INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2017, VOL. 63, NO. 4, PP.411-416
Manuscript received September 18, 2017; revised October, 2017. DOI: 10.1515/eletel-2017-0058

# Towards an Evaluation Model of Trust and Reputation Management Systems

Marek Janiszewski

***Abstract*—The paper presents a set of concepts which can establish a basis for the creation of new evaluation model of trust and reputation management systems (TRM). The presented approach takes into account essential characteristics of such systems to provide an assessment of its robustness. The model also specifies measures of effectiveness of trust and reputation systems. There is still a need to create a comprehensive evaluation model of attacks on trust and reputation management systems and evaluation model of TRM systems itself, which could facilitate establishing a framework to deeply evaluate the security of existing TRM systems. We believe that this paper could be perceived as a small step forward towards this goal.**

***Keywords*—trust, reputation, attacks, trust and reputation management system, TRM, attacks on trust and reputation management systems**

## I. Introduction

TRUST and reputation management (TRM) systems are built on the notion of trust and reputation taken from humanities and social sciences. The analogy is quite simple: in a society, citizens are establishing social relations, in an information system (or in a network) many agents (nodes) exist which can establish interactions and provide or make use of different services (for example packet forwarding, files sharing, etc.). In a society, social relations can be characterized by trust between two citizens or by reputation of a citizen. In an information system analogic notion of trust can be used as a measure of the reliability of an agent. Like in society, the level of trust to another agent depends on the history of interactions with that agent and also on recommendations (opinions) of other agents about that particular agent. The evaluation of trust on the basis of TRM systems, facilitates to make a rational decision about selection of an agent to an interaction, especially when agents which could act selfishly or maliciously are present. Because of that TRM systems could lead to risk reduction in interactions between autonomous agents [1]. The idea behind trust and reputation management systems gets significance because of the fact that conventional security measures (based on cryptography) are often not sufficient [2], [3], [4]. Trust and reputation systems are a systematic approach to build security on the basis of observations of node's behaviour and recommendations exchange.

M.Janiszewski is with NASK - Research and Academic Computer Network, Warsaw, Poland, and with the Institute of Telecommunication, Faculty of Electronics and Information Technology, Warsaw University of Technology, Warsaw, Poland (e-mail: marek.janiszewski@nask.pl).

The main area in which TRM systems can be applied is the problem of choosing a service provider (an agent to an interaction). In a system (or network) can be many agents from different autonomous systems (governed by different entities).

Agents can provide services with a certain quality, but providing a service is associated with a certain cost which is related to the quality of service. Some agents can be selfish (they try to maximize own gain) or malicious (they try to disrupt the system). Because of that, before an agent will request a service from another agent, it want to estimate the reliability of that agent and choose the agent which is the most reliable. This can be done on the basis of history of node's own interactions and recommendations received from other agents.

TRM system defines the way of calculation of parameters which characterize other agents (such as trust or reputation) as well as the way of exchanging information between agents. Trust can be perceived as a value of confidence that an agent (trustee) will provide a requested service to another agent (trustor). Of course, trust is calculated by the trustor. Reputation can be perceived as a global opinion about an agent in a certain context. TRM systems can use either the notion of trust or reputation or both of them.

Trust and reputation management systems can be applied in many areas, such as: e-commerce (auction sites, online stores), WSN (Wireless Sensor Networks), MANET (Mobile Ad hoc Networks), P2P (Peer-to-Peer) networks and also social networks in broad sense. Any system which can process any type of recommendations, can gain much benefits from application of a TRM system. Applications to fight against many types of spams (for example e-mail or phone spam) can also be built on the basis of trust and reputation systems.

TRM systems give not only benefits but also could be a thread itself. In fact, many attacks on trust and reputation systems exist. Researchers usually concentrate on new TRM systems' proposals or on creating taxonomy of such systems [5], [6], but in many papers, authors claim that the weaknesses of TRM systems still do not gained enough attention [7]. Until now, there is no acknowledged comprehensive methodology of evaluation of trust and reputation management systems [8] and this is a serious problem related to TRM systems.

This work contains a description of generalization of trust and reputation management systems which can be used to evaluate reliability of such systems in the context of preventing various attacks. Presented assumptions about evaluation model of TRM systems and of attacks on such systems are general. It means that the model can be used in various types of networks and applications (despite of characteristic of agents or

characteristic of services provided by agents). This paper can be perceived as a summary and an extension of earlier works conducted by the author (especially: [9] and [10]), related to constructing evaluation model of TRM systems and model of attacks on such systems.

## II. Related Works

Many taxonomies of TRM systems as well of attacks on such systems exist, although to the best of our knowledge there is no general characteristic of TRM systems which could be used to provide a comprehensive evaluation model of such systems

A survey of existing models of TRM systems can be found in paper [11]. In the paper authors contend that, because of disadvantages of existing models, there is still a need to create new models, which could be used to create a comprehensive framework to compare such systems and evaluate their effectiveness (for example in the context of attack prevention).

Article [12] contains extensive and comprehensive survey of trust and reputation models as well as a classification of such systems. Many trust and reputation systems are also presented in [6].

However, in some of the existing works, measures of effectiveness of TRM systems as well as of attack on such systems, are defined, the evaluation on the basis of such measures may be not sufficient. The paper [13] proposes a few measures of effectiveness of TRM systems, e.g. Malicious Node Detection Performance – MDP, which represents the average rate of detection of malicious nodes (agents) and False Alarms Rate – FAR, which represents the average ratio of mistakes during classification of reliability of nodes. The main problem with such measures lies in fact that in practice, most of the TRM systems during trust assessment do not use binary values (which could be used to classify nodes as benevolent or malicious), and because of that such measures are not precise. In paper [14] very similar approach is presented by the measure of Detection Accuracy. In some other papers regarding TRM systems, measures like: Packet Delivery Ratio[15], Packet Loss Ratio [15] and also Energy Consumption (by the TRM system itself) [14], [15] are defined. Of course, such measures can only be applied to few types of trust and reputation management systems (namely the types, which could be used to support routing protocols, for example in WSN or MANET networks), but cannot be applied to TRM systems in general.

There are many papers, which concentrate on attacks on trust and reputation management systems [2], [6], [7], [12], [16]-[20], many taxonomies of such attacks can also be found: [17], [19], [21]. The most common criteria of classification of attacks are the following:

- the level of knowledge of attackers about the TRM system [17],
- mechanisms used by the attackers (the decision in which step of TRM system, attackers take the malicious actions) [21],
- the aim of the attack [17], [19].
- directness of the attack [17],
- the number of the attackers (individual, group or collective attacks) [17].

Other criteria also exist (such as specified in [20]).

Many papers try to analyse TRM systems in the context of resilience to a certain attacks, but this can be perceived as an example of a reactive approach which is based on detection of certain attack signature [2], [13], [17], [20]-[22]. Such approach has very important disadvantages, more comprehensive described in [8]. Because of that more prospective approach can be based on creation of description (model) of TRM systems and attacks on such systems which could be used to more in-depth analysis to identify various currently unknown attacks. Moreover, in the literature [2] can be found the statement that still attacks on trust and reputation management systems have not gain enough attention of research teams. The special attention should be paid to create a quantitative approach to evaluate influence of attacks on TRM systems.

## III. General Model of TRM Systems

Each TRM system works according to the five following steps [9]:

1. Information gathering by observing interactions of other nodes, requesting recommendations from other nodes, and storing the history of previous interactions.
2. Trust evaluation on the basis of the information collected.
3. Service provider selection.
4. Interaction and evaluation of the interaction.
5. Punishing or rewarding (i.e. increasing or decreasing the value of trust to a node which have provided the service), depending on the assessment of the interaction's quality.

Information gathering is the most vulnerable step, because malicious nodes may present incorrect recommendations during this step. Malicious nodes can affect the trust assessment by manipulating the quality of services provided, and because of that also step 4 is vulnerable to malicious actions.

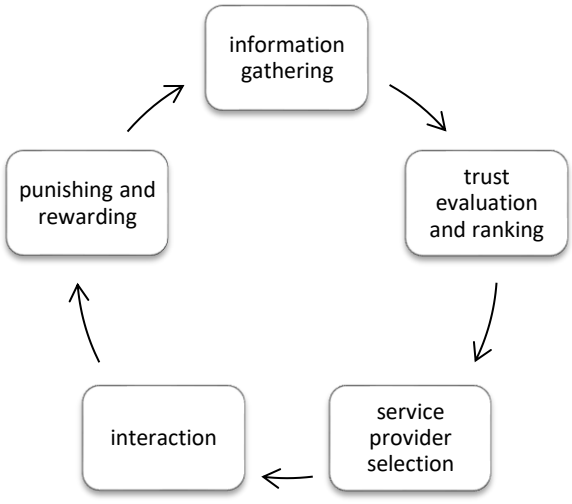


Fig. 1. Five steps of TRM systems

### 1) *Information gathering*

Trust and Reputation Management systems can use the following information types:

- the history of outcomes of nodes' own direct interactions,

- recommendations from other nodes (in TRM systems, which use recommendations),
- information about interactions of other nodes (it can be used only in systems, which store information about interactions in central database or in systems which facilitate providing such information to other nodes),
- nodes' own observations of interaction between other nodes.

It is worth to note that recommendations could be provided at least in two different ways:

- periodically (e.g. on every certain number interactions or after certain time),
- on request.

*2) Trust evaluation and ranking*

The way of aggregation of various types of information and creating ranking on that basis, is one of the most important characteristic of a TRM system. The most important differences between systems are a result of this step of the process.

*3) Service provider selection*

The most important ways of selection node as a service provider (partner of the interaction) are:

- selection of a node which are the most trustful,
- selection of a node from the group of nodes in which trust to any node is higher than a certain threshold.

*4) Interaction and the evaluation of interaction*

The evaluation of the interaction could be done in discrete or continuous values. During evaluation the following issues should be taken into consideration:

- the possibility of mistakes in the assessment process (for example because of external disruptions),
- time from interaction to the moment, in which the evaluation could take place.

*5) Punishing and rewarding*

During this step an agent (a node) can increase trust to other nodes (as reward for good recommendations or good service) or decrease trust to other nodes (as a punishment for wrong recommendations or bad service).

## IV. Model of Trust and Reputation Management Systems

The main idea behind trust and reputation management systems is the assessment that a node can evaluate trust to other nodes in the network. We assume that two groups of classes of trust (or reputation) can be distinguished: action trust and recommendation trust.

- **Action trust** refers to the probability that evaluated node will perform the service or action with satisfactory quality for the evaluator.
- **Recommendation trust** refers to the probability that evaluated node will deliver to the evaluator correct recommendation about action trust of another node.

We assume that every node in the network can evaluate trust values (which belong to one of these two groups). It is worth to note that some of TRM systems in practice use only one general trust value, but this fact is not reduce the usefulness of the presented model.

### A. Symbols

Let us denominate:

$N$ – the set of all nodes in the network,
$n$ – the total number of nodes ($n = n_M + n_B$),
$M$ – the set of malicious or selfish nodes,
$n_M$ – the number of malicious or selfish nodes,
$B$ – the set of benevolent nodes,
$n_B$ – the number of benevolent nodes,
$i, j$ and $k$ – node number $i, j$ or $k$ respectively,
$t$ – time (it can be defined discreetly - as the moment of the interaction),
$R_{i:k}^t$ – recommendation trust of node *k* to node *i* at time *t* (or during interaction number $t$),
$T_{i:k}^t$ – action trust of node *k* to node *i* at time *t* (or during interaction number $t$),
$TT_{i:k}^t$ – total trust of node *k* to node *i* at time *t* (or during interaction number $t$), total trust can be dependent of action trust of other nodes to node $i$ and of recommendation trust of node $k$ to other nodes,
$o_i$ – the outcome of *i-th* interaction (*i* is the global number of interaction in the whole network) - $o_i$ provides information about quality of interaction (service provide by a node), we can assume that $o \in < 0,1 >$ where $o = 1$ identify the best quality of a service and $o = 0$ identify the lack of the service,
$m$ – the total number of interactions in the network.

Values of parameters such as $R_{i:k}^t$ $T_{i:k}^t$, $TT_{i:k}^t$ can be discrite or continuous over a defined range. In case of some trust and reputation management systems these values could even be expressed in words (e.g.: high level of trust, low level of trust, undefined trust).

Complete description of a trust and reputation management system could be achieved by defining the character of the following parameters and functions:

- applied classes of action and recommendation trust - $C_{T_x}$, $C_{R_x}$: where $x$ denote the number of class of action or recommendation trust. Earlier in all symbols we have assumed (to simplify) that in a TRM system there can be only one class of action trust, and recommendation trust, but in general more such classes could exist. The generalization, by implementing more classes of action or reputation trust can be easily done, and it will not affect the correctness of conclusions.
- possible values of recommendations for each class of recommendation trust - $V_{R_x}$;
- possible values of action trust for each class - $V_{T_x}$;
- trust assessment function $TT_{i:k}^t = F_T(F_{dt}, F_{it})$, where $F_{dt}$ is a certain function which arguments are values of trust after former interactions (which is: $T_{i:k}^t$), and

can be perceived as a function which arguments are values of recommendations delivered by other nodes (which is: $R^t_{i:k}$);
- node selection function - $F_C(\,)$;
- recommendation deliver function - $F_R(\,)$, which define how recommendation for other nodes should be calculated;
- interaction assessment function - $F_O(\,)$;
- recommendation assessment function - $F_{O_R}(\,)$;
- frequency of issuing recommendations - $f_R$;
- parameters of node selection function (for example a threshold of trust, below which a node cannot be selected as a service provider) - $P_i^{F_T}$, where i denotes the number of a parameter.

### *B. The model*

Before the interaction, the node which needs service has to choose service provider. It can be done through evaluation of trust to all possible service providers. It is done by calculating $F_T(\,) = TT^t_{i:k}$ (we assume that node *k* is willing to find total trust of node *i* because is willing to interact with node *i*). The way in which the node will choose the service provider is defined by the node's selection function $F_C(\,)$, which is defined by the TRM system itself, but in general the node can select service provider in two ways:

1. Node *i* which needs service, choose node with the highest value of total trust among all nodes known by node *i*
2. Node *i* which needs service, choose the service provider randomly with the probability dependent on $TT^t_{i:k}$

After interaction, node *k* updates action trust to node *i* (which have provided requested service). In general, it is done by increasing action trust when the service/interaction was satisfying or decreasing otherwise. Of course, the way in which node *k* makes that update is defined by interaction assessment function - $T^t_{i:k} = F_O(\,)$.

Node *k* also update recommendation trust values to nodes which have provided recommendations about node *i*. In general node *k* increases the recommendation trust to nodes, which has provided correct recommendations, and decreases the recommendation trust to nodes which has provided wrong recommendations. The way in which node *k* makes that update is defined by recommendation assessment function: $R^t_{j:k} = F_{O_R}(\,)$.

### *C. The measures of effectiveness*

To measure the effectiveness of TRM systems (and also the effectiveness of attacks on TRM systems) we propose the following parameters:

**The network effectiveness** (E), which can be defined as proportion of sum of outcomes of all interactions to the number of all interactions and can be calculated as follows:

$$E = \frac{\sum_{i=1}^{m} o_i}{m}$$

**The resistance of the system** ($S_E$), which can be defined as the maximal proportion of the number of malicious nodes which are performing the most effective attack to the number of all nodes in the network, in which the system effectiveness does not fall below a certain value. For example. $S_{0.99} = 0.1$ means that when the ratio of malicious nodes is 10%, the system effectiveness would not fall below 0.99.

In other words:

$$S_E = \frac{n_{M'}}{n_A},$$

where $n_M{}'$ can be defined as the maximum number of malicious nodes in the network, which could not achieve higher degradation of the system (below E).

**The gain of network effectiveness** (G), which can be defined as the difference between the network effectiveness, in which there is a TRM system present (E), and the network effectiveness without TRM system implemented ($E^0$), under an assumption that in both cases attackers behave in the same way (they apply the same strategy of attacks, which could decrease the network effectiveness at most) : $G = E - E^0$

**The absolute gain of network effectiveness** ($G_A$), which can be defined as the difference between the network effectiveness, in which there is a TRM system present (E), and the network effectiveness without TRM system implemented ($E^{0\prime}$), under an assumption that in both cases attackers can apply different strategy of attacks to decrease the network effectiveness: $G_A = E - E^{0\prime}$

It is worth noting that from above definitions: $G_A \geq G$, because of the fact that: $E^{0\prime} \leq E^0$.

### *D. The measures of aggregated trust or reputation values*

The following parameters were defined to measure actual effectiveness of TRM system (on the basis of trust evaluation made by benevolent nodes). It is worth to note that these parameters can be calculated only when there is a possibility to identify malicious nodes (which in practice can be done only in controlled environment, for example during simulations).

The following measures of aggregated trust are defined under the assumption that only one class of action trust and only one class of recommendation trust are distinguished by the TRM system. In case of more class of action or recommendation trust, the following measures can be easily adjusted.

**Action reputation of all malicious nodes** ($T^t_{G;M:B}$), which can be calculated as the sum of action trust to all malicious nodes in the opinions of all benevolent nodes. For all *i*, *j*: $i \neq j$:

$$T^t_{G;M:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_M} T^t_{j:i}$$

where *i* is the *i-th* node in the set of benevolent nodes, *j* is the *j-th* node in the set of malicious nodes.

**Action reputation of all benevolent nodes** ($T^t_{G;B:B}$), which can be calculated as the sum of action trust to all benevolent nodes in the opinions of all other benevolent nodes:

$$T^t_{G;B:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_B} T^t_{j:i}$$

The measures of reputation of all malicious and benevolent nodes in the context of other class of trust (or reputation), can be defined in a similar way. For example in the context of recommendation reputation, these parameters can be defined as:
**Recommendation reputation of all malicious nodes** ($R^t_{G;M:B}$), which can be calculated as the sum of recommendation trust to all malicious nodes in the opinions of all benevolent nodes. For all $i, j\ i \neq j$:

$$R^t_{G;M:B} = \sum_{i=1}^{n_B}\sum_{j=1}^{n_M} R^t_{j:i}$$

**Recommendation reputation of all malicious nodes** ($R^t_{G;B:B}$), which can be calculated as the sum of recommendation trust to all benevolent nodes in the opinions of all other benevolent nodes:

$$R^t_{G;B:B} = \sum_{i=1}^{n_B}\sum_{j=1}^{n_B} R^t_{j:i}$$

The measures of total reputation (or total global trust), which is the way of combining all class of reputation in a way define by TRM itself, can be defined likewise:
**Total reputation of all malicious nodes** ($TT^t_{G;M:B}$), which can be calculated as the sum of total trust to all malicious nodes in the opinions of all benevolent nodes. For all $i, j\ i \neq j$:

$$TT^t_{G;M:B} = \sum_{i=1}^{n_B}\sum_{j=1}^{n_M} TT^t_{j:i}$$

**Total reputation of all benevolent nodes** ($TT^t_{G;B:B}$) which can be calculated as the sum of recommendation trust to all benevolent nodes in the opinions of all other benevolent nodes:

$$TT^t_{G;B:B} = \sum_{i=1}^{n_B}\sum_{j=1}^{n_B} TT^t_{j:i}$$

### *E. Aims of malicious nodes*

In general, malicious nodes aim at decreasing the network efficiency. However, malicious nodes may want to achieve more sophisticated goals. For example malicious nodes may want to prevent successful interactions and communications of a selected node.

The most important conclusion is that malicious nodes have to increase $R^t_{G;M:B}$, $T^t_{G;M:B}$ and decrease $R^t_{G;B:B}$, $T^t_{G;B:B}$ to be able to achieve certain goals.

If malicious nodes gain higher reputation, the probability of choosing a benevolent node as a service provider by other benevolent nodes could be decreased. On the other hand, in such case the probability of choosing a malicious node as a service provider by benevolent nodes could be increased. It can lead to paralyse the network for some time (as long as benevolent nodes do not decrease trust to attackers). Malicious nodes could also encourage benevolent nodes to choose always the same benevolent node as a service provider. Such behaviour can lead to exhaust resources (e.g. energy or processing power) of that node and in consequence to eliminate that node from the network (this attack can be considered as some kind of DDoS attack). In general gaining higher reputation by malicious nodes could enable making greater impact on the network.

Of course, benevolent nodes aim at increase $R^t_{G;B:B}$, $T^t_{G;B:B}$, E and decrease $R^t_{G;M:B}$, $T^t_{G;M:B}$

### *F. The characteristic of ideal TRM system*

On the basis of above parameters, it can be stated that an ideal TRM system is the system which (despite the fact that malicious nodes are present) facilitate to achieve the following values of the defined parameters (it can be assumed that all values of trust are in the range $< min\ ;\ max >$):

$$\boldsymbol{E = 1}$$
$$T^t_{G;M:B} = min, \quad T^t_{G;B:B} = max,$$
$$R^t_{G;M:B} = min, \quad R^t_{G;B:B} = max,$$
$$\boldsymbol{TT^t_{G;M:B} = min}, \quad \boldsymbol{TT^t_{G;B:B} = max}$$
$$\lim_{x\to 1} S_x = 1$$
$$G_A = G = 1$$

## V. Summary and Future Works

Evaluation model of trust and reputation management systems can be used to evaluate reliability of such systems in a quantitative way, especially when malicious agents can be present in the system. The question how the resistance for various types of attacks on TRM systems can be tested still remains open.

More deeply research are needed to prepare (on the basis of presented model) a general model of attacks on trust and reputation system to evaluate its usefulness to identify new attacks on trust and reputation management systems. The very first approaches to prepare such meta-model of attacks are in place already: [8], [23] but these approaches also need more research.

## References

[1] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)". *Recent Trends in Network Security and Applications*, pp. 420-429, 2010.
[2] Y. L. Sun, Z. Han, W. Yu, K. J. Ray Liu, "Attacks on Trust Evaluation in Distributed Networks" , *Proc. Inf. Sci. Syst. Conf.*, vol. 2, pp.1461 -1466, 2006.
[3] M. Blaze, J. Feigenbaum, and J. Ioannidis, "The role of trust manage-ment in distributed systems security", in *Secure Internet Programming*, Springer-Verlag, pp. 185-210, 1999.
[4] S. Ganeriwal , M. B. Srivastava, "Reputation-based framework for high integrity sensor networks", in *Proceedings of ACM Security for Ad-hoc and Sensor Networks (SASN)*, 2004.
[5] I. Pinyol, J. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: a review", *Artif. Intell. Rev.*, 40(1), pp. 1–25, 2013.
[6] J. Sabater, C. Sierra, "Review on computational trust and reputation models" *Artif. Intell. Rev.*, 24(1), pp. 33–60, 2005.
[7] X. Li, Z. Xuan, L. Wen, "Research on the Architecture of Trusted Security System Based on the Internet of Things", *Proc. 2011 Fourth Int. Conf. Intell. Comput. Technol. Autom.*, Vol. 02, pp. 1172–1175, IEEE Computer Society, Washington, DC, USA, 2011.
[8] M. Janiszewski, „Matamodel of trust and reputation management systems", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, vol. 8-9/2017, pp. 803-808, 2017.
[9] M. Janiszewski, „TRM-EAT - narzędzie oceny odporności na ataki i efektywności systemów zarządzania zaufaniem", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, vol. 8-9/2015, pp. 813-821, 2015.

[10] M. Janiszewski, „MEAEM – metoda identyfikacji i oceny najbardziej efektywnego ataku przeciwko systemom zarządzania zaufaniem i reputacją", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, vol. 8-9/2016, pp. 852-858, 2016.

[11] E. Koutrouli, A. Tsalgatidou, "Reputation Systems Evaluation Survey". *ACM Computing Surveys*, vol.48, no. 3, 2015.

[12] J. Sabater, C. Sierra, "Computational trust and reputation models for open multi-agent systems - a review", 2013.

[13] Y. Sun, Z. Han, K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks", *IEEE Communications Magazine*, vol.46, pp.112-119, 2008.

[14] H.Marzi, M. Li, "An Enhanced Bio-Inspired Trust and Reputation Model for Wireless Sensor Network", *Procedia Computer Science 19*, pp. 1159 – 1166, 2013.

[15] T. Zahariadis, H. Leligou, S. Voliois, S. Maniatis, P. Trakadas, P. Karkazis, "An Energy and Trust-aware Routing Protocol for Large Wireless Sensor Networks", *Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications*, 2009.

[16] A. Srinivasany, J. Teitelbaumy, H. Liangz, J. Wuy, M Cardei, "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks", W: A. Boukerche (red.), *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks*, pp. 375-404, 2009.

[17] Y. L. Sun and Y. Liu, Security of Online Reputation Systems The evolution of attacks and defenses, 2012.

[18] M. Srivatsa, L. Xiong, and L. Liu, "Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks," *Proc. 14th Int. Conf. World Wide Web*, pp. 422–431, 2005.

[19] Y. Yang, Q. Feng, Y. Sun, and Y. Dai, "Reputation trap: A powerful attack on repu-tation system of file sharing P2P environment," *Proc. 4th Int. Conf. Security and Privacy in Communication Networks*, pp. 1766–1780, 2008.

[20] F. Gomez Marmol, G. Martınez Perez, "Security threats scenarios in trust and reputation models for distributed systems," *Computers &, Security*, vol. 28, no. 7, pp. 545-556, 2009.

[21] K. Hoffman, D. Zage, C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems", ACM Computing Surveys, vol. 42, pp. 1-31, 2009.

[22] F. Gomez Marmol, G. Martınez Perez, "Trust and reputation models comparison," *Internet Research*, Vol. 21, No. 2, pp. 138-153, 2011.

[23] Bidgoly Amir Jalaly, Ladani Behrouz Tork, "Benchmarking reputation systems: A quantitative verification approach", *Computers in Human Behaviour* 57, pp. 274-291, 2016