A Bio-Inspired Trust and Reputation Model for Wireless Sensor Networks

Ramya, M[1], M.Govindaraj[2]
Department of Computer Science and Engineering
RVS College of Engineering and Technology
Coimbatore, India
ramyam485@gmail.com, govindh96@gmail.com

ABSTRACT: *The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor networks. In the existing system, cancelling feedback between cluster heads (CH) or cluster member can significantly improve system efficiency while reducing the effects of malicious nodes. This approach can effectively reduce networking consumption while malicious, selfish, and faulty CHs. In the proposed system, a bio-inspired trust and reputation model, called BTRM-WSN, based on ant colony systems aiming at providing trust and reputation in WSNs. A bio-inspired trust and reputation model (BTRM) remains to resilient to a high percentage of malicious servers, when this percentage of less than or equal to 90%, in which the accuracy, robustness and lightness of the proposed model in a wide set of situations.*

Keywords: Trust & Reputation Management, Wireless Sensor Networks, Bio-inspired Algorithms

Received: 8 January 2016, Revised 2 February 2016, Accepted 12 February 2016

1. Introduction

WSNs are networks based on small size nodes cooperation. Those nodes are mainly characterized by their low energy consumption, their low cost and, of course, their wireless communication. They can be used to make measurements of temperature, pressure, humidity, lightness, etc., but currently they often have certain probabilities of failure, as well as high restrictions of computing, memory and energy capabilities.WSNs are usually composed of a large number of these nodes which, together with their highly dynamic topology, may lead to some scalability problems. A number of research groups are working on them since this kind of networks has several interesting applications ranging from military ones to environmental ones, passing through sanitary applications, domotics, Intelligent Transportation Systems (ITS) etc. However, due to their important restrictions, they usually suffer from many security weaknesses, which make them often vulnerable to certain threats. Hardware failures could be a source of wrong critical information spreading, for instance. But even more, nodes belonging to a WSN could misbehave when they are asked for a measurement, or some data. Without loss of generality, we will adopt the scheme where some nodes of the network request some services and some others provide those services. In such a scenario, a node could provide a fraudulent service when this is requested. In addition, since we have supposed one of the most restrictive cases, where every sensor is only able to communicate with its direct neighbors, a malicious node could avoid reaching its benevolent neighbors,

or leading always to other malicious nodes, forming thus a collusion. It is therefore necessary to accurately distinguish trustworthy nodes from fraudulent ones. This trustworthy nodes identification can be achieved through a trust and reputation model.In this paper we specifically present a trust and reputation model for WSNs, called Bio-inspired Trust and Reputation Model for Wireless Sensor Networks in order to carry out the selection of the most trustworthy node through the most reputable path offering a certain service. Our proposed model is based on a bio-inspired algorithm called ant colony system (ACS), where ants build paths fulfilling certain conditions in a graph. These ants leave some pheromone traces that help next ants to find and follow those routes. Although ACS was initially mainly designed for static networks, experiments demonstrate that the adaptations done to make it suitable for WSNs lead to an accurate performance of the model. As we will see later, it allows a client to interact most of the times with a trustworthy server, rather than with a misbehaving one.

2. Literature Survey

A number of trust and reputation models and works oriented to WSNs. Boukerche, A., Xu, L., & El-Khatib, K.(2007).ATRM [9] is an agent-based trust and reputation management scheme for WSNs where trust and reputation management is carried out locally with minimal overhead in terms of extra messages and time delay. It is based on a clustered WSN with backbone, and its core is a mobile agent system. It requires a node's trust and reputation information to be stored in the forms of *t*-instrument and *r*-certificate by the node itself. Dhurandher, S. K., Misra, S., Obaidat, M. S., & Gupta, N. Authors of [10] present an Ant Colony Optimization approach for reputation and quality-of-service-based security in WSNs. They specifically propose a quality-based distance vector protocol known as QDV, where the more reputation a node has, the more reliable it is for communication purposes. QDV is able to protect the network against packet injection by those malicious nodes which have been detected. This protection is made by identifying those nodes that drop the packets forwarded to them. Chen, H., Wu, H., Zhou, X., & Gao, C. An agent-based trust model (ATSM) for WSN is presented in [11] using a watchdog scheme to observe the behavior of nodes and broadcast their trust ratings. The sensor nodes receive the trust ratings from the agent nodes, which are responsible for monitoring the former and computing and broadcasting those trust ratings. According to the received information, sensors nodes will make the decision about cooperate with their neighbors or not. Ganeriwal, S., & Srivastava, M. B. RFSN [12] is a framework where sensor nodes maintain reputation for other nodes in the network. A node monitors through a watchdog mechanism the behavior of other nodes, based on which it builds up their reputation over time. It uses this reputation to evaluate trustworthiness and in predicting their future behavior. At the time of collaboration, a node only cooperates with those nodes that it trusts. Srinivasan, A., Teitelbaum, J., & Wu, J.DRBTS [14] is a distributed security protocol aimed at providing a method by which beacon nodes (nodes that assist other sensor nodes to determine their location), BN, can monitor each other and provide information so that sensor nodes, SN, can choose who to trust, based on a quorum voting approach. In order to trust a BN's information, a sensor must get votes for its trustworthiness from at least half of their common neighbors

3. Bio-Inspired Trust Model for WSN

3.1 Assumptions/Scenario Description

Several types of wireless sensor networks can be found depending on what kind of nodes they are composed of. You can meet from a static WSN where nodes have a certain location, to a highly mobile one where nodes move everywhere like in a VANET. As we mentioned above, we are considering dynamic topologies, so we needed to use a technic capable of dealing efficiently with this issue. And in our opinion, one mechanism that fulfills quite well this matter is the ant colony system (ACS).

3.2 BTRM-WSN, A Bio-inspired Approach

BTRM-WSN is a bio-inspired trust and reputation model for Wireless Sensor Networks aimed to achieve to most trustworthy path leading to the most reputable node in a WSN offering a certain service. It is based on the bio-inspired algorithm of ant colony system but, due to the specific restrictions and limitations found in WSNs, the ACS cannot be directly applied there. Some adaptations, therefore, have to be made. In our model, for instance, every node maintains a pheromone trace for each of its neighbors. This pheromone traces $\tau \in [0, 1]$ will determine the probability of ants choosing a certain route or another, and can be seen as the amount of trust given by a node to other one.

The heuristic values $\eta \in [0, 1]$, however, are defined as the inverse of the delay transmission time between two nodes. The fact that every node controls its own pheromone traces and heuristic values, and no one else but it can modify them can become an important security threat.

Other issue that avoids the direct application of the ACS in this environment is the fact that while an ant is searching for the

most reputable server providing a requested service, it could happen that some of the nodes that form the path followedby that ant become inaccessible. In that situation, the ant would be unable to come back to the client and it would get lost. In other words, when a client launches a set of ants, it has no guarantee at all that all of them are going to return and, of course, it cannot wait until all the launched ants came back in one iteration of the algorithm.

Therefore, the algorithmic scheme presented in ACS has to be redefined as shown in Algorithm 1

```
Algorithm 1 BTRM-WSN
While(condition) do
for k = 1 to Number_of_ants do
Sk←initial sensor (client)
 Launch ant k
{
do
for every returned ant k do
if(Q(Sk)>Q(Current_Best)) then
Current_Best ← Sk
while (timeout does not expire) and
Num_returned_ants <%Number_of_ants
}
if(Q(Current_Best)> Q(Global_Best)) then
 Global_Best ← Current_Best
 Pheromone_global_updating
(Global_Best, Q(Global_Best), ρ)
return Global_Best
```

On the other hand, this algorithm consists of the following steps:

1. Every ant adds the first sensor to its solution, which is always the client they are departing from. Then each ant decides which next sensor to move to according to the transition rule and it is sent there.

2. Once every ant has left the client, this one waits until they come back. For every returned ant, the client compares its solution and keeps the best one. As explained before, in a WSN the client has no guarantee that all the ants that were launched are going to come back, so it just waits until a timeout expires or a certain percentage of all the ants has returned.

3. The best solution found by all or some of the ants issued in the current iteration is compared with the global best solution and swapped if it is appropriate.

4. A pheromone global updating is performed over the links belonging to the global best path.

3.2.1 Path Quality

Each time a launched ant returns to its client carrying a solution with it, that client has to assess the quality of that solution. Specifically the ant keeps a list of all the sensors belonging to the selected path, together with the pheromone traces of the links that join them.

According to this, the path quality computation can be done in the following way:

$$Q(Sk) = \tau k$$
$$Length\ (Sk)_{PLF}$$
$$.\%Ak$$

where τk is the average pheromone of the path found by ant k, $PLF \in [0, 1]$ and $\%Ak$ represents the percentage of ants that have selected the same solution as ant k.

3.2.2 Ants Transition and Stop Condition

When an ant is travelling along the WSN searching for the most trustworthy route leading to the most reputable server it has to decide at each sensor which of its neighbors it has to move to. Every ant has also to decide whether to stop when it finds a server offering the requested service or if it should keep trying to find a more reputable one.

3.2.3 Punish & Reward

Once BTRM-WSN has selected what it thinks is the most trustworthy path leading to the most reputable server, the client actually requests the desired service to that server. Then, depending on the goodness of the server, it will provide the same service it was offering, or another worse. In this first stage we will consider only two possibilities.

The server can be totally benevolent and provide the same service it was offering can be totally fraudulent and provide a completely different service than the one that was offered. If the client is satisfied, a reward by means of additional pheromone contribution is done all along the selected path. The same expression used for pheromone global updating can be applied here as well.

3.3 Two Proposed Models

If we have a WSN where we are only interested on monitoring the behavior of sensors about just one service (or even if the WSN only provides one service), we could use this model without the problem of distinguishing a sensor's particular behavior for each provided service. Second, we have a low-constraint WSN (equally, a high performance WSN) and we need a more resilient model, capable of dealing with multiple services, we could adopt the second version of BTRM-WSN. In this one, every sensor has a pheromone trace for each one of its neighbors, and for each one of the services provided by the WSN. Likewise, sensors will remain always awake.

3.4 Scalability and Lightness

One of the strong points of our trust and reputation model is its scalability. In this kind of networks, whose size can vary from a handful of nodes until thousands of them, developing a scalable model is a critical issue. Since in our model every sensor manages and controls its own pheromone traces and there is not any central entity gathering ratings or supervising all or a subset of the sensors, we can state that BTRM-WSN is scalable.

4. Security Threats

The fact that every node maintains the pheromone traces of its neighbors and it is the only one who can manage, control and modify them, can lead to some security threats. But the only security threats related to this matter can appear if a malicious server colludes with other malicious servers, because a sensor is only able to manage the pheromone traces of its neighbors, but by the same reason it cannot control the pheromone traces that its neighbors have associated with it.

Therefore, two types of security threats may happen if collusion among malicious sensors can be created. Malicious sensors can praise their malicious neighbors by assigning them the maximum level of pheromone. Equally they can slander their benevolent neighbors by giving them the minimum value of pheromone. We will discuss in detail both situations next.

4.1 Praising Malicious Sensors

A set of malicious sensors can form collusion in order to increase their self-profit and interests. Each of them manage the pheromone traces of its neighbors, so what they can do isto praise those neighbors belonging to the collusion by giving them the maximum level of pheromone.

In this situation the malicious node who modifies the pheromone traces of its neighbors can act as a malicious service provider or could behave properly and supply the right requested service. If the second thing occurs ants will choose it as the service provider and its collusion will have no sense.

4.2 Slandering Benevolent Sensors

Another possible security threat would consist in slandering benevolent nodes. This is achieved by assigning the minimum

level of pheromone to those benevolent neighbors of a malicious one.

Again the malicious node can actually provide fraudulent services or right ones. In the first case, if there are alternative paths leading to the slandered benevolent sensor, ants should be able to discover them; otherwise, ants would select another different benevolent node.

And if the malicious server acts properly and provides the right service, ants will select it and its collusion will not have sense neither.

It is important to have in mind that there must be at least one accessible benevolent server in the WSN and the key consists of finding it. It actually does not matter which specific sensor is selected to interact with, the important thing is to select a trustworthy one.

5. Experiments and Results

Our bio-inspired trust and reputation model over Wireless Sensor Networks and have described some related security threats, it is time to demonstrate its accuracy, scalability and robustness.

To do so, we have developed a whole tested focused on three main targets. First, we are interested in finding out how many times our model is able to select the right benevolent server to interact with. In other words, we would like to know the selection percentage of trustworthy servers.

Since our model has a strong basis on random or probabilistic decisions, we considered that it would be also quite interesting to take care about the standard deviation of that selection percentage of trustworthy servers.

Finally, as a possible measure of the adaptability of our model specifically to WSNs, we gathered as well the average path length of the solutions found by our model. As we mentioned before, in a environment with a lot of restrictions like WSNs, the shorter path is always preferred since it supposes less consumption of sensors' resources.

5.1 Experiments and Results over Static WSNs

The first tested scenario consisted of static Wireless Sensor Networks, that is, networks where their sensors do not Switch-off and do not move, maintaining thus always the same topology.

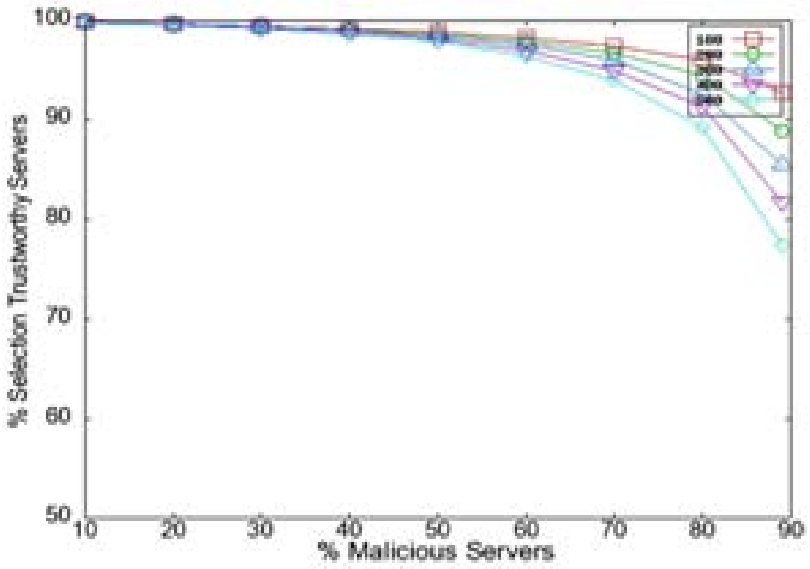

Figure 1. Static WSNs. Selection percentage of trustworthy servers

5.1.1 Selection Percentage of Trustworthy Servers

In order to consider a trust and reputation model as acceptable in our opinion, the selection percentage of trustworthy servers

should be greater or at least equal to 70%. A smaller percentage would result in a model with certain security deficiencies. And what is clear is that a selection percentage below the 50% means that the model is not useful at all.

Our experiments have shown that BTRM-WSN remains resilient to a high percentage of malicious servers when this percentage is less than or equal to 90%. Its performance gets worse when the percentage of malicious servers in the WSN increases, and the problem intensifies when the size of the WSN grows.

5.1.2 Average Path Length Leading to Trustworthy Servers

Finally, the last developed experiment consisted of measuring the length of those paths found by BTRM-WSN leading to trustworthy servers. That is, when the model fails and selects an untrustworthy server, that path is discarded and not taken into account.

This means that if the random tested WSNs size is too high, those networks topology can vary from ones where BTRM-WSN works quite fine to others where it is hardly able to find the most trustworthy server. Nevertheless, if the size of the random tested networks is high, their topologies drive the model behaving most of the times in the same way (most of the times well, or most of the times not).

5.1.3 Average Path Lngth Leading to Trustworthy Servers

Finally, the last developed experiment consisted of measuring the length (number of hops) of those paths found by BTRM-WSN leading to trustworthy servers. That is, when the model fails and selects an untrustworthy server, that path is discarded and not taken into account. Doing this way we are able to estimate the average path length of those paths found by our model when it successfully reaches a benevolent server. Our model is aimed to find the closest benevolent servers to the client requesting the service. On the one hand we think that the lesser number of intermediaries present in a transaction, the more secure and robust it can be performed. On the other hand, due to the specific restrictions related to wireless sensor networks, the resources consumption saving is acritical issue. Therefore, a shorter path leading to the final trust worthy server implies less involved sensors and, consequently, less global utilization of resources such as energyor bandwidth.

The outcomes of this experiment are presented in Fig. 1.As it can be observed, any trustworthy server is neverreached (on average terms) at more than 4 hops. In fact, the highest average path length is achieved with 100 sensors WSNs with a 90% of malicious servers. In that situation, the average path length takes the value 3.844.One more time, differences between the several sizes tested for WSNs become distinguishable when the percentage of malicious servers is greater than or equal to 90%.

Under this percentage, the average number of hops is quite low (near to 2), as it can be checked in the figure.

5.2 Experiments and Results over Dynamic WSNs

As we have already mentioned, the first of the two proposed versions of our model is aimed to deal with WSNs composed of sensors with quite high restrictions in energy consumption, bandwidth, storage capacity, etc.

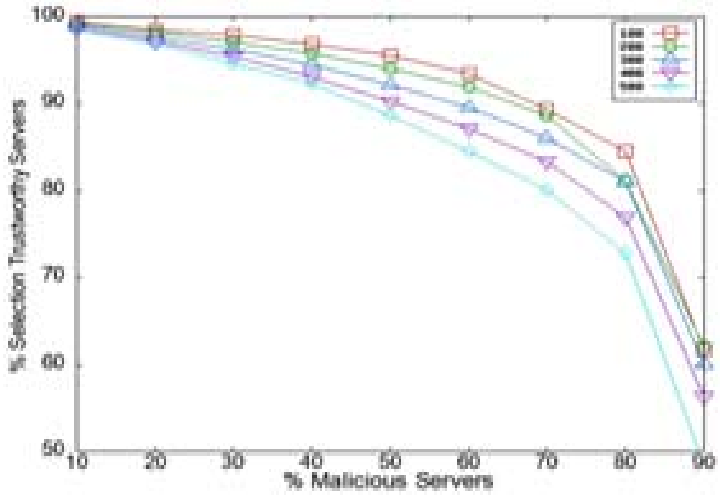

Figure 2. Dynamic WSNs. Selection percentage of trustworthy servers

5.2.1 Selection Percentage of Trustworthy Servers

BTRM-WSN is very accurate and almost always finds the same percentage of trustworthy servers. If we are dealing with a smaller Wireless Sensor Network or the proportion of malicious servers is greater than or equal to 90%, however, this standard deviation increases remarkably, being its maximum values a 19.35%,when the tested WSN is composed of 100 sensors.

5.3.3 Average Path Length Leading to Trustworthy Servers

Figure 9 shows the outcomes about the average path length of those routes found by BTRM-WSN leading to a trustworthy server over oscillating WSNs.

It can be checked that these results are very similar to the ones shown in Fig. 2, so the same conclusions can be obtained. The three last experiments demonstrate that BTRM-WSN is also a feasible technique in order to find the most trustworthy server over oscillating WSNs.

5.4 Energy Consumption

Energy consumption is a critical issue when dealing with wireless sensor networks, since these ones are commonly composed by resource-constrained devices with limited features in terms of processing, memory and communicating capabilities.

Therefore, we could not ignore this topic in our trust and reputation model, so we developed a last experiment aimed to measure the average energy consumption needed by our approach.

5.5TRMSim-WSN. Trust & Reputation Models Simulator for WSNs

In order to carry out all the explained experiments we have developed a Java-based Trust & Reputation Models Simulator for WSNs, called TRMSim-WSN. It allows a user to test BTRM-WSN over all the scenarios described in this paper (static, dynamic, oscillating and collusion), and even combinations of them, deciding the number and size of WSNs and the number of transactions or executions of the model carried out by every client. It also allows to set the percentage of clients, relay servers and malicious servers.

6. Conclusion

Managing trust and reputation in Wireless Sensor Networks in an efficient, accurate and robust way has not been completely solved yet. Providing this management would notably increase the security in such a sentient environment, supporting thus its development and deployment. In this paper we have proposed a Bio-inspired Trust and Reputation Model for WSNs, called BTRM-WSN. It is based on the Ant Colony System (ACS) and a complete description of its main features has been shown. We haveseen how the pheromone traces deposited by ants help next ants to find the most trust worthy server through the most reputable path all over the network. It has therefore been proved that BTRM-WSN is highly scalable, accurate, light and robust.

References

[1] Römer, K., Mattern, F. (2004). The design space of wireless sensor networks. *IEEE Wireless Communications, 11*(6), 54–61.

[2] Li, F., Wang, Y. (2007). Routing in vehicular ad hoc networks: a survey. *Vehicular Technology Magazine IEEE, 2*(2), 12–22.

[3] Marsh, S. P. (1994). *Formalising trust as a computational concept*. PhD thesis, Department of Computing Science and Mathematics, University of Stirling.

[4] Marti, S., Garcia-Molina, H. (2006). Taxonomy of trust: categorizing P2P reputation systems. *Computer Networks, 50*(4), 472–484.

[5] Dorigo, M., Gambardella, L. (1997). Ant colony system: a cooperative learning approach in the traveling salesman problem. *IEEE Transaction on Evolutionary Computing*, 1 (1), 53–66.

[6] Dorigo, M., Gambardella, L., Birattari, M., Martinoli, A., Poli, R., Stützle, T. (2006). Ant colony optimization and swarm intelligence.In*LNCS: Vol. 4150. 5th international workshop, ANTS2006*. Brussels: Springer.

[7] Cordón, O., Herrera, F., &Stützle, T. (2002). A review on the ant colony optimization metaheuristic: basis, models and new trends.*Mathware and Soft Computing, 9* (2–3), 141–175.

[8] Dorigo, M., &Stützle, T. (2004). *Ant colony optimization*. Bradford Book

[9] Boukerche, A., Xu, L., El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, 30 (11–12) 2413–2427.

[10] Dhurandher, S. K., Misra, S., Obaidat, M. S., Gupta, N. (2009).An ant colony optimization approach for reputation and qualityof-service-based security in wireless sensor networks. *Security and Communication Networks*, 2 (2) 215–224.

[11] Chen, H., Wu, H., Zhou, X., Gao, C. (2007). Agent-based trust model in wireless sensor networks. *In: Eighth ACIS International Conference on Software Eengineering, Artificial intelligence, Networking, and Parallel/distributed computing, SNPD'03* (119–124).

[12] Ganeriwal, S., Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. *In:* SASN'04: Proceedings of the 2nd ACM workshop on security of Ad hoc and sensor networks (66–77). New York: ACM.

[13] Michiardi, P., Molva, R. (2002). CORE: a collaborative reputation mechanism to enforce node cooperation in mobile Ad hoc networks, *In*: Proceedings of the IFIP TC6/TC11 sixth joint working conference on communications and multimedia security (107–121). Deventer: Kluwer, B.V.

[14] Srinivasan, A., Teitelbaum, J., Wu, J. (2006). DRBTS: distributed reputation-based beacon trust system. *In:* DASC'06: Proceedingsof the 2nd IEEE International Symposium on dependable, autonomic and secure computing (277–283). Washington: IEEE Computer Society.

[15] Buchegger, S., Le Boudec, J. Y. (2004). A robust reputation system for P2P and mobile Ad-hoc networks. *In*: Proceedings ofthe second workshop on the economics of peer-to-peer systems,Cambridge MA, USA.

[16] Buchegger, S., Boudec, J.-Y. L. (2002). Performance analysis of the CONFIDANT protocol: cooperation of nodes. In *Proceedings of IEEE/ACM symposium on mobile Ad hoc networking and computing (MobiHOC)*. Lausanne: IEEE.

[17] Almenárez, F., Marín, A., Campo, C., García, C. (2004). PTM: A pervasive trust management model for dynamic open environments, *In:* Privacy and trust, first workshop on pervasive security and trust, Boston, USA.

[18] Glover, F. W., Kochenberger, G. A. (2003). *Handbook of meta heuristics* (*International series in operations research & management science*). Berlin: Springer.

[19] Li, L., Halpern, J. Y. (2001). Minimum-energy, mobile wireless networks revisited. *In*: *IEEE International Conference on Communications, ICC* (1, 278–283).

[20] Sánchez, J.A., Ruiz, P.M. (2006). Improving delivery ratio and power efficiency in unicast geographic routing with a realisticphysical layer for wireless sensor networks. *In*: Proceedings 9th Euro Micro Conference on Digital System Design (DSD'06) (591–597).

[21] Xiong, L., Liu, L. (2004). Peer Trust: supporting reputation based trust in peer-to-peer communities. *IEEE Transactions on Knowledge and Data Engineering*, 16 (7) 843–857.