow opposition, non-repudiation, as well as revocability. In this scheme, the certificate less encryption and a signature with proficient annulment against short-term key exposure, that considers independent interest. Also, this scheme is fabricated by integrating the encryption scheme and signature scheme. This scheme is particularly enhance the scalability. However, this scheme creates complexity. Secure data transaction scheme [12] is used to protect the information transmissions among sensors and the users with employing 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.

3 PROPOSED METHOD

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 phase, a route discovery phase, as well as an audit phase. Then isolate the malevolent nodes finally, the source transmit the data through the energy efficiency path without malevolent node in WBAN.

3.1 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 β 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 upstairs threshold factor which sensor node is a good behavior node. A node with a reputation value is lower threshold factor in many time that node is chances for acting malevolent node. The indirect trust information is used while the direct trust details gets sour, otherwise is does not accessible owing to the deficiency of earlier communication among 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 τ_i represents the neighbor nodes report the information about node j to source node i.

3.2 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.

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

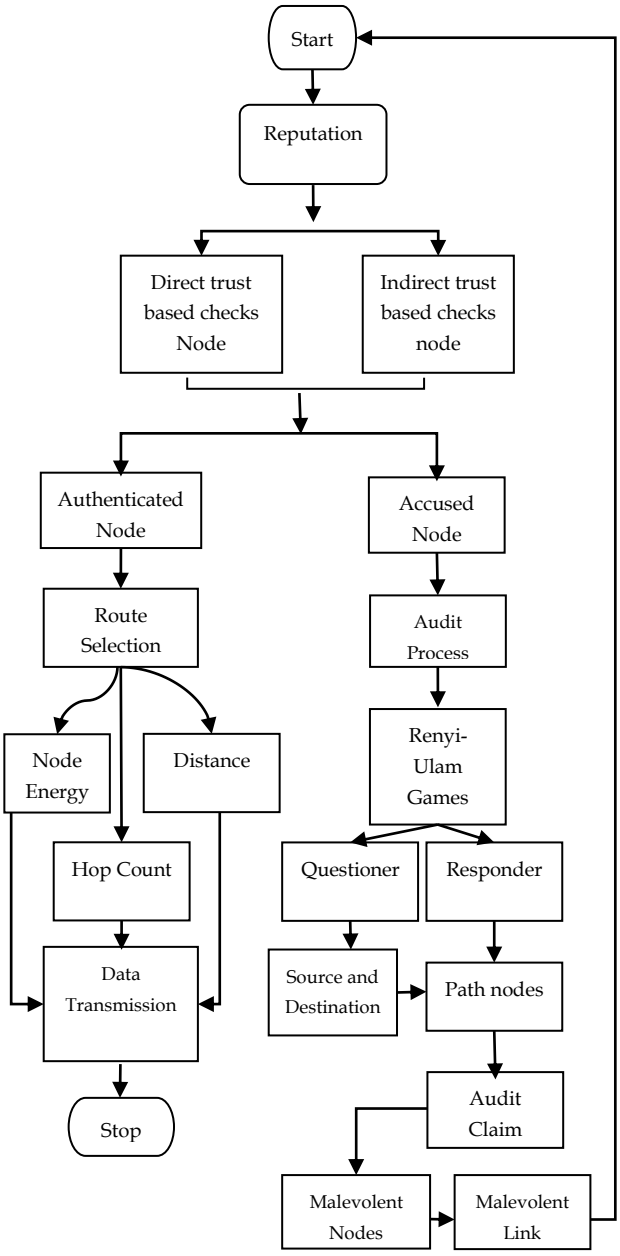
Here, calculate the path reputation value by multiplying individual intermediate sensor reputation value. Suppose malevolent node present, the path reputation value is cannot increase superior than its own reputation. Then the isolates the accused node and verified it is a malevolent node or not in
audit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

Figure.2 Flowchart of AMD-EE Scheme

3.2 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 enquirer and a responder. Here, the enquirer is a sender or destination and the responder is a routing nodes. The queries stated by the enquirer represent to the audits executed by the sender to nodes in the path from

sender to receiver. While replying for auditing, nodes condition the rest of packets transmits



to the adjacent hop.

The sender aggregates extra audits to make cut or membership queries. The responder dishonesty whiles a malevolent dishonesty by regard to the packets forward to the following hop. Such as, dishonesty by also taking to transmit entire packets established whiles in actuality not forward the data packets. Then, the sender confirms that node is a malevolent node and then send notification message to the network. The figure 2 illustrates the flow diagram of proposed scheme.

Finally, the sender 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.

4 RESULT AND DISCUSSION

The simulation examination is prepared via the Network Simulator. The conventional mechanism HKMS as well as the introduced AMD-EE mechanism are investigated as well as equated with the model outcomes. The table 1 illustrates the simulation parameters of AMD-EE mechanism.

Table 1. Simulation Parameters of AMD-EE Scheme

Parameter	Value
Nodes	50
Time	100 seconds
Channel Type	Wireless Channel
Packet Size	1024 bytes
Interface Queue Antenna	Priority Queue Omini Antenna
Radio Propagation	Two Ray Ground

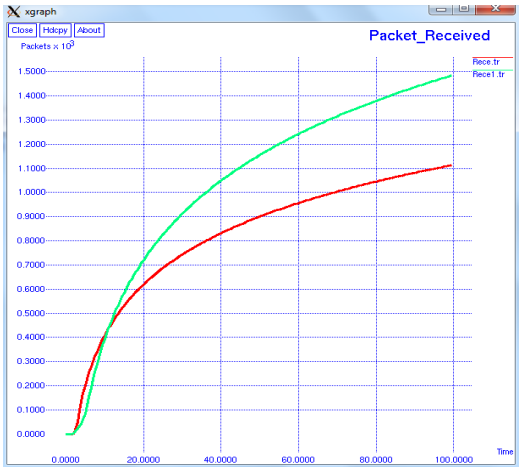
$$PDR = \sum_{0}^{n} \frac{PacketsDelv}{Time}$$

4.1 Packet Delivery Rate

It is defined as the rate of distributed packets to the destination node. It is computed by the expression 4.

(4)

Where n = number of nodes, green color line represents the AMD-EE mechanism and red color line represents the HKMS mechanism. The PDR of the introduced mechanism AMD-EE is higher than the packet delivery HKMS mechanism that is demonstrated in Figure 3. The highest protuberant evaluation of PDR involves the better execution of the protocol.



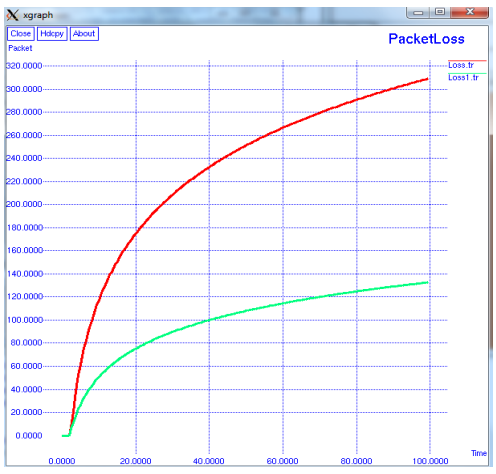


Figure.3 PDR of AMD-EE and HKMS mechanisms

Simulation Time (Sec)	PDR of HKMS (Packets)	AMD-EE (Packets)
0	0	0
20	6095	7088
40	8219	10523
60	9638	12480
80	10576	13891
100	11028	14962

4.2 Packet Loss Rate

PLR represents the loss of amount of data packets per unit time. PLR is restrained by the expression (5).

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

The table 3 illustrates the PLR value of HKMS as well as AMD-EE mechanisms.

Table 2.PLR of HKMS and AMD-EE Mechanisms

Simulation Time (sec)	PLR of HKMS (Packets)	PLR of AMD-EE (Packets)
0	0	0
20	179	75
40	233	100
60	265	118
80	292	124
100	310	137

From figure 4, the PLR of the introduced mechanism AMD-EE is inferior compare to the HKMS mechanism.

Figure.4 PLR of AMD-EE and HKMS mechanisms

Table

4.3 Average Delay

Average Delay represents the time variance among the received and sent data packets to the total number of nodes. It is evaluated by the expression 6.

$$\mathrm{AD} = \frac{\sum_{0}^{n} \text{Packet Obtained Time - Packet Forwarded Time}}{n}$$

(6)

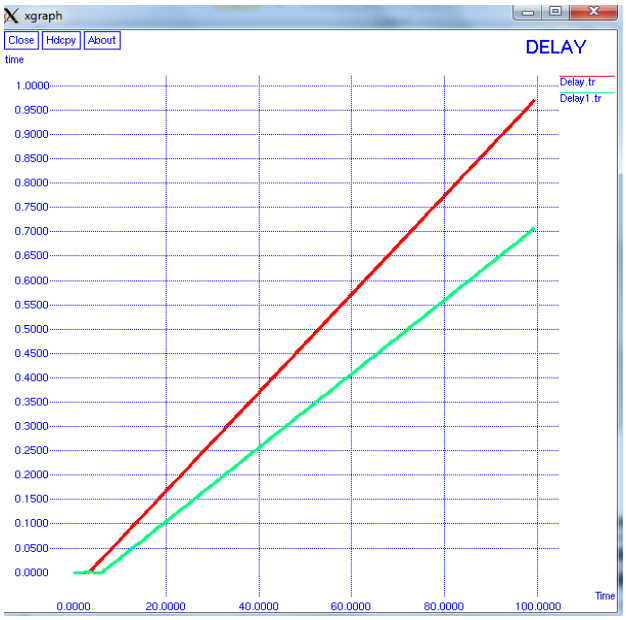


Figure.5 AD of AMD-EE and HKMS mechanism

Table 4.AD of HKMS and AMD-EE Mechanisms

Simulation Time (Sec)	AD of HKMS (Packets)	AD of AMD-EE (Packets)
0	0	0
20	0.165	0.102
40	0.750	0.253
60	0.575	0.412
80	0.772	0.564
100	0.978	0.716

The AD value is small for the AMD-EE compared to the HKMS is revealed in Figure 5. The table 4 illustrates the AD value of HKMS as well as AMD-EE mechanisms.

4.4 Throughput

Throughput is defined as the average packets distributed to the receiver successfully. The throughput is evaluated by expression 7.

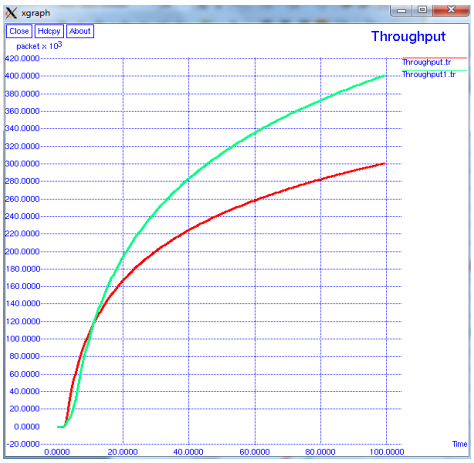
$$Throughput = \frac{\sum_0^n Packets\ Received\ (n) * Packet\ Size * 8}{1000} \quad (7)$$

Table 5. Throughput of HKMS and AMD-EE Mechanisms

Simulation	Throughpu	Throughpu

Time (Sec)	t of HKMS (Packets)	t of AMD-EE (Packets)
0	0	0
20	163120	195412
40	223805	281326
60	260311	337437
80	283227	375181
100	302214	403624

Figure.6 Throughput of AMD-EE and HKMS mechanisms



The table 5 illustrates the throughput value of HKMS as well as AMD-EE mechanisms. The AMD-EE mechanism has better throughput than the HKMS mechanism is illustrated in Figure 6.

5 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 recognizing as well as separating malevolent sensor nodes which drops to transmitted packets in WBANs. The AMD_EE mechanism incorporates reputation management, Energy Efficiency route detection, trustworthy as well as recognition of malevolent sensor nodes by the behavior audits. Thus it effectively evades malevolent nodes. Also it detects the discriminating falling attacks in the WBAN. Thus the user accesses the reliable data from the authenticated sensor in the WBAN. The simulation results indicate that our scheme to progress both the better throughput efficiency as well as minimizes the packet losses in the network performance in the WBAN.

REFERENCES

[1] Z. Habib, M. Asif, M. Ahmad, S. Jabbar, S.Khalid, J.Chaudhry, K. Saleem, J.Rodrigues,

and M.S Khalil. “Security and privacy based access control model for internet of connected vehicles”, Future Generation Computer Systems,2019.

[2] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, S. Shamshirband, S, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications”, Egyptian Informatics Journal, vol. 18, no. 2, pp.113-122, 2017.

[3] P. Kumar, H.J Lee, “Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors”, vol. 12, no. 1, pp.55-91, 2012.

[4] R. Dautov, G. R., Tsouri, “Securing while sampling in wireless body area networks with application to electrocardiography”, IEEE journal of biomedical and health informatics, vol. 20, no. 1, pp.135-142,2016.

[5] Z. Xie, G.Huang, J. He, Y. Zhang, “A clique-based WBAN scheduling for mobile wireless body area networks”, Procedia computer science, vol. 31, pp.1092-1101, 2014.

[6] D. He, S. Zeadally, N. Kumar, J.H. Lee, “Anonymous authentication for wireless body area networks with provable security”, IEEE Systems Journal, vol. 11, no.4, pp.2590-2601, 2017.

[7] P. Meharia, D.P. Agrawal, “A hybrid key management scheme for healthcare sensor networks”, IEEE International Conference on Communications, pp. 1-6, 2016.

[8] F. Khan, A. Ali, H. Abbas, N.A.H. Haldar, “A cloud-based healthcare framework for security and patients’ data privacy using wireless body area networks”, Procedia Computer Science, Vol. 34, pp. 511-517, 2014.

[9] G.S. Devasena, S. Kanmani, “Robust Security for Health Information by ECC with Signature Hash Function in WBAN”, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 11, No. 1, pp. 256-262,2018.

[10] J. Shen, H.Tan, S. Moh, I. Chung, Q. Liu, X. Sun, “Enhanced secure sensor association and key management in wireless body area networks. Journal of Communications and Networks”, Vol. 17, No. 5, pp.453-462, 2015.

[11] H. Xiong, Z. Qin, “Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks”, IEEE transactions on information forensics and security, vol. 10, No. 7, pp. 1442-1455, 2015.

[12] C. Hu, H., Li, Y. Huo, T. Xiang, X. Liao, “Secure and efficient data communication protocol for wireless body area networks. IEEE Transactions on Multi-Scale Computing Systems, Vol. 2, No. 2, pp. 94-107, 2016.