Int. J. Open Problems Compt. Math., Vol. 16, No. 4, December 2023
Print ISSN: 1998-6262, Online ISSN: 2079-0376;

Internet of things in diabetes healthcare:

Network Transmissions security

Leenah Aljuhani

College of Computer Science and Information Technology King Faisal University, Saudi Arabia
e-mail: leenanj22@gmail.com

Received 1 November 2023; Accepted 28 December 2023

Abstract

This research paper explores the multifaceted nature of diabetes, encompassing a spectrum of disorders characterized by disruptions in insulin, a hormone crucial for facilitating the absorption of blood sugar by the body. Dysregulation in insulin production can elevate blood sugar levels, thereby precipitating various diseases and complications, some of which may prove fatal. The present study advocates the integration of technology in healthcare as a means to aid medical professionals in classifying diabetes and monitoring ketone levels in the blood. A crucial facet of this endeavor involves the establishment of a robust platform for self-management of diabetes, aiming to regulate glucose levels, blood pressure, and the requisite insulin levels essential for the overall functioning of the human body. Leveraging medical sensors based on the Internet of Things (IoT) is proposed to be a transformative approach, promising to streamline costs and enhance the user experience within the medical domain. This research paper delves into the potential implications and benefits of incorporating advanced technology in the management of diabetes, presenting a comprehensive analysis of its impact on healthcare practices and patient outcomes.

Keywords: *Sybil attack, Wireless Sensor Network, svm Attacks in WSN, Malicious nodes, Machine learning in WSN.*

1 Introduction

The integration of Wireless Sensor Networks (WSN) in the context of diabetes transmission data within the Internet of Things (IoT) has revolutionized healthcare monitoring [1] [2]. In this innovative paradigm, miniature sensors embedded in wearable devices continuously gather and transmit crucial data related to a diabetic patient's health. These sensors can monitor blood glucose levels, heart rate, and other relevant physiological parameters in real-time. The WSN enables seamless

communication between these sensors and a centralized IoT platform, facilitating the swift and secure transmission of data. This interconnected system empowers healthcare professionals with timely and accurate information, allowing for proactive management of diabetes. The dynamic nature of the WSN-IoT ecosystem not only enhances the monitoring process but also promotes personalized healthcare interventions. As a result, individuals with diabetes experience improved quality of life, as the system enables early detection of anomalies and timely adjustments to treatment plans, ultimately contributing to more effective disease management. [3]

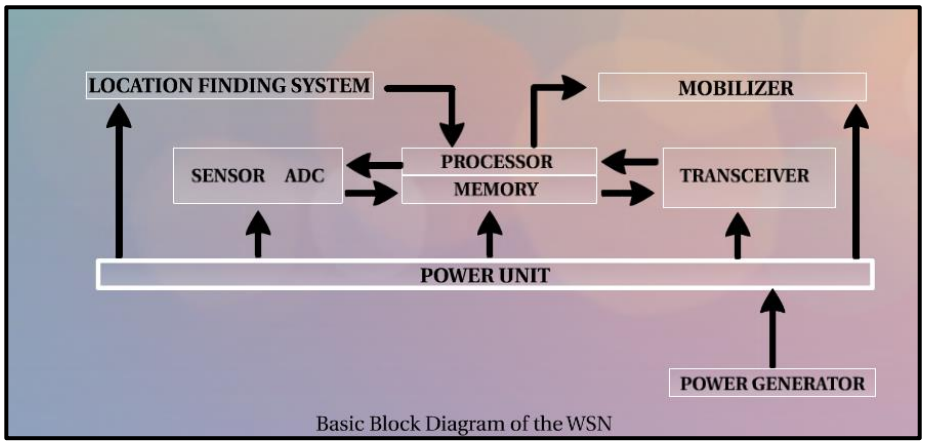


Figure 1: WSN

This paper addresses the imperative need for heightened security in the context of Wireless Sensor Networks (WSN), [4] [5]. particularly concerning the transmission of diabetes-related data. WSNs, consisting of a multitude of sensors interconnected through wireless links, play a pivotal role in various applications. Given the expansive scale of WSNs and their connectivity, it becomes crucial to implement effective methods to detect and thwart attacks by undesirable users. The transmission of data in a WSN typically initiates from the source and culminates at the base station, with the primary objective of constructing WSNs being the reduction of power consumption and the extension of network lifetime [3]. This research endeavors to explore and propose enhanced security measures tailored to the unique challenges presented by the transmission of diabetes data within WSNs,

aiming to contribute to the broader discourse on securing information in contemporary communication networks.

Figure 2: Diabetes monitoring sensors

2 Problem Statement

The network layer plays a pivotal role in the overall security of networks, making it susceptible to various types of security threats. Sensor networks, in particular, face a range of attacks in their routing processes, including but not limited to spoofing, selective forwarding, sinkhole attacks, Sybil attacks, wormhole attacks, node replication attacks, flooding, and privacy breaches. Wireless communication among sensor nodes in Wireless Sensor Networks (WSNs) is vulnerable to adversarial actions, such as eavesdropping, compromising nodes, packet interruption or modification, and injection of malicious packets, all of which compromise privacy and pose serious threats to WSN security. Consequently, attackers often compromise internal sensor nodes to launch attacks, making their detection a challenging task.

3 Wireless sensor networks (WSN)

Wireless Sensor Networks (WSN) [8] is a set of sensors that are used to monitor a specific physical or chemical phenomenon (such as heat, humidity, vibration, light, etc.), and then transmit information about the phenomenon wirelessly to the data processing center. These processes are carried out without the need for the presence of human in the place of physical phenomenon.

4 Literature Review

Because digital data are the most common use way to share information between nodes in WSN, in most times, contain private information. Many researchers in security field exerting much more efforts to innovate new non-traditional techniques to achieve strong protection for these Network from any attacks. Many studies and research were presented in the field of attack detections techniques. In addition, different systems of attack detections techniques were proposed. There

are various techniques which are proposed from time to time to detect and protect WSN from Sybil attack for more secure.

The [9] evaluates node trust value by the node behavior effect on network security. It presents behavior parameters and joint cognition model for 9 types of common node behaviors to set a correct trust value. The results show that in a static and dynamic network environment it reaches a high grading accuracy which can exclude malicious node from network activity effectively.

In [10] new algorithm introduced called CRSD, it proposed a static node in WSN that take (RSSI) distance between two nodes, in this proposed paper the distance between node is previous known because all nodes distance saves and the Sybil attack detected when two or more nodes have the same position or the distance between node are different. The above proposal detects the Sybil attack by applying the following equation

$$[\![RSS]\!]\_(S-D) = C\_e^{*}[\![d(S,D)]\!]\hat{}(-b)^{*}[\![RSS]\!]\_S.$$

Where RSSs: is the transmitted signal strength at S.

$$[\![RSS]\!]\_(S-D),$$

is the received signal strength at D.

$$C\_e,$$

is an independent variable reflecting the impact of environment.

$$d(S,D),$$

is distance between node S and node D.

The paper [11] proposed a technique to detect a Sybil attack on vehicles. It works into two steps the first step when the node created it produce authentication by the other node if it done the second step is start by allow identification to vehicles and RSU gathering information from neighbor's node and calculate speed threshold, the Sybil attack detect if the different threshold found.

In [12] proposed a technique to detect a Sybil attack by build a lightweight trust system using energy as a metric parameter for a hierarchical WSN. The above proposal management by CH which include each information of nodes such as (ID, position, Energy), when node send data to CH with it information the CH check the

sender information (ID, Position) and compare if it right, the second check is calculate the trust path as the following equations:

$$E = E\_t + \beta,$$

where

E: is the energy value saved in the matrix of the CH.

E_t : is the energy value in the message sent to the CH.

β: is rate of energy variation.

And Trust is calculated as the following equation which is used in [13].

$$T(\Delta t) = \left\lceil \left((10 \times S(\Delta t)/S(\Delta t) + U(\Delta t))(1/U(\Delta t)) \right) \right\rceil.$$

Where the timing window (Δt) used to count the successful and unsuccessful interactions of nodes based on the result of previous equation.

In [16] the author propose technique that calculate the Trust connection based on neighbor's nodes and Bayes rules. this technique calculate utility of each node and determined if node can have trusted or not, each node can monitor neighbors and collect information from the neighbors then decide to trust neighbors and sends packet or not. Furthermore, if we consider most nodes are malicious, we cannot send messages to them and transmission will consume more time.

In [14] in a Sybil attack, an attacker generates multiple identities for single node, these identities found to achieve more benefits or drop the network.

In [15] the author illustrates a strong solution that facilitate detection of all cyber-attack cases. They utilize lightweight to resolve attack in the sense that meanwhile the collaboration between receiver and the other node. Their demonstration via an experiments despite RSSI is time-varying and unreliable in general and a non-isotropic radio transmission. Utilize RSSIs ratio from multiple receivers. To accomplish lightweight solution, initially indicate that dismiss to figure out sender's location. So easy to computation requirement's by evading calculation of fading via distance. In addition, they demonstrate via experiments that even for a 3-D coordinate system, for Sybil node detection, pair node is enough more than using two pairs of receiver nodes that is required in the theory. They find out that it is likely in practice by using a pair of receiver's high accuracy completeness and less than a few percent false positive rate is possible in practice.

The current methods consume a lot of energy to detect intrusion and the progress of technology has become necessary to find new methods to solve the problems of the previous in terms of large power consumption, accuracy of intrusion detection

and delay in sending packets, so it was necessary to propose and use new features to detect this type of attacks as it is explained in our algorithm.

5 Proposed Technique

Security issues in wireless sensor networks are critical. Therefore, components that are designed without security can easily become an area for attack. In recent years, the security of WSNs has become increasingly concerning. A sensor node has limited communication and computational resources. It has a short radio range, and simply compromised by an attacker. In a Sybil attack, malicious nodes may assume many identities in (WSNs). However, it can be detected by using our method.

In this paper, we apply and implementation an algorithm for detecting Sybil attacks in wireless sensor network. Creation of Sybil attack through use of the other personal identities is well known. Most of the existing research deals with the detection of the Sybil attack through verification of identities.

The goal of our method is to detect the malicious node, and extend the network lifetime. The hybrid method, on the other hand, have the advantage of increased detection accuracy, low false alarm rates and also if the cluster head gets compromised or the base station gets surrounded by the malicious nodes, the other sensor nodes within the network can still detect the attack and delete the malicious node. We assume that once the network initializes, the adversaries are not attack the network for the first period.

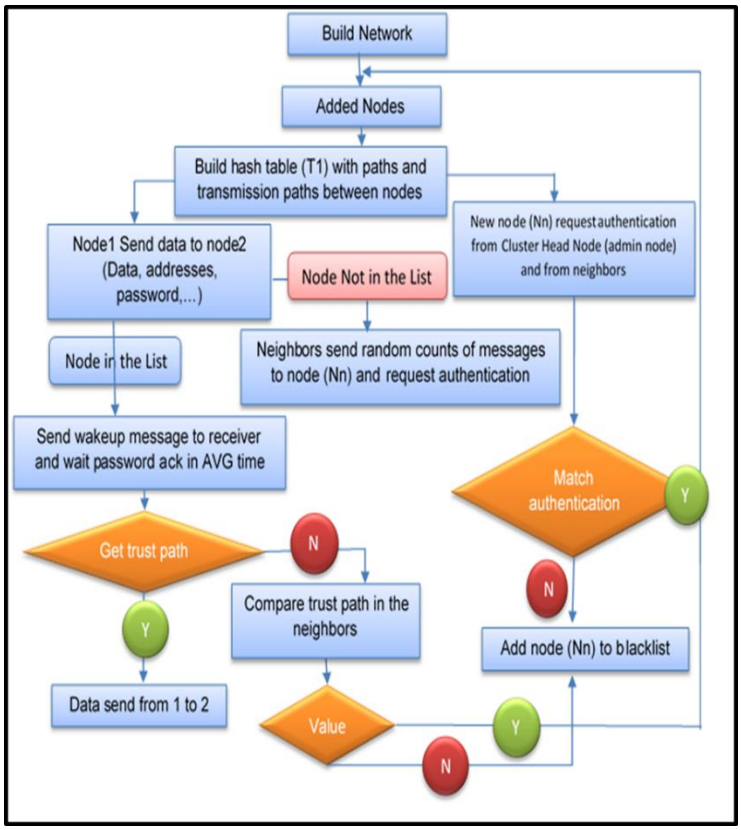


Figure 3: Diagram of the proposed algorithm

6 Classification using SVM

in the classifier phase, the system calls support vector machine classifier to compare between training date (that describe in case one) and the result of the tested node (the checked node).

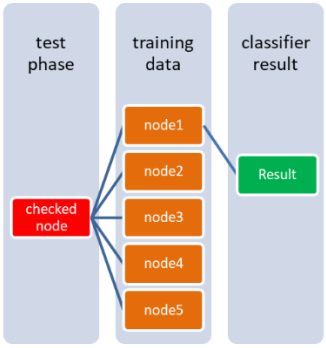


Figure 4: Classification

Finally, we can make some desition about this case

1- Any nodes have same ID and position its identified as Sybil node.
2- Different authentication matching from sender and receiver it identified as Sybil node.
3- More power consuming its identified as Sybil node.
4- More time its maybe identified as Sybil node.

7 Conclusion

In our simulation scenario, we use 50 nodes. we divided into 70% nodes as trusted or legitimate and 30% nodes as malicious. The nodes are placed randomly in the area of 200 * 200 m2 using MATLAB simulation. we run the simulation with the initial parameters

we used PC with core i7 processor, 8 G RAM, 1G VGA, and work under Windows 10 operating system.

We use multi-factors for our testing (power consuming, time, and RSSI). the tests classify each factor separately, then combined these factors and classify them result and compare the result between single factor with the combined factors.

TIME:

Table 1: Time Result for 50 nodes

Tests	Run Time	NO. Sybil	NO. Trust	Accurecy %
Test one	1103.941	13	37	86.66%
Test Two	991.64	13	37	86.66%
Test Three	1097.778	13	37	86.66%
Average	1064.453	13	37	86.66%

In the above table, we show the three-time tests the column "run-time" display the time used for each test, the second column displays the number of Sybil attack detected, third column display number of the legitimate node, and the last column displays the accuracy of the test.

Power Consuming:

Table 2: Power consuming result

Tests	NO. Sybil	NO. Trust	Accurecy %
Test one	10	40	66.66%
Test Two	11	39	73.33%
Test Three	11	39	73.33%
Average	10.66	29.64	71.06%

RSSI:

Table 3: RSSI Result

Tests	**NO. Sybil**	**NO. Trust**	**Accurecy %**
Test one	**9**	**41**	**60%**
Test Two	**7**	**43**	**46.66%**
Test Three	**8**	**42**	**53.33%**
Average	**8**	**42**	**53.33%**

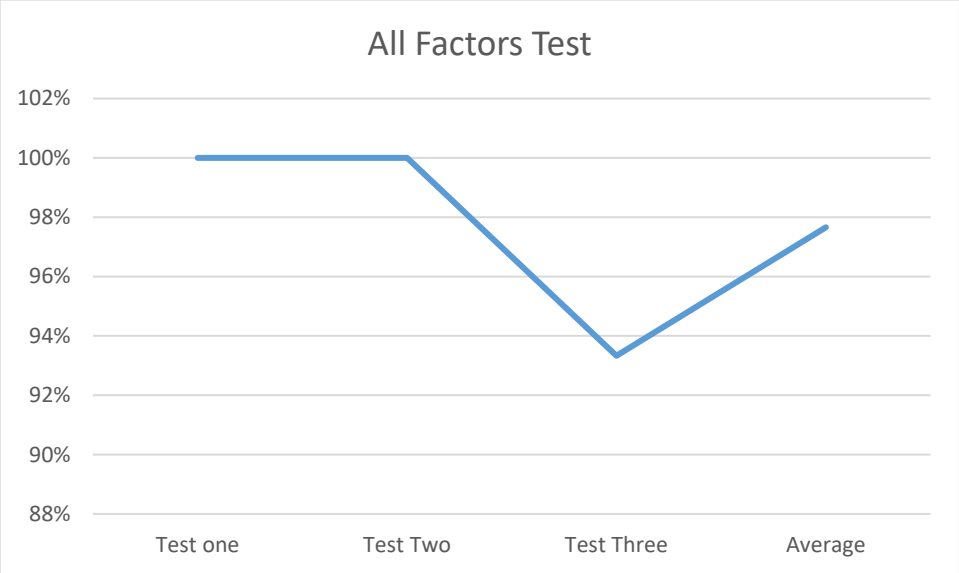
All Factors:

Table 4: All Factors Result

Tests	**NO. Sybil**	**NO. Trust**	**Accurecy %**
Test one	15	35	100%
Test Two	15	35	100%
Test Three	14	36	93.33%
Average	14.66	35.34	97.66%

The above table shows that the feature integration process improves the process of detecting the Sybil attack

Figure 5: All factors result



8 Open Problem

Wireless Sensor Networks (WSNs) are vulnerable to security threats and developing effective Intrusion Detection and Prevention Systems (IDPS) tailored for WSNs is crucial. Traditional IDPS may not be suitable for WSNs due to resource limitations. Challenges include developing lightweight and energy efficient IDPS algorithms, adapting to dynamic network conditions, addressing privacy breaches, and ensuring real-time response and mitigation. Solving these challenges would enhance the security and reliability of WSNs for critical applications like healthcare monitoring and infrastructure monitoring.

References

[1] Leenah Aljuhani, Alaa Sagheer, Enhancement the Susceptibility of Developing Diabetes Treatment by Time Series Data Analysis, International Journal of Advances in Soft Computing and its Application, 15, 2(2023), 194-206. doi: 10.15849/IJASCA.230720.13.

[2] M. S. Farooq, „Role of Internet of things in diabetes healthcare: Network infrastructure, taxonomy, challenges, and security model,“ Open Access, sv. 9, pp. 1-12, 2023.

[3] G. H. F. W. L. S. a. M. G. Jinfang Jiang, "An Efficient Distributed Trust Model for Wireless Sensor Networks," LATEX, 2015.

[4] Y. Y. a. L. A. O. R. Muraleedharan, "Detecting sybil attacks in image senor network using cognitive intelligence,," in Proceedings of the First ACM workshop on Sensor and actor networks, pp. 59-60, 2007.

[5] J. R. Douceur, "The sybil attack," in Peer-to-peer Systems, ed: Springer, pp. 251-260, 2002.

[6] P. M. K. Rakesh Maharana, "An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC," International Journal of Computer Applications, p. 0975 – 8887 Volume 67– No.22, April 2013.

[7] J. R. Binod Vaidya, "Improved robust user authentication scheme for wireless sensor networks," Wireless Communication and Sensor Networks (WCSN), 2009, anuary 2010.

[8] R. Soltani, B. Bash, D. Goeckel and D. Guha Towsley, ""Covert single-hop communication in a wireless network with distributed artificial noise generation". 2014 52nd Annual Allerton Conference on Communication, Control, and Computing," p. 1078–1085. doi:10.1109/ALLERTON.2014.7028575., 2014.

[9] W. Z. K. et.al, "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks," Computer Network and Information Security, pp. 1-10, 2011.

[10] A. S. a. A. Chandrakasan, "Dynamic Power Management in Wireless Sensor Networks," IEEE Design & Test of Computers, 2001.

[11] "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006.

[12] F. &. D. J. Li Zhou, "A lightweight and dependable trust system for clustered wireless sensor networks.Information Forensics and Security," IEEE Transactions, pp. 924-935, 2013.

[13] "A Trust Structure for Detection of Sybil Attacks in Opportunistic Networks," The 11th International Conference for Internet Technology and Secured Transaction, 2016.

[14] X. Z. F. N.-A. a. A. K. Heping Wang, "Cross-Layer Optimized MAC to Support Multihop QoS Routing for Wireless Sensor Networks," IEEE Transactions on Vehicular Technology, 2010.

[15] "Improved robust user authentication scheme for wireless sensor networks," Conference Paper January IEEE, 2010.

[16] S. Samonas and D. Coss, ""The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security," Journal of Information System Security, p. 21–45., 2014.

[17] J. P. Umashankar Ghugar, "A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol," International Journal of Computer Science and Network, vol. 5, no. 4, pp. 2277-5420, 2016.

[18] M. a. S. Y. Demirbas, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," International Symposium on on World of Wireless, Mobile and Multimedia Networks, Washington DC, USA, IEEE Computer Society, p. 564–570, 2006.

[19] Y. Y. Zhiling Tu, "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," CSF Analysis on Effective Information Security Management, vol. 12, no. 1, pp. 1-13, 2014.

[20] J. Behavior, "Detection in Wireless Sensing Networks," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2016.

[21] M. Kuching, "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks," IEEE 12th Malaysia International Conference on Communications (MICC), pp. 23-25, 2015.

[22] C. M. ,. L. M. Li Wei, "Information Security Routing Protocol in the WSN," 2009 Fifth International Conference on Information Assurance and Security IEEE, pp. 978-0-7695-3744-3, 2009.

[23] H. S. a. M. Feham, "International Journal of Network Security & Its Applications (IJNSA)," IJNSA), pp. Vol.3, No.4,, 2011.

[24] K. S. B. Abirami, "Sybil attack in wireless sensor network," International Journal of Engineering and Technology,, pp. 5 (2), pp. 620-623., 2013.

[25] "Sybil Attacks and Their Defenses in the Internet of Things," IEEE INTERNET OF THINGS JOURNAL, 2014.

[26] G. D. a. others, "TDOA-Based and RSSI-Based Underground Wireless Positioning Methods and Performance Analysis," International Journal of Future Generation Communication and Networking, 2015.

[27] E. S. D. S. a. A. P. J. Newsome, "The sybil attack in sensor networks: analysis & defenses," in Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268, 2004.

[28] H. C. Y. K. W. S. S. Z. &. C. C. H. J. Hu, "Weighted trust evaluation-based malicious node detection for wireless sensor networks.," International Journal of Information and ComputerSecurity,, pp. , 3(2), 132-149., 2009.

[29] K. A. C. K. Muni Venkateswarlu Kumaramangalam, „Zone-Based Routing Protocol for Wireless Sensor Networks," International Scholarly Research Notices, pp. 1-4, 2014.