A Cluster Based Energy Efficient Trust Management Mechanism for Medical Wireless Sensor Networks (MWSNs)

Syed Asad Hussain
Department of Computer Science
COMSATS Institute of Information Technology,
Lahore, Pakistan
e-mail: asadhussain@ciitlahore.edu.pk

Imran Raza
Department of Computer Science
COMSATS Institute of Information Technology,
Lahore, Pakistan
e-mail: iraza@ciitlahore.edu.pk

Muhammad Mohsin Mehdi
Department of Computer Science
COMSATS Institute of Information Technology,
Lahore, Pakistan
e-mail: mohsin.mehdi@ciitlahore.edu.pk

***Abstract*—This paper presents an energy efficient trust management model for securing life-saving information with optimal power/energy consumption by sensor nodes. The proposed model is a cluster based three tier-architecture where first tier records the first-run configuration of the nodes. The second tier secures the data between the nodes, and the third tier ensures energy efficiency by calculating energy consumption at every level and rotates cluster head among the nodes. The difficult task of energy efficiency is achieved through a robust algorithm, which configures the nodes and train the network using a machine learning technique. The simulation results show smooth functioning of the network with less energy consumption. The proposed scheme performs better than Anonymous Authentication for Wireless Body Area Networks with Provable Security (AAWBAN) in terms of computational overhead, energy consumption, throughput and data drop rate.**

Keywords-trust management system; medical wireless sensor networks; security; energy efficiency

I. INTRODUCTION

Diverse characteristics of Medical Wireless Sensor Networks (MWSNs) facilitate remote monitoring of patients in healthcare applications. A brief exploration of several health care projects (AlarmNet, MobiCare, MediSN, UbiMone) reveals that provision and maintenance of reliable security against several attacks is a major requirement for providing immediate treatment to the patients. An integration of health care service systems with the cloud computing architecture employs physiological sensing devices that are capable of continuous monitoring and raising alarm for emergency situations. Such a successful operation is guaranteed only when all nodes function in a trustworthy manner. Trust among the nodes ensures robustness, reliability, and verification. Several trust management mechanisms have been proposed for healthcare systems [1-5]. Trust in WSNs is assessed periodically based on the number of failed and successful communication attempts by a certain node in specific interval of time [6–8]. The issue with this recursive method of trust estimation technique is that it emphases more on recent state of the node and does not consider any previous failed communication attempts. Consequently, a malicious node can simply eliminate any bad reputation by using some verified successful communications and the later continue to attack. For example, in an on-off attack, the malicious node changes its behaviour from good to bad and from bad to good rendering itself undetectable during the attack [8]. Detection of such a state is important to avoid wastage of resources if more nodes behave like this. The performance and security of a WSN depend on cooperation and trust assurance of nodes.

Some of the major issues in calculating trust in sensor networks are extreme computations and energy efficiency. The sensor trust model and ambient trust sensor routing in [1] use complex Gaussian distribution and location-based routing protocol which incur computational overhead and more battery consumption. A routing protocol requires more communication resources to decide the best route. Addition encouragement and multiplication punishment (AEMP) [2] routing protocol and direct trust dependent link state routing protocol [3] are examples of resource intensive trust-based routing protocols. Policy maker, Keynote, SPKI/SDSI, Role Based Access control (RBAC) are based on role-based trust management language [4]. They specify policies over the nodes, delegating their roles to other nodes when location alters. They identify delegation based on attributes and not on their identities. Maintenance of connectivity and trust are important criteria in secure link establishment between the nodes. The impact of high resource utilization constraints and the heterogeneous characteristics of devices in MWSNs render the key management schemes [5-8] inefficient. Hence, a pervasive authentication protocol [9] and secure data transmission protocol [10] are employed to meet the constraints and characteristics of MWSN nodes. The certificate-less remote anonymous protocol [11] is used to overcome the issues in security provision. Attribute-based encryption schemes [12-15] and fuzzy attribute-based

978-1-5386-6391-2/18/$31.00 ©2018 IEEE

signcryption schemes [16] address these issues by providing the trade-off between the security and elasticity in health care applications. Data protection against the insider attacks is a major concern in a remote patient monitoring system. The numerous processes involved in cryptographic and attribute-based algorithms cause computational overhead and consume time. Hence security assurance with less computational overhead and more energy efficiency are major requirements of MWSNs.

This paper presents a 3-tier architecture to address issues in trust management, security, and privacy in MWSNs. The sensor nodes in this architecture can continuously update their configuration and trust level to avoid being malicious. They continue to transmit usable, private and sensitive information as well. The 3-tier architecture is based on initial configuration of the wireless sensor nodes. The memory architecture of nodes allows default configuration to be changed [16]. This is the reason a node can act maliciously when its initial configuration is compromised. Proposed model records the initial configuration and saves it in separate file in an encrypted form and then uses that encrypted file for further operations. The encrypted configuration file is used for energy efficient communication. This is continued until the system is fully trained to identify the trustworthy nodes. The trusted nodes are used in the form of small clusters to ensure random checks by neighbouring nodes. The cluster heads are changed continuously to divide the network energy computation overhead among the nodes. The second tier is a training module based on machine learning capability. It identifies and makes sure trustworthiness of the nodes. Third tier deals with uniformity of network over-heads and ensures energy efficiency for nodes. The model is implemented in NS-2 for successful network communication and efficient energy usage. The results of proposed mechanism are compared with an anonymous authentication scheme presented in [17]. The results demonstrate that the proposed model performs better than the scheme in [17].

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 explains the proposed model. Section 4 presents the simulation results and the paper is concluded in Section 5.

II. Related Work

Current researchers have worked mostly on authentication, verification, and privacy techniques for managing trust in MWSNs. Authors in [17] have used anonymous authentication (AA) for finding a reliable node. This AA scheme not only performs better than previous AA schemes but also provides complete confidentiality of patients. The AA scheme should satisfy some security requirements. These requirements include mutual authentication, non-traceability, anonymity, no verification table, and session key agreement, perfect forward secrecy and attack resistance [17]. The authors after meeting these security requirements proposed an AA scheme and compared its performance against another AA scheme [18].

Authors in [18] presented an anonymous access control for WBANs. This scheme reduces the complexity by using the same architecture as described in [17]. They have introduced a separate step called signcryption (sign-based encryption). It requires a person/doctor to initialize the first communication message. This action forms the basis of authentication and verification of upcoming messages. Apart from this initialization phase, the three phases of authentication, authorization and revocation are dependent on the input of first person/user/doctor, thus rendering this technique heavily dependent on user input.

The mechanism in [19] is based on public auditing scheme. This is used with multi-user sharing data technique which publicizes cloud for forward security and identifies illegal group members. The scheme has implemented some heavy encryption techniques for message authentication. This heavy computation depends upon cloud storage hence it works only for cloud based wireless sensor networks backed by heavy processing and a memory unit.

The mechanism in [20] uses the modified version of low-energy adaptive clustering hierarchy (LEACH) protocol called LEACH++. Authors have included intrusion-based detection to enhance the protocol. The problem with LEACH is the setup phase. The network of nodes before it could be deployed needs to be setup as per LEACH requirements and only then it could be used properly, and a secure network is created.

An improved and anonymous authentication protocol has been introduced in [21]. This protocol uses two factor authentications for message security and verification. The patient ID and password are two factors which are used for this purpose. This technique is also based on first person acknowledgement.

A MAC based payload tuning technique for reliable communication has been discussed in [22]. This technique is based on collision probability which calculates the payload critical index for a node to identity its trust. The probability of payload function gives an edge to the attacker which if disguises as a defender can cause network deadlock with the increasing probability of an attack.

Another first person input based technique is discussed in [23]. The encryption key technique to secure message reliability causes computation overhead. The biometric sensor requires input of the first person to initiate working of the network.

A path length factor-based trustworthiness estimations method for WSNs has been worked out in [24]. Path length factor refers to closest neighbour based on hop distance. The proposed estimations method is based on fuzzy logic to calculate reliability of the node. The trust mechanism takes care of reliability of nodes, but it is far less accurate in terms of message verification.

Authors in [25] have discussed various threats present in wireless sensor networks. The two types of attacks are classified as external attacks and internal attacks. The external attacks include denial of service (DoS) attacks, replay attack and sniffing. The internal attacks comprise of malicious attacks which nodes launch against other nodes. Internal attacks consist of Wormhole, Greyhole, Sinkhole and Blackhole. Internal attacks are considered more serious as compared to external attacks. In order to defend against

internal attacks, there is a need for a trust management system which calculates trust value of a node and determine whether the node is malicious or not. However, the authors also mention that even with a proper trust management system, there are attacks which are aimed against network communication. The authors in their proposed model first calculated a node trust value using dynamic sliding time window and defined a trust tree model. The model is tested in a TOSSIM simulator against some current algorithms. The results showed better performance and security against other solutions.

This review of schemes is summarized in Table I. The performance criteria are based on message authenticity, message verification, node authenticity, computation overhead and energy efficiency. These parameters are also considered for trust calculation and performance evaluation of the proposed model.

TABLE I. OVERVIEW OF EXISTING TECHNOLOGIES

Reference No.	Message Authentication	Message Verification	Node Authenticity	Computation Overhead	Energy Efficiency
[17]	Yes through key management	Yes. Through authentication ID	No	Yes	No
[18]	Yes. First person signature based encryption	Yes through authorization	No	Yes	No
[19]	Yes. Through PrivateKey	Yes.	Yes	Yes	No
[20]	No	Yes	No	Yes	Yes
[21]	No	No	Yes	No	No
[22]	Yes	Yes	No	No	No
[23]	Yes	Yes	No	Yes	No
[24]	No	No	Yes	No	Yes
[25]	Yes	Yes	No	Yes	No

III. THE PROPOSED MODEL

A typical MWSN setup is shown in Fig. 1. Typical examples of applications of MWSNs include monitoring of patients in hospital settings, remote monitoring of elderly patients at homes, collection of clinical and vital signs data of patients for decision making by doctors. A patient is the main source of information/data through various sensors. The data gathered from sensors is stored in a remote location where it can be used to generate several reports as per need. The sensor nodes in a MWSN are typical sensor nodes. But these nodes are well configured to work with necessary medical equipment for vital signs monitoring. This data can be transferred to remote locations through base stations. The data is configured in the form of a file set as an AVP (Attribute Value Pairs) value [26]. The configuration file has standard and default information of heart rate, pulse rate and blood pressure, default ID, battery, and temperature information. The values are set to verify the node.

The configuration file can easily be accessed through a firmware and is vulnerable to attacks. Hence it is important to ensure integrity of this file.

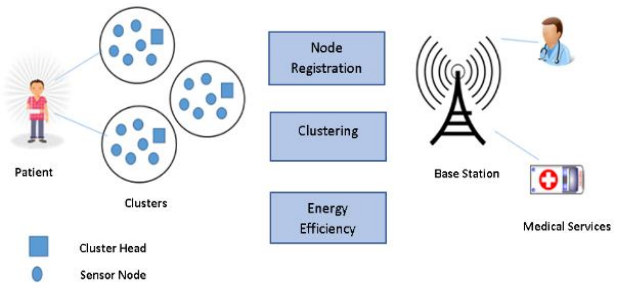

Figure 1. A sample scenario of a MWSN

A. First Tier Architecture-Node Registeration

There is a different AVP for each information stored in the configuration file. The structure of AVP is as follows.

AP Code	AP Length	AP Value

In proposed model, for every entry AVP is encrypted during the first execution. The encryption of the AVP is performed by adding another tag consisting of node ID. The final configuration of AVP is as follows.

Node ID	AP Code	AP Length	AP Value

The new AVP is stored in new configuration file. Now the original configuration file can be tampered but not the new one as it is encrypted. After each communication the AVP is updated and encrypted again. The system keeps calculating energy usage to make sure that this recursive nature of encryption may not cause computation overhead or energy leakage. If computation overhead causes energy leakage, machine learning technique is applied at second tier.

B. Second Tier Architecture Clustering

In order to divide the computation overhead over the network we have proposed clusters of closely related nodes based on the distance and signal strength. Each cluster is headed by a cluster head (CH) which takes most of the computation and stores the configuration file of all the nodes. When energy consumption goes beyond the set limit the cluster head configuration is sent to another node. This divides the overhead and maintains energy efficiency.

Trust evaluation of a node is carried out based on misbehaviour types. Apart from defining misbehaviour types

for direct trust evaluation, we have ranked each type based on level of severity. The types of misbehaviour that we have considered are as follows:

If a node does not forward messages (Level 5).

If a node advertises many paths and the paths are declared good (Level 4).

If a node re-routes to avoid a broken link. However, no errors are observed (Level 3).

If a node frequently updates routes which is deemed unusual (Level 2).

If a node tampers with the message header and makes a silent route change (Level 1).

Based on these defined levels of severity, we assume that a node cannot misbehave on two events at the same time. Using these levels of severity, a trust value is assigned to every node. It is important to mention that in proposed scheme, the level of severity is inversely related to the trust value that is if a node misbehaves at a level 1, the node will be assigned the maximum trust value. However, if a node acts on a level 5 severity, then that node will be assigned a low trust value. Following equation represents the relationship between severity and trust value.

$$T_{dt}(A{:}\,B, act) = k_{dt} * \frac{1}{(act)} + S_{lt} \quad (1)$$

where S_{lt} represents the level of severity. T_{dt} represents the direct trust value of a node. k_{dt} refers to a constant which we have defined in the protocol stack. The value of *Kdt* is determined based on the level of severity to make sure trust is low when the level of severity is high. *act* represents the acknowledgement, and its value is 0 or 1 to ensure trust is calculated on receiving a response.

Depending on the history of information and the time of verification a node through machine learning capability can determine whether the node is malicious or not. For example, if a node CH_a is trying to verify the authenticity of another node CH_b, then the CH_a would first check the time at which the information provided by CH_b was last verified. If the information of verification was around for few more successful communications, then the CH_b node would be considered a trusted node and will be assigned a high trust value accordingly. However, in other case the CH_b would be declared as a possible malicious node and would be assigned a low trust value.

$$T_{Hni} = \{T_{Hn1}, T_{Hn2}, T_{Hn3}, \ldots\ldots T_{Hnj}\} \quad (2)$$

T_{Hni} represents the time factor at which the validity of information was verified

$$T_{idt} = f(x) = \begin{cases} W_{Hn}, & RI_n \le T_{Hni} \\ W_{Ln}, & RI_n > T_{Hni} \end{cases} \quad (3)$$

where, T_{idt} represents the indirect trust value of a node, W_{Hn} represents the higher weight of a node, W_{Ln} represents the lower weight of a node, RI_n represents the rating of information depending on its verification time. Indirect trust is defined as the trust of node n which is 1 hop distance from its communicating nodes.

After the calculation of both the direct and indirect trust values of a node, there is a need to calculate the complete trust (directly of a node or indirectly through one hop neighbours) value of a node. Following equation calculates trust value of a node through the summation of both the direct and indirect trust values.

$$T_{CHi} = \sum_{x=1}^{n} (T_{dtx}, T_{idtx}) \quad (4)$$

where T_{CHi} represents the trust value of the cluster head under consideration.

C. Third Tier Architecture-Energy Efficiency

Energy efficiency is the overall requirement and the proposed algorithm keeps on calculating it and when energy consumption reaches the defined limit a new CH is assigned. New CH assignment depends upon the trust value of the node. In order to become a CH the node has to achieve a certain level of trust. This is achieved by ranking of rating by other nodes and assignment of lower and upper weight limits depending on a successful communication log.

The algorithm which details the working of first two tiers along with energy consumption is follows:

Algorithm for 3 Tier Architecture

Function Fi(a) // i is the node and a is the area of network

```
Begin
  Open Node_i
  Encrypt ARP_i
   Select CH randomly
   Begin
       Assign OverHead = Sizeof(ARP)
       Assign time = rate of network speed
       Energy Consumed = OverHead/time
   End
   If Energy Consumed > Threshold
       Begin
                Record T_HNi
                Assign data(T_Hni) to RI_n
                Record W_Hn and W_Ln
                Compute f(x)
                Calculate T_idt based on W_Hn and W_Ln
                Assign Node(T_idt) to CH_i
          End
End
```

IV. Simulation Results

Table II represents the simulation scenario.

TABLE II. Simulation Parameters

Selected Protocols	AODV
Application Type	FTP

Node Density	100 nodes on area 3000x3000m
Area Sizes (meters)	3000x3000 m
Simulated Time	70 Seconds
Nodes Types	Mobile Nodes
Traffic Type	Constant Bit Rate
Performance Parameters	Computation overhead, Energy consumption, Throughput, Data drop rate
No. of Receiver	One at a time

The simulations are carried out in NS2 simulator [27]. Computational overhead rate, throughput based on trust calculation, energy consumption and data drop rate are calculated and compared with algorithm described in [17]. Fig. 2 shows that proposed model and existing model in [17] performed nearly the same in the beginning (till 10 nodes). This is because the nodes in proposed model take some time to form clusters and calculate the trust among them, once clusters are formed and trust relationships are established proposed model starts to perform better. Energy consumption by nodes in proposed model is less as compared to nodes in [17] as shown in Fig. 3. The cluster heads are changed continuously to divide network energy computation overhead among the nodes. In Fig. 4 throughput of proposed model is more than the throughput of [17]. It does not cross 1400 bits/sec value showing failure of the network in [17].

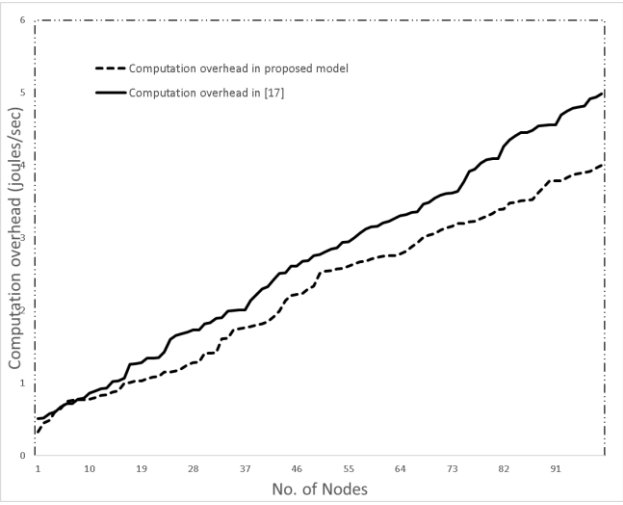

Figure 2. Computation overhead of proposed model and existing model [17].

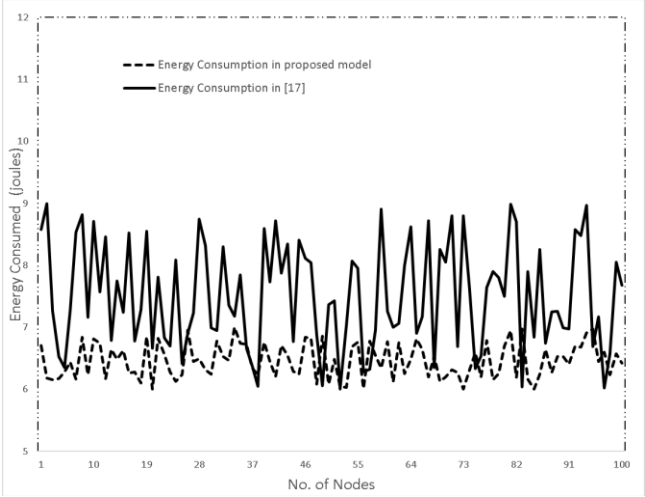

Figure 3. Energy Consumption in proposed model and existing model [17].

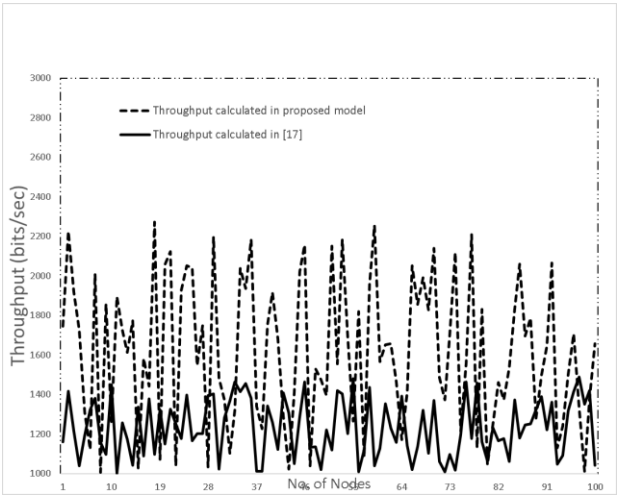

Figure 4. Throughput calculation of proposed model and existing model in [17].

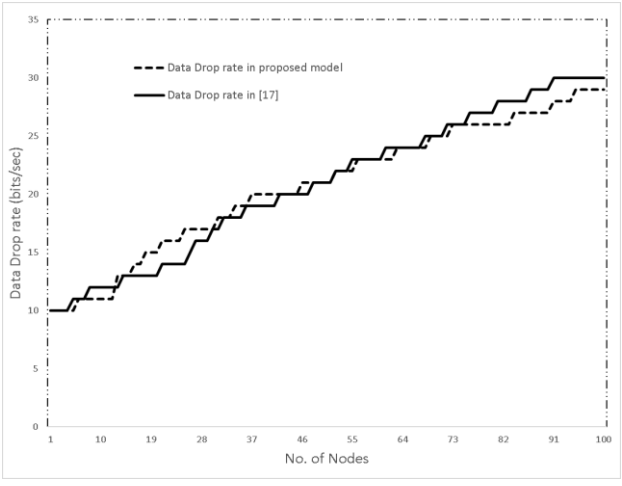

Figure 5. Data Drop Rate of proposed model and existing model in [17] for 100 nodes.

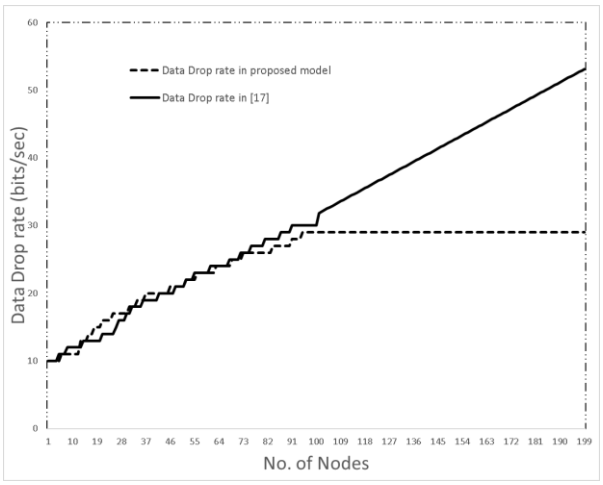

Figure 6. Data Drop Rate of proposed model and existing model [17] for 200 nodes

In Fig. 5 due to anonymous authentication, the data drop rate for the proposed model is slightly high in the beginning as compared to the existing model in [17] and then it starts to drop. This improvement is due to clusters formation and trust establishment in the proposed model. Addition of more nodes show uniformity in data drop rate due to existing clusters in proposed model as compared to the model in [17] which steadily increases as shown in Fig. 6.

V. CONCLUSIONS

Energy efficiency is an important concern in resource sensitive healthcare sensor-based devices. Due to the neglect of this vital parameter several latest technologies have failed to address trust management issues with optimal energy consumption. The proposed model with its 3-tier architecture and efficient cluster-based computation allowed the network to perform better in terms of computational overhead, throughput, energy consumption and data drop rate. Trust among nodes is achieved by registration through AVP values and then re-clustering of nodes allows distribution of computation overhead. This results in a comprehensive energy efficient solution.

ACKNOWLEDGMENT

The authors gratefully acknowledge the financial support provided by National ICT R&D fund Pakistan (Ignite) for this project

REFERENCES

[1] F. Ullah, A. H. Adullah, M. Q. Jan, and K. N. Qureshi, "Patient data prioritization in the cross-layer designs of wireless body area network," Journal of Computer Networks and Communications, vol. 2015, Article ID 516838, 21 pages, 2015. doi:10.1155/2015/516838 2015.

[2] Gu Xiang, Qiu Jianlina, Wang Jina, "Research on Trust Model of Sensor Nodes in WSNs", in International Workshop on Information and Electronics Engineering (IWIEE), pp.45-57, 2012.

[3] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 4, pp. 623-632, 2012

[4] M. Somasundaram and R. Sivakumar, "Game Theory Based Security in Wireless Body Area Network with Stackelberg Security Equilibrium," The Scientific World Journal, vol. 2015, Article ID 174512, 9 pages, 2015. doi:10.1155/2015/174512.

[5] X. Qi, K. Wang, A. Huang, H. Hu, and G. Han, "MAC protocol in wireless body area network for mobile health: a survey and an architecture design," International Journal of Distributed Sensor Networks, vol. 11, issue 10. 2015.

[6] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in INFOCOM 2013 Proceedings IEEE, 2013, pp. 2274-2282.

[7] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," in The International Conference on Information Networking 2014 (ICOIN2014), 2014, pp. 453-457.

[8] P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil, "Secure publish-subscribe protocols for heterogeneous medical wireless body area networks," Sensors, vol. 14, issue 12, pp. 22619- 22642, 2014.

[9] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," International Journal of Distributed Sensor Networks, vol. 2014, 2014.

[10] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Secure data transmission protocol for medical wireless sensor networks," in IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, pp. 649-656.

[11] M. S. Padma, D. J. W. Wise, M. S. Malaiarasan, and M. N. Rajapriya, "Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography," International Research Journal of Engineering and Technology, vol. 3, issue 3, pp. 1711-1715, 2016.

[12] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on hot topics on wireless network security and privacy, 2013, pp. 31-36.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE transactions on parallel and distributed systems, vol. 24, issue 1, pp. 131-143, 2013.

[14] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-health wireless sensor networks," in 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1-7.

[15] Y. Tian, Y. Peng, X. Peng, and H. Li, "An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks," International Journal of Distributed Sensor Networks, vol. 2014.

[16] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, issue. 9, pp. 37- 46, 2013.

[17] D. He; S. Zeadally; N. Kumar; J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," in IEEE Systems Journal , vol.11, issue. 4, pp. 2590 – 2601, 2016.

[18] F. Li; Y. Han; C. Jin, "Cost-Effective and Anonymous Access Control for Wireless Body Area Networks," in IEEE Systems Journal , vol.PP, no.99, pp.1-12, 2017.

[19] S. Li, Z. Hong and C. Jie, "Public Auditing Scheme for Cloud-Based Wireless Body Area Network," IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC), Shanghai, 2016, pp. 375-381

[20] A.H. Farooqi, and F.A Khan, "Securing wireless sensor networks for improved performance in cloud-based environments". Annals of Telecommunications, Vol. 72, No. 5 1958-9395. 2017.

[21] Wu F, Xu L, Kumari S, Li X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Systems 2015: 1–11, DOI: 10.1007/s00530-015-0476-3

[22] G. R. Tsouri, S. R. Zambito and J. Venkataraman, "On the Benefits of Creeping Wave Antennas in Reducing Interference Between Neighboring Wireless Body Area Networks," IEEE Transactions on Biomedical Circuits and Systems, vol. 11, no. 1, pp. 153-160, Feb. 2017.

[23] F. Hu, X. Liu, D. Sui, M. Shao and L. Wang, "Performance analysis of reliability in wireless body area networks," IET Communications, vol. 11, no. 6, pp. 925-929, 2017.

[24] D. He, S. Zeadally, B. Xu and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681-2691, Dec. 2015.

[25] V. K. Verma, "Pheromone and Path Length Factor-Based Trustworthiness Estimations in Heterogeneous Wireless Sensor Networks," in IEEE Sensors Journal, vol. 17, no. 1, pp. 215-220, 2017.

[26] L. Gang, M. Songwei and C. Jiming, "Auto-configuration mechanism for sensor node integrated into Wireless Intelligent Service Highway," 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, pp. 2090-2094, 2009.

[27] Available at: https://ns2projects.org/ns2-simulation-code-for-vanet/.