Trustworthiness Management Through Social Relationships in Internet of Medical Things

Marisângela P. Brittes, Bertoldo Schneider Jr. and Emilio C. G. Wille

***Abstract*— In recent years, the Internet of Things (IoT) paradigm has been introduced, getting attention as an emerging technology, built upon pervasive connectivity of objects in heterogeneous networks. In this context, biomedical networks are supporting biomedical environments, with many biomedical devices named objects, that are able to interact with each other and collaborate in order to achieve a common objective (diagnosis, treatment, and monitoring, patient rehabilitation). For this scenario, we use the concept of Internet of Medical Things (IoMT), as well the challenges to develop trustworthiness networks to exchange data in a biomedical environment. We propose a model to manage trustworthiness for IoMT networks based on social network concepts and priority criteria. Our model is based on a trust recommendation index, computed using the proposed trustworthiness management protocol. We analyze the effect of our protocol and demonstrate its effectiveness simulating an IoMT scenario, with improvements when analyzing the relationships establishment and network performance, also considering data and services exchanges.**

Keywords— Biomedical environment, Internet of Medical Things, IoT, Social Networks, Trust.

I. Introduction

IoT is defined as a dynamic global network infrastructure with capabilities of self-configuring, interoperability of communication protocols, where the objects can be physical or virtual and have identities, attributes and personalities, integrated as part of the same network [1].

IoT Technologies have entered the healthcare field through telehealth and ambient assisted living, which aim at increasing patient autonomy and confidence, as to bring quality of life, to prevent domestic accidents, to monitor chronic patients and to optimize traditional health systems, such public or private health providers, to use better economic resources [2].

Ambient assisted living and personal health monitoring are fields, which have gained special interest for their relation with elderly and chronic patients, and their growing in the actual world scenario. Through the use of resources such artificial intelligence and IoT, we can identify the health status of patients, learn about their behavior patterns, gain knowledge of the context, define rules for scenarios and study the relations about patients' health and their behavior [3][4][5].

There is an intense interaction between the things/objects and related services in IoT, which can collaborate to realize complex tasks and improve the quality of life of people.

The challenge in such environments is to guarantee the objects trustworthiness to allow trustful transactions through the establishment of connections to service or data exchange.

Some approaches have been proposed to apply social network concepts to validate the good reputation of the objects through recommendations, introducing concepts of Social IoT [6][7].

By the particularities of biomedical environments, we work with the concept of Internet of Medical Things (IoMT), to characterize the biomedical features and the proposed trustworthiness management protocol. The biomedical features support the trust index calculation, by the function of the objects in the IoMT network.

This article is organized as follows: Section I presents an IoT introduction, Section II presents the background of Social Networks and Trustworthiness Management; the proposed model is shown in Section III. Section IV presents the results, Section V the discussion about the findings and Section VI the conclusions and future work.

II. Background

A. Social Networks and IoT

Some works have been demonstrating the effectiveness of social network concepts applied to IoT paradigm. The driven motivation is that these social approaches can support the operations of discovery, selection and composition of services and data exchanges among the objects.

One of the first proposals involving some level of socialization between objects can be found in [8], applying the concept called Smart-Its Friends procedure to provide access to a very user friendly interface, with temporary relationships of friendship on Smart-Its, (i.e, smart wireless devices with capabilities of sensing, processing and communicating) since the devices context.

Blog-jects or objects that blog [9], is an example of this new paradigm of interaction with the world. The things/objects are connected to the internet and active in the social network.

An important research can be seen in [10], where the authors developed a vision of the internet as a pervasive IoT architecture. They presented the Social Organization Framework (SOF) model. This architecture is a central data

The Ad Hoc Associate Editor coordinating the review of this manuscript and approving it for publication was Prof. José Roberto de Almeida Amazonas.

M. P. Brittes is with Federal University of Technology of Paraná (UTFPR), Campus Dois Vizinhos, Paraná, Brazil (e-mail: mbrittes@utfpr.edu.br).

B. Schneider Jr. is with Federal University of Technology of Paraná (UTFPR), Campus Curitiba, Paraná, Brazil (e-mail: bertoldo@utfpr.edu.br).

E. C. G. Wille. is with Federal University of Technology of Paraná (UTFPR), Campus Curitiba, Paraná, Brazil (e-mail: ewille@utfpr.edu.br).

Digital Object Identifier: 10.14209/jcis.2017.1

management to allow more computational power to the objects in the network.

In [11] is investigated the integration of IoT and social networks, through the study of some applications.

Another study exploring the social possibilities in IoT was developed in [12], which describes an architecture with objects that have capabilities to participate in groups of objects, with common interest acting collaboratively.

The project in [7] proposed a platform where robots can have social relationships among each other, as well with humans. In the work scenario, robots try to recognize objects and request help from their friends to execute some procedure.

None of these related works considers trustworthiness requirements.

The concept of Social Internet of Things (SIoT) is formally introduced in [13], with analyses of various types of social relationships among objects, proposing approaches to solve the trustworthiness problems in IoT. SIoT proposes the relationships establishment similarly to humans behavior, according to the following system architecture [13]:

1. Parental Object Relationship (POR): Relationship established between objects with the same industrial source.
2. Co-Location Object Relationship (C-LOR): Relationship established between objects according to their location, they can be heterogeneous or homogeneous.
3. Co-Work Object Relationship (C-WOR): Relationship established between objects according to their tasks, to cooperate in applications such medical emergency, telehealth, biomonitoring.
4. Ownership Object Relationship (OOR): Relationship between objects according to their ownership, such smartphones, pressure monitor, game console, smartwatches.
5. Social Object Relationship (SOR): Social relationship established between objects whenever they are in contact, in order their owners keep in touch.

The SIoT network is based on the concept that every object can search for services throughout their relationship, setting their friends, friends´ friends, in a distributed form to guarantee that objects and services discover is done with scalability and variety, since the same principles followed by human social networks. SIoT works with a spread data system and concept of objects centrality. The trustworthiness is calculated from recommendation mechanisms, based on direct and indirect opinion of each object.

In IoMT networks, we propose an approach considering relevance of biomedical functions of the objects in the IoMT as rule of priority trust to establish of connections/relationships.

B. Trustworthiness Management

There are some works about trustworthiness management in IoT. In [14] the authors proposed a model based on object reputation with fuzzy logic to evaluate the trust, to allow the cooperation between the objects in a wireless sensor network, part of an IoT, observing the objects behavior.In another work [15], it was proposed parameters to evaluate the social trustworthiness and the quality of service (QoS) trustworthiness, according to a hierarchical trustworthiness management protocol. On the other hand, in [16] the authors used a table to estimate the service classification to evaluate the user trustworthiness level.

Finally, in [17] is used the trustworthiness of the objects in a social network to support the service composition, based on events of interaction or encounter.

Some approaches are based in pair interactions to minimize the problem of connection between unknown objects in the network, as the Peer-to-Peer model (P2P) [30]. It investigates questions about malicious objects in the network, as well trustworthiness subjects. In this model, the evaluation of the pair trustworthiness is calculated for systems that store and share the reputation information in the network define rules since the reputation and offer trust levels between the pairs. These rules can be observed in the Table 1, as follows:

TABLE 1
STRATEGIES TO EVALUATE THE REPUTATION.

Storage	Sharing	Processing
Centralized	Local	Average
Distributed	Part	Weighted Average
Rater based	Global	Probabilistic Estimation

Several approaches can be used to trustworthiness information storage. As described in [20], all the information can be stored in a local center to feed the sharing information and to facilitate the processing. However, this can converge easier to a unique failure point. In [18] the information is distributed throughout the pairs, which store it. Another approach works with storage rate [19], when each pair stores information about other pairs trustworthiness. The storage based on rate uses a model where each pair stores its own reputation based on the last transactions [21].

Despite many works have described models to manage trustworthiness, none of them was yet proposed in specific to biomedical networks context. In this work, we present a proposal to minimize this gap, shaping a protocol to trustworthiness management to IoMT.

III. THE PROPOSED MODEL

Medical objects that can exchange data and services to each other compose IoMT networks, their number is increasing by the advances of sensors development and the facilities they provide to the health area.

In this work, we propose social relationships based in [7][13][17] to support the needs of the biomedical environments, supposing a critical and heterogeneous network, composed by a great number and variety of static and mobile objects.

The construction of a trustworthiness model for an IoMT network may observe some aspects, such the type of objects, the relationship levels and critical needs.

In [17] the authors described the trust-related forms of malicious object attacks, as follows:

1. Self-promoting attacks: it can promote its importance (by providing good recommendation to itself) so as to be selected as a service provider, but then stop providing services or provide malfunction service.
2. Bad-mouthing attacks: it can ruin the reputation of well-behaved objects (by providing bad recommendation for good objects) so as to decrease the chance of good objects being selected as service providers.
3. Good-mouthing attacks: it can boost the reputation of bad objects (by providing good recommendations for them) so as to increase the chance of bad objects being selected as service providers.

A malicious or suspicious object aims to break up the basic functionality of the IoMT and the data exchanges among the objects. In biomedical area, this is critical and deserves special attention specifically if the objects are bio data collectors with collaborative functions. If this object is affected, many others will be out of service.

A. The Trustworthiness Management Protocol (TMP)

We consider a heterogeneous scenario where a biomedical environment has many types of local static biomedical devices, as well mobile smart objects, such tags (RFID, NFC) for medication, communication devices from people who are in the environment and medical personal devices to monitor patients. In the IoMT environment, many types of objects exchange data. This data has different formats, to be used alone or in data aggregation functions, in cooperativeness scenarios, as well in context awareness analysis. For instance, many objects can send biomedical monitoring information of a patient at the same time, corresponding to the real time patient health status. When an object requests a service, some assumptions can be verified, as shown in Figure 1.

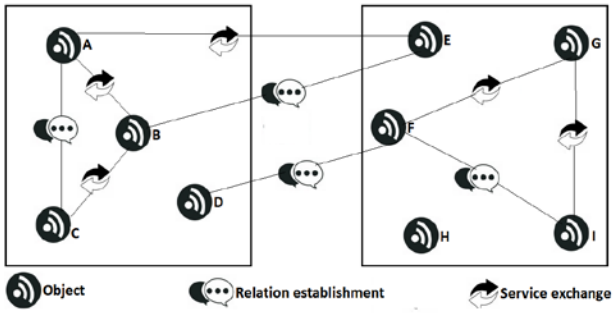

Fig. 1. Relationship request and service exchange scenario.

To execute these functions properly, the objects need to establish a relationship and exchange services. Trustworthiness mechanisms are necessary to guarantee the integrity of the IoMT network. In this context (Figure 1), object B exchanges services with objects A and C. A requests a relationship connection to C. In this situation, we assume object B can recommend A to C, by the relationship (friendship) between A and B. Object B requests connection to E and exchanges services with A. In the same situation, we assume A can recommend B to E, based on the existing relationship (friendship) between them.

On the other hand, object D has not established relationships and requests connection to F. In this case, we assume it has none (friend) to recommend it and it is harder its entrance in the network. The same situation of object H with no relationships.

In this research, we assume a scenario where the objects can communicate to each other to establish multiple connections (relationships) and exchange data.

These connections are similar to human social network relationships. According to the relationship type (strong or weak), people can recommend each other to new friends or not, depending on the past knowledge and number of common friends.

We assume IoMT networks follow some social behaviors [7][13][17], and can be applied to the biomedical context.

In our proposal, we also consider another social network characteristic [23]:

(i) Each individual in the network has a limited capacity of possible friendship.
(ii) The individuals have balanced friendships, considering their centrality in the network.
(iii) They change their friendship network during the time.

Besides, social networks are dynamic, with limited amount of available time and connections to each individual. The remaining relationships must have importance to individuals, so that it is defined the threshold strength for relationships. These threshold values will help to calculate the trust index in our trustworthiness management model.

We propose a Trustworthiness Management Protocol (TMP) based on the following criteria:

C1: the trust index is calculated using indirect recommendation from de objects.
C2: relationship threshold, to manage the number of connections.
C3: priority rules, based on the biomedical relevance in the IoMT network.

When an object (k) requests a connection to an object (i), the requested object evaluates the requester trust index $T(i,k)$, consulting his own friends (N) to recommend or not the connection, according to C1 criteria, as follows:

$$T(i,k) = \sum_{n=1}^{N} R(i,k,n), where\ R(i,k,n) = \begin{cases} 1 \\ 0 \\ -1 \end{cases} \quad (1)$$

When k requests a connection to i, this one consults if their friends know k and recommend it. A neutral recommendation means the object n does not know k or does not has an opinion about it. The k trust index is a sum of all the i friend's recommendation. Object k is allowed to connect to i only if its trust index is ≥ 0. The possible R value is 1 if the object is trustful, 0 if it is neutral or unknown and -1 if it is suspicious. A friend recommends another if their behavior is according to the expected pattern for its biomedical function, i.e., if a biomedical object is expected to transfer biomedical data in a time frame and it exchanges its data in the expected time, it has a good recommendation. If it does not do it, forcing his friend to wait more time without response, is a suspicious

behavior. In this case, the suspicious object has a bad recommendation.

If object k has an accepted trust index, then object i must verify its relationships number, according to C2 criteria, to guarantee they can connect:

$$C(i) = C_{Max}(i) - C_t(i) \quad (2)$$

The available number of connections is C, C_{Max} is its threshold and C_t is the current number of connections. If i is not full connected it can accept a new request for connection.

If i is already full connected, it must analyze its current connection status and verify if it can discard a connection to accept the new request.

It is necessary to calculate D, the discard index:

$$D(i,j) = \frac{\gamma_i}{\Delta T(i,j)} \quad (3)$$

Where j is already connected to i. Object i will discard the connection with object j with lowest D value, which means the most inactive connection in a certain time interval ΔT, according to its biomedical factor γ.

Biomedical factor in IoMT is described as follows: (a) Type 3, high relevance in the biomedical networks, such medical monitoring and life support devices; (b) Type 2, medium relevance, such as medical tracers, RFID/NFC; (c) Type 1, low relevance, such communication/information devices. Thus i discards the most inactive relationship and accept k's connection request.

IV. Model Analysis and Results

We implemented objective parameters to compose the trust index, according to the behavior of the objects in the IoMT network. Considering a medical environment with heterogeneous personal and portable medical devices, we supposed three classes of medical devices, according to the biomedical factor, as follows:

$$\gamma = \begin{cases} 3,\ high\ relevance \\ 2,\ medium\ relevance \\ 1,\ low\ relevance \end{cases} \quad (4)$$

The evaluation of an object to be recommended depends on some parameters about its behavior through the IoMT network. We propose the analysis of three objective parameters: stability, integrity and connectivity.

The object stability is related to its capability to exchange services/messages over its time connection and it is given by:

$$\sigma = 1 - \gamma\varepsilon \log\left(\frac{M}{T}\right) \quad (5)$$

Where σ is the stability index, M the total messages exchange, T connection time and ε is the level of protection desired to the global IoMT. The values vary according to the γ biomedical relevance function. We can adjust ε to evaluate how the objects behave in the IoMT network.

By relation to health area, IoMT needs to identify suspicious behaviors as soon as possible, so we implemented a rate called level of protection. We evaluate σ according to those classes of objects and their relevance in the IoMT network.

The decay of messages rate is considered suspicious behavior, due the need of constant data exchange in biomedical environment, in special to monitor bio parameters. We can notice in Figure 2 that objects with higher relevance can detect this suspicious behavior before the others and compute negative behavior to the stability index, from the 40% rate. Even when level of protection corresponds to 60%, it can react to suspicious behavior rapidly. According to the messages rate decay, the stability index becomes negative.

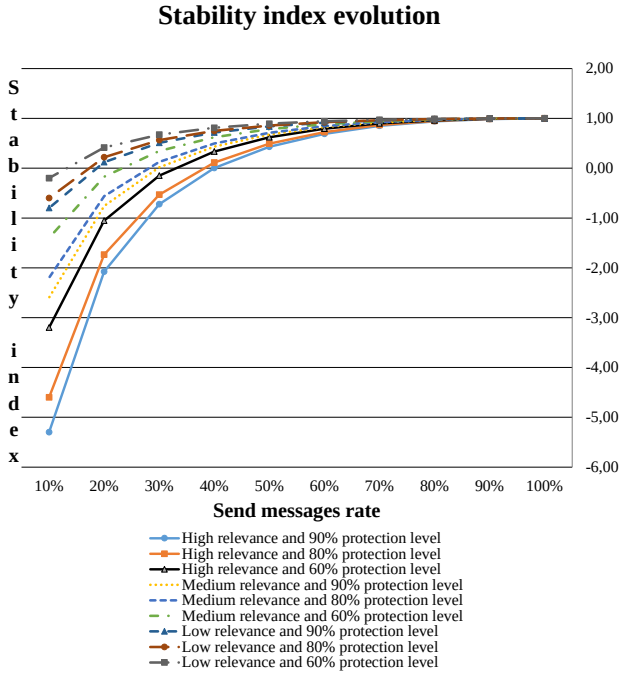

Fig. 2. Stability index evolution related to the send messages rate.

We also propose to evaluate the data integrity index τ. It computes the number of discarded messages over the data exchange, as follows:

$$\tau = 1 - \gamma\varepsilon\frac{B}{M} \quad (6)$$

We consider discard of messages (B) as another suspicious behavior. When the rate of discard messages increase, the objects may attribute to object provider negative score to its evaluation.

In Figure 3, we can see the integrity index evolution according to the discarded messages rate. Again, we applied the level of protection rate on γ to evaluate the objects´ behavior. The more relevant the class of the object (high relevance 3) faster the objects notice the suspicious behavior in the objects with increasing rate of discarded messages.

The third parameter considered is the object connectivity, which is estimated evaluating how central it is, considering its relevance in the IoMT service exchange and connections over the time. Thus, we have:

$$\theta = \frac{C}{C_{Max}} \quad (7)$$

where θ is the connectivity, considering the connections allocation of the object.

At last, the recommendation index R is a composition of these three indexes, calculating the average number of connections between objects, their message exchange rate and patterns of connection and disconnection, using stability, integrity and connectivity, as follows:

$$R = sign(\sigma + \tau + \bar{\theta}) \quad (8)$$

To avoid discrepancies, the average connections $\bar{\theta}$ was used and the 'sign' function is applied to get only the signal of the resulting sum. Thus, the final value will be only -1, 0 or 1 depending of each index value. Now it is possible to estimate suspicious objects in the IoMT network.

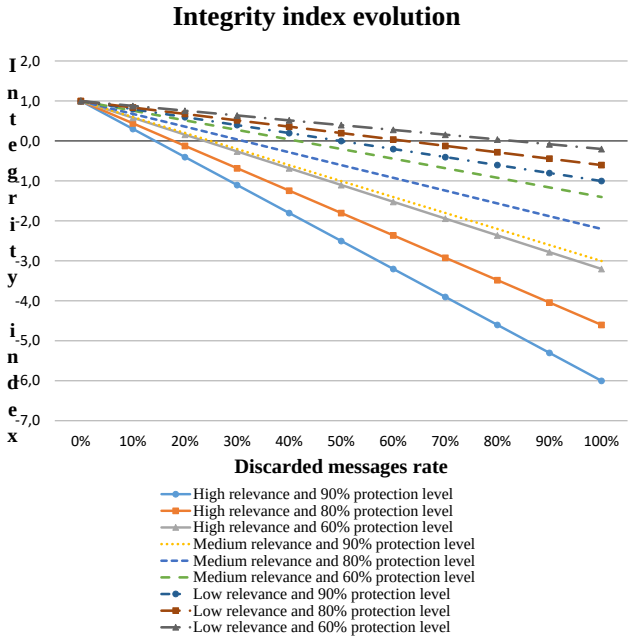

Fig. 3. Integrity index evolution related to the discarded messages rate.

To evaluate the evolution of recommendation index R, we assigned a 50% rate to θ and analyze the interaction rate through the objects, considering desired level of protection and the results according to the classes of objects.

In Figure 4, we can see the recommendation reduces according the decrease of interaction rate. The interaction rate is related to the parameters of stability, integrity and connectivity.

The composition of R was designed to cover the main aspects during events of interaction between objects.

Our approach is deterministic rather than probabilistic, the events considered are proposed to be similar to real IoMT environments, so the assumptions tend to be closer to the real applications.

V. Discussion

With the analysis of the results, we assume that it is possible to identify suspicious behaviors according to the interactions between the objects to exchange messages and services, collaborating to minimize losses in the IoMT network.

Other approaches have been used in trust management proposals based on concepts of social relationships [13] [17]. In our proposal, we apply social network theory to evaluate the centrality of objects, [23] calculating the average number of connections between objects, their message exchange rate and patterns of connection and disconnection, using stability, integrity and connectivity indexes.

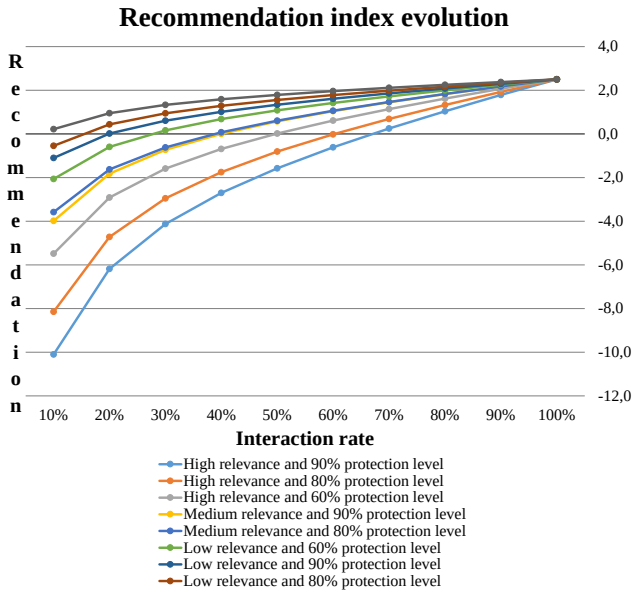

Fig. 4. Recommendation index evolution while objects interact to each other exchanging messages.

In [13] the authors proposed a generalist probabilistic model for personal devices based on parameters such as location, parental, ownership, social and work, with evaluation through simulations created from human mobility data. In [17] they also proposed probabilistic algorithms for trust management in generic dynamic networks, considering aspects such as honesty, cooperativeness and community of interest, with validations made through mathematical analysis using a Semi-Markov chain model.

These approaches used probabilistic models, in our model we propose a deterministic model from the indexes of stability, integrity and connectivity to reach our results.

The proposal presented in [13] considers computational parameters according to 4 classes: mobile devices with large computational capacity, static devices with significant computational capacity, devices with only sensing capability and RFID or NFC devices. This model is designed to act at the application layer, using a server, gateways, and agents. In [17], parameters related to computational capacity were not considered and the proposed model was designed to act on the network layer distributed between the objects.

Our model proposes the biomedical relevance factor focused on trust management between relationships for IoMT

networks, composed of three types: life support and monitoring devices, traceability and identification devices, and communication and information devices. Our model can be adjusted to the application layer and network layer, with distributed processing between objects.

In the graphs that present the performance analyzes, it is possible to observe the importance of the biomedical relevance factor proposed in the TMP protocol. Unlike other protocols, we propose to evaluate the level of protection necessary to identify suspicious behaviors of objects in the network, as well as to set tolerance levels of these occurrences, according to the type and function of the device in the IoMT network.

Our trust management protocol also contributes to the management and maintenance of relationships between objects, even when objects with doubtful behavior present themselves in the IoMT network. Different from the other proposals we propose to calculate indexes to obtain objective results, from events that can be computed in the IoMT network. This minimizes the computational and energy consumption of objects, which are usually limited by these features. In this way, it is possible to avoid harm in the service exchanges between the objects and to improve the distribution of the connections, with particular importance in environments with IoMT networks composed by objects where the services exchange cannot stop.

The evolution of the curves in the presented graphs presents the same pattern, demonstrating that the computed parameters contribute to indicate suspicious behaviors of the objects during their activity in the IoMT network. This identification becomes more accurate as the level of protection of the network increases.

We infer from the data obtained in the mathematical analysis that the TMP protocol offers a significant contribution to the management of the IoMT network, allowing to predefine the level of protection according to the types of objects that perform services exchange. This can be observed in the mathematical analysis related to the level of protection in each classes of objects, according to their function in the network. The more relevant the object's function, the more quickly suspicious behaviors are identified.

Performing service exchanges in an environment composed of trusted objects is a challenge in IoMT networks. In this work, we present the TMP protocol aiming to mitigate this gap, improving the establishment of reliable connections between objects and evaluate the object´s behavior related to stability, integrity and connectivity, generating recommendations.

It is a contribution to the development of safer and more reliable environments, platforms and applications for patients and professionals, as well as for the creation of a new generation of autonomous objects, which represent the evolution of current technology.

VI. Conclusions and Future work

The main contribution of this work is the TMP protocol to improve the management of trust in IoMT. We consider that the results obtained with this proposal are important for the development of IoMT applications in hospital environments, as well as assisted living and monitoring using wearable technologies.

All objects that make up such applications need to exchange services with each other and rely on trust-based protocols to ensure that secure connections are established. In the near future, all these objects will have more autonomy and possibly will not need human intervention to perform their actions.

Future studies should consider other aspects such as: propose an extension of the TMP protocol to detect the presence of objects in the IoMT network and avoid connections; another version of the protocol to increase the resilience of the IoMT network, using a local table with records about recommendations between objects.

References

[1] O. Vermesan, P. Friess, “Internet of Things – From Research and Innovation to Market Deployment” Aalborg: Rivers Publishers; 2014, pp. 32-40.

[2] European Commission. “Internet of things. An action plan for Europe” Commun from Comm to Eur Parliam *Council European Economic Soccial Community Regulation* 2009, pp. 1–12.

[3] H. Steg, H. Strese, C. Loroff, “Europe Is Facing a Demographic Challenge Ambient Assisted Living Offers Solutions”, *European Society* 2006, pp.1–85.

[4] A.J. Jara, M.A. Zamora-Izquierdo, A.F. Gomez-Skarmeta, “An ambient assisted living system for telemedicine with detection of symptoms”, *Lecture Notes Computer Science*, vol. 5602 LNCS, 2009, pp. 75–84. doi:10.1007/978-3-642-02267-8_9.

[5] A.F. Jara, M.A. Zamora, A.F. Gomez-Skarmeta, “An architecture based on internet of things to support mobility and security in medical environments”, in *Proceedings of the 7th IEEE Consumer Communication Networks Conference* CCNC, 2010. doi:10.1109/CCNC.2010.5421661.

[6] L. Atzori, A. Iera, G. Morabito, “SIoT: Giving a social structure to the internet of things”, *IEEE Communications Letters*, 2011, vol 15, pp. 1193–5. doi:10.1109/LCOMM.2011.090911.111340.

[7] C. Turcu, C. Turcu, “The Social Internet of Things and the RFID-based robots”, in *Proceedings of the Congress Ultra Modelying Telecommunication Control Systems Working*, 2012, pp. 77–83. doi:10.1109/ICUMT.2012.6459769.

[8] L. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, H-W. Gellersen, “Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts”, in *Proceedings of the Ubicomp 2001 Ubiquitous Computing*, 2001, pp. 116–22. doi:10.1007/3-540-45427-6_10.

[9] J. Bleecker, “A Manifesto for Networked Objects — Cohabiting with Pigeons , Arphids and Aibos in the Internet of Things”, Networked Publics 2005, pp.1–17.

[10] H. Ning, Z. Wang, “Future Internet of Things Architecture”, *IEEE Communication Letters* 2011, vol 15,pp.461–3. doi:10.1109/lcomm.2011.022411.110120.

[11] M. Kranz, L. Roalter, F. Michahelles, “Things That Twitter: Social Networks and the Internet of Things”, in *Proceedings of the 8th International Conference of Pervasive Computing*, 2010, pp. 1–10.

[12] E. Kosmatos, N.D. Tselikas, A.C. Boucouvalas, “Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture”, *Science*, 2011, pp.5–12. doi:10.4236/ait.2011.11002.

[13] L. Atzori, A. Iera, G. Morabito, M. Nitti, “The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization”, *Computer Networks*, 2012, vol 56, pp.3594–608. doi:10.1016/j.comnet.2012.07.010.

[14] C. Dong, C. Guiran, S. Dawei, L. Jiajia, J. Jie, W. Xingwei, “TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things”, *Computer Science Informatic Systems*, 2011, vol 8, pp.1207–28. doi:10.2298/CSIS110303056C.

[15] F. Bao, I-R. Chen, M. Chang, J-H. Cho, “Hierarchical trust management for wireless sensor networks and its application to trust-based routing”, in *Proceedings of the ACM Symposium of Applied Computing*, 2011, pp. 1732–8.

[16] Y.L.Y. Liu, Z.C.Z. Chen, F.X.F. Xia, X.L.X. Lv, F.B.F. Bu, "A Trust Model Based on Service Classification in Mobile Services", in *Proceedings of the IEEE/ACM International Conference of Green Computing and Communications*, 2010, pp. 572–576. doi:10.1109/GreenCom-CPSCom.2010.19.

[17] F. Bao, I-R. Chen, "Trust management for the internet of things and its application to service composition", in *Proceedings of the World Wireless, Mobile Multimedia Networks (WoWMoM), 2012 IEEE International Symposium*, 2012, pp. 1–6. doi:10.1109/WoWMoM.2012.6263792.

[18] S.D. Kamvar, M.T.Schlosser, H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks", in *Proceedings of the 12th International Conference World Wide Web (WWW)*, 2003, pp.640. doi:10.1145/775240.775242.

[19] A.A. Selçuk, E. Uzun, M.R. Pariente, "A Reputation-based trust management system for P2P networks", in *Proceedings of the Internation of Networks Security*, 2008, pp.227–37. doi:10.1109/CCGrid.2004.1336575.

[20] P. Resnick, R. Zeckhauser, E. Friedman, K. Kuwabara, "Reputation systems", *Communications ACM* 2000, vol 43, pp.45–8.

[21] R. Sherwood, S. Lee, B. Bhattacharjee, "Cooperative peer groups in NICE", *Computer Networks*, 2006,, vol 50, pp.523–44. doi:10.1016/j.comnet.2005.07.012.

[22] L. Atzori, A. Lera, G. Morabito, "Internet of Things: A Survey", *Computer Networks*, 2010 vol 54, pp.2787–2805. doi:http://dx.doi.org/10.1016/j.comnet.2010.05.010.

[23] R. Guimerà, L. Danon, A. Díaz-Guilera, F. Giralt, A. Arenas, "Self-similar community structure in a network of human interactions", *Physics Review E*, 2002, vol 68, pp.1–4. doi:10.1103/PhysRevE.68.065103.

Marisângela P. Brittes was born in Clevelândia (PR) – Brazil. She received her degree in Information Systems in December 2002, and a M.Sc. in Electrical Engineering in September 2007, both from Federal University of Technology of Paraná – UTFPR (Brazil). She is Professor at the UTFPR since march 2015, currently in Software Engineering department. She teaches software engineering practices to graduate level and her research interests are centered upon telecommunication networks, biomedical applications, software requirements and technology tools for education. She has co-authored several papers presented in national and international conferences, all of them in her research areas of interest.

Bertoldo Schneider Jr. was born in Curitiba (PR) – Brazil. He received his degree in Electrical Engineering in 1987, a M.Sc. in Biomedical Engineering in 1994 and Ph.D. in Biomedical Engineering in 2004, all of them from Federal University of Technology of Paraná - UTFPR (Curitiba - Brazil). He is Professor at the UTFPR, and since 1997 he works with biomedical instrumentation and biotelemetry. Currently he is in the Electronics Department. His teaching duties at UTFPR comprise graduate and undergraduate-level courses on electronic and biomedical areas. He has co-authored several papers presented in national and international conferences, all of them in the biomedical engineering area. His research interests are centered upon biomedical instrumentation, biotelemetry and rehabilitation engineering.

Emilio C. G. Wille was born in Lapa (PR) - Brazil. He received his degree in Electrical Engineering in February 1989, and a M.Sc. in Electrical Engineering in July 1991, both from Federal University of Technology of Paraná - UTFPR (Curitiba - Brazil). He received his Ph.D. degree in Electronic and Telecommunications Engineering from Politecnico di Torino (Italy) in February 2004. He is Professor at the UTFPR, and since October 1991 he is with the Electronics Department. His teaching duties at UTFPR comprise graduate and undergraduate-level courses on electronic and telecommunication theory. He has co-authored several papers presented in national and international conferences, all of them in the area of telecommunication systems and networks. His research interests are centered upon telecommunication networks, Markov processes, queueing models, and performance analysis.