Annales UMCS Informatica AI XIV, 2 (2014) 86–102
DOI: 10.2478/umcsinfo-2014-0012

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

The Oracle a New Intelligent Cooperative Strategy of Attacks on Trust and Reputation Systems

Marek Janiszewski[1*]

[1] *Institute of Telecommunication, Warsaw University of Technology, Warsaw, Poland*

Abstract – The paper presents a new concept of attack on trust and reputation systems. The oracle attack could violate the security provided by some of the existing reputation systems. The formal model of the attack is presented in the article on the base of the reference trust model, provided by the author. The author has proved that this type of attack could be efficient. On the other hand, a sort of measures is provided in the paper which could be implemented in the reputation systems to overcome identified vulnerabilities, unfortunately at the cost of increase of system complication. The paper also provides a definition of intelligent strategies of attacks on trust and reputation systems based on cooperation of many malicious nodes and justifies why this type of attacks is a serious threat.

1 Introduction

Monitoring behaviour of other nodes in the network could give very valuable indicators about reliability of this node. Moreover, exchange of nodes opinions about other nodes is very useful to indicate nodes which act selfishly or maliciously. Trust and reputation models are a systematic approach to build security on the basis of observations of nodes behaviour. The level of trust to other nodes in the network can be evaluated on the basis of interaction assessment. The idea behind trust and reputation models gets significance because of the fact that conventional security measures (based on cryptography) are often not sufficient [**1, 2, 3**]. Trust and reputation models give not only benefits but also could be a threat. Many attacks aim at trust and reputation management models exist. This work describes a new attack on trust and reputation management systems and also provides the way of defence against an attack. This paper also contains a formal description of generalization of many trust and reputation

*mjaniszewski@tele.pw.edu.pl

models which are used to analyze the efficiency of the proposed attack. The paper is organised as follows: the second chapter provides the list of works related to the subject. The third chapter contains the reference trust and reputation model. The description of the oracle attack is provided in the fourth chapter. the last chapter provides a summary and future work propositions.

2 Related Works

There exist many works about attacks on trust and reputations models, but existed the taxonomy of such attacks [**4, 5, 6**] does not include more sophisticated types of attacks. The papers listed above describe only a small fraction of attacks, most commonly referenced in the literature as classical attacks. The best known types of attack on trust and reputation management models are: False-Praise Attack (promoting attack) [**15**], [**1**], [**11**]; Bad-Mouthing Attack, (slandering attack) [**15**], [**11**]; Sybil Attack [**1**], [**13**]; Whitewashing, (New-Comer Attack) [**11**]; On-Off Attack [**1**], [**11**]; and Conflicting Behaviour Attack [**1**]. Some researchers try to create more sophisticated attack on the base of attacks listed above, for example article [**14**] contains six simple strategies of attacks which are combination of classical attacks. The example of attack based on cooperation (the slander attack) can be found in [**10**], but this attack can be efficient only in a very small fraction of trust and reputation systems, and more sophisticated trust models are completely resistant to this attack. The oscillation Attack presented in [**15, 16**] is another example of attack based on cooperation of many malicious nodes, but this attack is only small development of simple on-off attack. The RepTrap attack was proposed in the literature [**17**], [**15**] which is also combination of identified classical attacks. In article [**18**] the authors present Intelligent behaviour attack, but they do not give full description of such attack. To the best of authors knowledge the most advanced paper about attacks based on cooperation of many malicious nodes is [**13**]. In that paper the authors have proposed a few strategies of such attacks. The authors emphasize that propositions of attacks provided by them are not extensive and there is a great possibility that another attack exists. Despite that, in the literature [**1**] one can find the statement that still attacks on trust and reputation models have not gain enough attention of research teams. Moreover, joint effect of many of known attacks has been determined as a very interesting field of research [**12**]. Some of white papers [**1**], [**7**] emphasise the fact that intelligent strategies of attacks on trust and reputation systems could exist, and that there is necessity to investigate such attacks, but there is are no examples of such strategies. In the opinion of the authors of article [**1**]: intelligent strategies of attacks would be based on cooperation of many malicious nodes and the only way to prevent such attacks is pursuit to identify nodes which cooperate in an unusual way. This is not, however, a trivial case because to do this there is a need to find an effective solution to a clique identification problem (which is np-hard problem) [**4**]. The most extensive paper about trust and reputation models is [**8**], but this work does not describe any types of attack on such systems, but instead this article includes

a comprehensive survey of trust and reputation models as well as classification of such systems. Many trust and reputation systems are also presented in [**9**].

3 Reference Trust and Reputation Model

There are many different trust and reputation models but many of them have much in common. Because of that fact, in this chapter the Reference Trust and Reputation Model (RTM) is provided which is a generalization of many trust and reputation models. The Reference Trust and Reputation Model will facilitate the description of new attack on trust and reputation models the oracle attack.

3.1 Principles of the RTM

Each node in the network evaluates another known node by two measures: action trust and recommendation trust:

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

Assumptions:

α^R - the increase in recommendation trust as a result of correct recommendation

β^R - the decrease in recommendation trust as a result of incorrect recommendation

α^A - the increase in action trust as a result of good service

β^A - the decrease in action trust as a result of bad service

h - threshold - when a node has action trust to anther node below the threshold, it means that this node will never interact with such a node

h^R - recommendation threshold when the recommendation of action trust of another node will differ truly from the quality of service less than the recommendation threshold, the node recognizes that this node delivers correct recommendation, otherwise it assumes that the recommendation was wrong

$R^t_{i:k}$ - the recommendation trust of node i in the assessment of node k in time t

$T^t_{i:k}$ - the action trust of node i in the assessment of node k in time t

T^t_i - the action reputation of node i, calculated as follows (n-number of nodes in the network knowing node i):

$$T^t_i = \frac{\sum_{k=1}^{n} T^t_{i:k}}{n} \tag{1}$$

$n_{i:k}$ - the number of interactions between nodes i and k

$t_{i:k}$ - the time of the last interaction between nodes i and k

$a(n_{i:k}, t_{i:k})$ - the weight of nodes own estimation of trust, $1 - a(n_{i:k}, t_{i:k})$ weight of recommendations of others, we assume that $a(n_{i:k}, t_{i:k}) = a$ - const
$TT^t_{i:k}$ the total trust of node i in the assessment of node k in time t

3.2 Node (Service Provider) Selection

The node k is willing to find total trust of node i because it is willing to interact with node i:

$$TT^t_{i:k} = a \cdot T^{t-1}_{i:k} + \frac{(1-a) \cdot \sum_{j=1}^{n} T^{t-1}_{i:j} \cdot R^{t-1}_{j:k}}{\sum_{j=1}^{n} R^{t-1}_{j:k}} \tag{2}$$

when $TT^t_{i:k} > h$ - there can be an interaction between node i and k.
Before the interaction, the node which needs service has to choose the service provider. The node can the select service provider in two ways:

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

3.3 Trust Evaluation

After interaction, evaluation is made by node k: o - the outcome of the interaction: ($o - 1$ when the interaction is successful and $o = 0$ otherwise, o can also represent the quality of service provided by the node $o \in <0, 1>$, where $o = 1$ corresponds to the best quality and $o = 0$ corresponds to the lack of service).

The k node updates the action trust to node i:

$$T^t_{i:k} = \begin{cases} T^{t-1}_{i:k} + \alpha^A \cdot o, \ when\ o \geq h \\ T^{t-1}_{i:k} - \beta^A \cdot o, \ when\ o < h \end{cases} \tag{3}$$

and also node k updates recommendation trust to the nodes which have provided recommendations about node i:

$$R^t_{j:k} = \begin{cases} R^{t-1}_{j:k} + \alpha^R \cdot o, \ when \ |T^{t-1}_{i:j} - o| \leq h^R \\ R^{t-1}_{j:k} - \beta^R \cdot o, \ when \ |T^{t-1}_{i:j} - o| > h^R \end{cases} \tag{4}$$

which means that node k increases the recommendation trust to the nodes, which have provided correct recommendations, and decreases the recommendation trust to the nodes which have provided wrong recommendations.

The initial state before any interaction: $\wedge_{i,j,i\neq j} T^0_{i:j} = x; \ R^0_{i:j} = y.$

3.4 Measures of Effectiveness

o_i - the outcome of i-th interaction (i is the global number of interactions to the whole network)

n - the total number of interactions in the network

The network effectiveness:

$$E = \frac{\sum_{i=1}^{n} o_i}{n} \tag{5}$$

B - the set of benevolent nodes, n_B - the number of benevolent nodes in the network

M - the set of malicious nodes, n_M - the number of malicious nodes in the network

$T^t_{G;M:B}$ represents the sum of action trust to all malicious nodes in the opinions of all benevolent nodes.

For all $i, j, i \neq j$:

$$T^t_{G;M:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_M} T^t_{j:i} \tag{6}$$

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.

$T^t_{G;B:B}$ represents the sum of action trust to all benevolent nodes in the opinions of all other benevolent nodes:

$$T^t_{G;B:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_B} T^t_{j:i} \tag{7}$$

The last two measures can be referred as global action trust of malicious and benevolent nodes respectively.

The measures of global recommendation trust can be defined likewise:

$R^t_{G;M:B}$ represents the sum of recommendation trust to all malicious nodes in the opinions of all benevolent nodes.

For all $i, j, i \neq j$:

$$R^t_{G;M:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_M} R^t_{j:i} \tag{8}$$

$R^t_{G;B:B}$ represents the sum of recommendation trust to all benevolent nodes in the opinions of all other benevolent nodes:

$$R^t_{G;B:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_B} R^t_{j:i} \tag{9}$$

The last two measures can be referred as global recommendation trust of malicious and benevolent nodes respectively.

The measures of global total trust can be defined likewise:

$TT^t_{G;M:B}$ represents the sum of total trust to all malicious nodes in the opinions of all benevolent nodes.

For all $i, j, i \neq j$:

$$TT^t_{G;M:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_M} TT^t_{j:i} \tag{10}$$

$TT^t_{G;B:B}$ represents the sum of recommendation trust to all benevolent nodes in the opinions of all other benevolent nodes:

$$TT^t_{G;B:B} = \sum_{i=1}^{n_B} \sum_{j=1}^{n_B} TT^t_{j:i} \tag{11}$$

The last two measures can be referred as global total trust of malicious and benevolent nodes respectively.

3.5 Nodes Aims

The main aim of malicious nodes is decrease of network efficiency, but this can be not true in all cases. Malicious nodes may want to carry more refined goals for example to prevent successful interaction with the network of selected node. To achieve this goal malicious nodes have to increase $R^t_{G;M:B}$, $T^t_{G;M:B}$ and decrease $R^t_{G;B:B}$, $T^t_{G;B:B}$.

If malicious nodes gain higher reputation, the probability of choosing a benevolent node as a service provider by other benevolent nodes could be decreased by attackers. 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 paralysing 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 a kind of DDoS attack).

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

4 Oracle Attack as an Example of Intelligent Strategy of Attacks Based on Cooperation of Many Malicious Nodes

The oracle attack is a coordinated attack mounted by a group of malicious nodes. Although this is a common strategy by malicious attackers, the details of this attack are quite new. The Oracle attack presented in this chapter is an example of an intelligent strategy of attacks based on cooperation of many malicious nodes, this means that:

- many malicious nodes are engaged in this attack. Moreover, malicious nodes actively cooperate with each other and together set their actions,
- malicious nodes use different forms of classical attacks to achieve their goals,
- malicious nodes monitor actions of other nodes and actively adjust their own behaviour to these actions.

4.1 Course of the Attack

The strategy of the Oracle attack is based on attackers proper anticipation of behaviour of other malicious nodes, even when there is no possibility to predict the behaviour on the basis of previous interaction. In the oracle attack two groups of malicious nodes can be distinguished. In the first group there are nodes (named: the observed) which generally behave in a reliable way, but from time to time the act maliciously (they use a kind of on-off attack). The second group is composed of nodes (named the oracles), which always provide proper recommendation to other nodes about prediction of future behaviour of the observed nodes. Both groups communicate with each other and decide whether this time the oracles should provide positive recommendations about the observed nodes to other nodes in the network and then the observed ones would act properly or whether the oracles should give negative opinions to others and then the observed nodes would act maliciously. The clue of the strategy is the fact that because of cooperation between malicious nodes, the oracles always give proper recommendations, but the other benevolent nodes in the network, which

provide recommendation about the observed, are wrong from time to time (because of carrying out an on-off attack by the observed nodes). Benevolent nodes are mistaken when the observed nodes act maliciously (they provide positive recommendation because of former benevolent behaviour of the observed nodes). Because of this attack, the evaluation made a posteriori by benevolent nodes would increase reputation of the oracle nodes and decrease reputation of benevolent nodes, which have provided incorrect recommendations. This situation could be presented by the following example: the observed node acts benevolent so far, but the oracles send to nodes negative recommendations about this node. Then, this node start to act maliciously and because of that benevolent nodes increase the recommendation trust of the oracles, and decrease the recommendation trust of other nodes, which have provided recommendations (which was wrong in fact). It is worth noting that malicious behaviour (in the off phase) of the observed node could not be repeated too often. Otherwise, it could result in too large decrease of reputation of the observed node and in consequence, in discontinuous relations between the benevolent nodes and the observed one.

4.2 Effect in Case of Success

The main outcome of the attack is growth of the reputation of some attackers (oracles) and decrease in reputation of some benevolent nodes. Consequently, the attackers can achieve higher reputation than the benevolent nodes, which can lead to network effectiveness drop.

4.3 Consequences in Case of Failure and Reasons for Failure

In the case of properly carried attack, it should not have any negative consequences for attackers. The failure can result from the lack of proper synchronization of actions among malicious nodes (for example: oracles give negative recommendations but the observed node reliably performs a service). In such a case attackers achieve a reverse effect than they need: the recommendation trust of oracles among benevolent nodes is decreased.

Another potential reason for failure of this strategy can be the situation that benevolent nodes will decrease action trust to the observed node so much that they do not want to interact with this node any more.

Another threat for attackers comes from the parameters of trust model: worse performance of the observed node can result in very rare interactions with other nodes, and because of that oracles can not gain noticeably higher recommendation trust than other nodes. This can happen when just a few (or even single) bad service result in degradation of action trust to the node. This threat is not very serious because of the fact that such functioning of trust model is not a good idea especially in lossy networks (such as WSN).

Another cause of failure can be the lack of possibility for the attacker to obtain information about the threshold below which nodes will not want to establish communication (then the attacker can not estimate whether the observed node can perform unreliable service or it has to act benevolently to build up its reputation).

4.4 Further Actions of Attackers

The Oracle attack enables the attackers to achieve greater reputation than the benevolent nodes in the network, and because of that the attackers pursuit to limit the effectiveness of the network can be facilitated.

This attack can be used to achieve knowledge about characteristics of communication in the network and even to eavesdrop on the communication (because the oracles have higher reputation, they will be more often chosen for interactions by benevolent nodes).

Furthermore, the attacker can continue the attack to further reduce the reputation of benevolent nodes (for example by using the bad-mouthing attack).

Achievement of high reputation by attackers could also lead to paralysing the whole network because of discontinuation services and still providing high recommendation of other attackers.

4.5 Other Variants of Attacks

In theory another variant of the oracle attack exists. In this variant the observed node acts unreliably, but from time to time the oracle nodes give positive recommendation about this observed node and when a benevolent node choose the observed node as a service provider, the observed node acts reliably. Then the benevolent node increases action trust of the observed node and recommendation trust of oracle nodes, as well as decreases the recommendation trust of benevolent nodes which have provided negative (and wrong) recommendations about the observed node.

This variant of the oracle attack seems to be not very effective because the observed node in such a variant would have very bad reputation among the benevolent nodes which can result in cooperation avoidance to this node.

4.6 Vulnerable Trust Management Models

It is worth noting that some types of trust and reputation models are completely resistant to this attack. First of all, the systems with centralized reputation scores are not vulnerable to this attack (when the calculation of trust value is conducted by a central entity, the opportunity to carry out the attack is reduced). Secondly, the trust model has to use recommendations provided by other nodes in the network to be susceptible to the attack. All systems which use only own observations (direct trust) are resistant to this attack.

To sum up, all distributed trust and reputation management models which enable acquiring opinions about other nodes before every interaction are vulnerable to the oracle attack. In such a case attackers will have an opportunity to selectively conduct

the attack. All models susceptible to this attack are similar to the Reference Trust and Reputation Model, described in section 3.

4.7 Attack Components

The observed nodes apply just an on-off attack. The fact that the oracle node acts as an ideal node is very interesting the oracle node always provides right recommendations. It means that the oracle nodes apply none of the classical attacks.

4.8 Resources and Knowledge of the Attackers

Synchronization of actions of all malicious nodes is crucial to successfully conduct the attack. Because of that all malicious nodes have to possess a fast communication channel (to determine current behaviour of all malicious nodes). The separate communication channel, which would be inaccessible to other nodes would be the best option.

It is worth noting that malicious nodes do not need to have computational power higher than the other nodes in the network.

Ability to monitor the behaviour of other nodes is very useful for malicious nodes, because of the need to maintain action trust to the observed node above the threshold to prevent the situation in which benevolent nodes would not want to interact with the observed node. The knowledge about the algorithm of trust model and its parameters is also required (for example about the level of the threshold below which interactions are not undertaken).

4.9 Defence

The easiest way to prevent the oracle attack is keeping the history of recommendations provided by nodes about other nodes in the network. Sharp changes in the value of recommendations about a node could indicate an attack, especially when such changes could not be justified by normal operations of the node according to the trust model used by the node.

Evaluation of similarity to other nodes could be another way of defence from the oracle attack. In such approach the node A would increase trust to a node, which is similar to it. When the node A and the node B give similar recommendations (and also make the same mistakes), it means that they are similar. It is worth noting that this type of defence could not be very efficient because of the fact that such approach opposes an idea behind trust and reputation models.

To detect the oracle attack the ability to clique detection could also be very useful, but this is not trivial (clique detection is a np-hard problem).

4.10 Evaluation of Effectiveness of the Oracle Attack

Some of the existing trust and reputation models do not provide protection from the Oracle attack. This strategy can be effective and can be a serious threat, because

potential benefits for attackers are considerable. It is worth noting that implementation of the proposed defence mechanisms can result in decrease in efficiency of the attack. Increase in resources of nodes needed to carry trust model and increase in complication of trust model are the costs of the prevention mechanisms.

4.11 Formal Model of the Attack

We assume that all benevolent nodes in the network employ the RTM with the same parameters: α^R, β^R, α^A, β^A.

Let us denote:

M_o - the set of the oracle nodes;
M_w - the set of the observed nodes.

Let us assume that there are m_o oracle nodes, m_w observed nodes and b benevolent nodes. W can assume that all nodes are connected directly (this assumption is slightly artificial but it can facilitate further reasoning), then:

One of the observed nodes, let us say m_w is going to the off phase, then let say that node k ($k \in B$) interact with m_w node, then: $T^t_{m_{w_i}:k} = T^{t-1}_{m_{w_i}:k} - \beta^A$ - is decreasing but node k increases recommendation trust of all of the oracle nodes, which have provided recommendations: $R^t_{m_j} = R^{t-1}_{m_{o_j}:k} + \alpha^R$ for all $j \in M_o$; which means that $R^t_{G;M:B} = R^{t-1}_{G;M:B} + m_o \cdot \alpha^R$, and $R^t_{b_j:k} = R^{t-1}_{b_j:k} - \beta^R$ for all $j\ inB$; which in fact means that: $R^t_{G;B:B} = R^{t-1}_{G;B:B} - b \cdot \beta^R$.

It is easy to notice that global benefit for malicious nodes because performing a single attack is equal to: $m_o \cdot \alpha^R + b \cdot \beta^R$ and the global cost for malicious nodes is: $\alpha \cdot \beta^A$. It means that malicious nodes will benefit from the attack if: $(1-a) \cdot (m_o \cdot \alpha^R + b \cdot \beta^R) > a \cdot \beta^A$ and the total gain of the malicious nodes from the attack equals: $G = (1-a) \cdot (m_o \cdot \alpha^R + b \cdot \beta^R) - a \cdot \beta^A$, which means that the higher α^R, β^R, and the lower a, β^A, is the more effective is the attack.

It is worth noting that computation made above concerns only a single interaction between the benevolent and malicious nodes, but the intensity of interactions between the benevolent and malicious nodes is also very important.

4.12 Simulations

A home-made simulator was used to run simulations. The simulator enables to implement and measure the effectiveness of attacks on trust and reputation systems. the author has assumed that nodes deliver recommendation even when they do not have sufficient experience in interactions with the node which aspires to be a service provider. The author has also assumed that there are no data loses in the network.

In the simulations, networks consisting of 20 nodes were created (each node is directly connected with another node). In the first simulation there is no malicious node in the network, in the second there are 4 malicious nodes performing classical on-off attack. In the third simulation there are 4 malicious nodes (the observed node and 3 oracle nodes) performing the oracle attack. The total number of 10000 interactions was set. the comparison of global network effectiveness in these simulations is presented in Fgure 1.

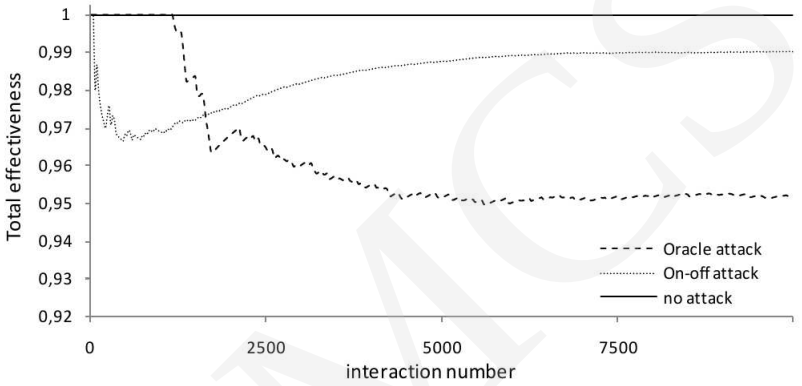

FIG. 1. The network effectiveness (E) comparison

As can be seen in Figure 1, the oracle attack is generally more effective (more hazardous for the network) than the classical on-off attack. It is worth noting that on-off attack has greater influence on network at the beginning of interactions (the total network effectiveness is lower in the on-off attack through around 1200 first interactions). This is due to the fact that in the oracle attack malicious nodes start to conduct attack after they have built up their reputations, but malicious nodes in the naive on-off attack just act maliciously from time to time, and start to act in this way from the very beginning. A more interesting fact is that after around 5000 interactions the total network effectiveness during the on-off attack is around 0.99, while during the oracle attack is around 0.95. The oracle attack leads to growth of recommendation reputation of attackers and decrease of recommendation reputation of benevolent nodes as well as slight decrease of action reputation of attackers. This statement was confirmed by the simulations and can be seen in Figure 2. It is worth mentioning that the difference between the global action trust of malicious and benevolent nodes is rather small, but the global recommendation trust of malicious nodes is much higher than the global recommendation trust of benevolent nodes, which means that benevolent nodes consider recommendations from malicious nodes as more reliable than those from other benevolent nodes.

The advantage of the oracle attack for the attacker can be noticed not only in the case of network effectiveness. Figure 3 presents the comparison between the total trust of benevolent nodes during the first (no malicious nodes in the network), second (4

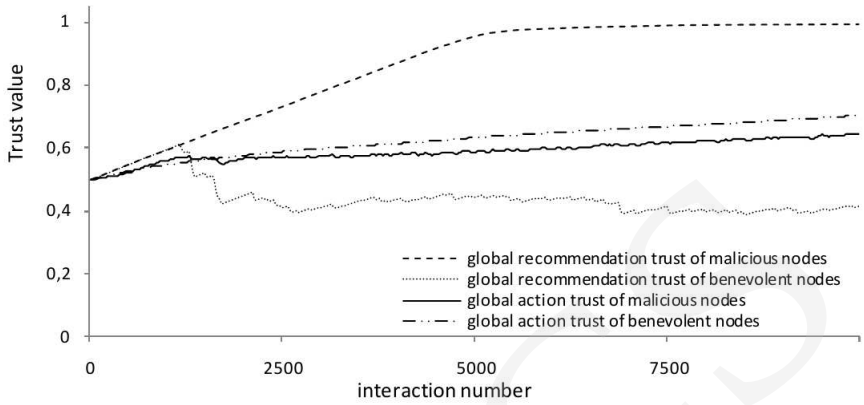

FIG. 2. Global trust values of nodes in the Oracle attack $(R^t_{G;M:B}; R^t_{G;B:B}; T^t_{G;M:B}; T^t_{G;B:B})$

malicious nodes performing the on-off attack) and third simulations (4 malicious nodes performing the oracle attack).

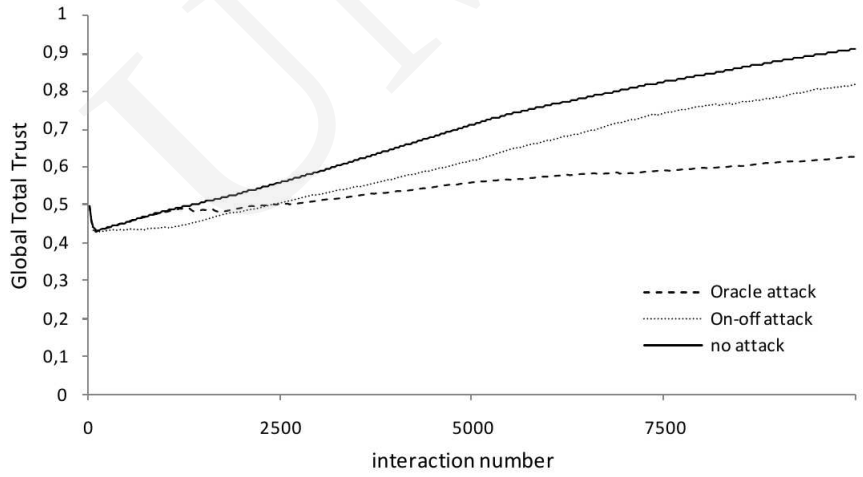

FIG. 3. Global total trust of benevolent nodes $(TT^t_{G;B:B})$

As can be seen from figure 3, the trust value of benevolent nodes to other benevolent nodes is the smallest during the oracle attack. It means that attackers are successful in decreasing the reputation of benevolent nodes.

Global total trust of malicious nodes and benevolent nodes during the oracle attack and the on-off attack is presented in Figure 4. In the case of on-off attack benevolent nodes have much higher reputation than the malicious nodes. In the case of the oracle

attack the difference between the total reputation of benevolent and malicious nodes is smaller.

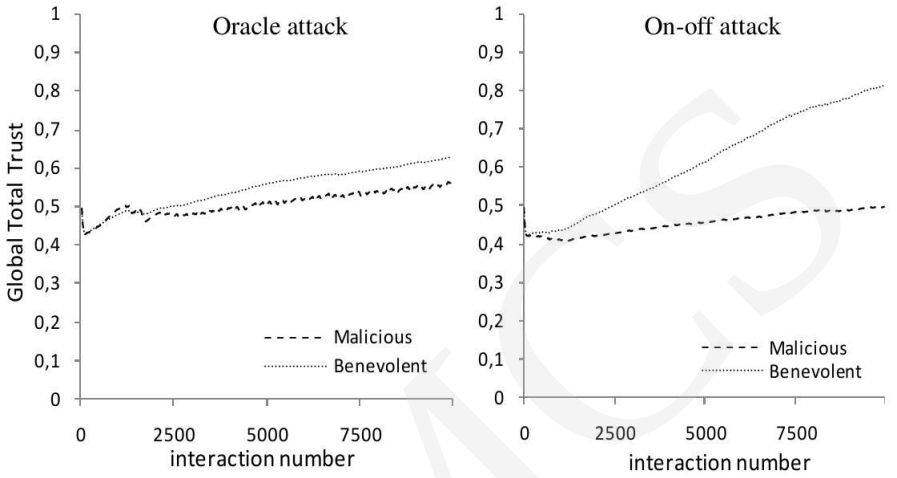

FIG. 4. Comparison of global total trust values ($TT^t_{G;M:B}$ *vs.* $TT^t_{G;B:B}$)

Comparison of global total trust of malicious nodes during the oracle and on-off attack is presented in Figure 5. As can be seen, malicious nodes performing the oracle attack have slighty higher reputation than the malicious nodes performing the on-off attack.

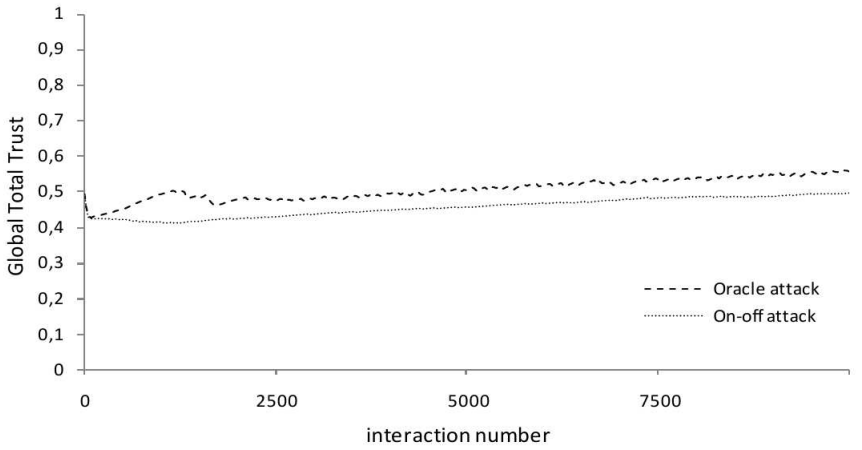

FIG. 5. Global total trust of malicious nodes ($TT^t_{G;M:B}$)

5 Summary and Future Work

As well as generally the Oracle attack is more efficient than the ordinary on-off attack as regards a number of unsuccessful interactions, this attack could be very dangerous in the case of new coming node to the network, which can be a frequent situation for example in the MANET networks. On the basis of high value of recommendation trust from other nodes, the oracles could effectively discourage these nodes from undertaking interactions with the new-comer node, which can lead to alienation of this node.

The conducted simulations assumed that 20% nodes in the network are malicious, also topology of the network used in the simulation was slightly artificial. Because of that the Oracle attack needs more profound research but even now it can be noticed that this type of attack can be a serious threat to trust management systems which do not implement sufficient countermeasures.

References

[1] Sun Y. L., Han Z., Yu W., Ray Liu K. J., Attacks on Trust Evaluation in Distributed Networks , Proc. Inf. Sci. Syst. Conf., 2 (2006): 1461–1466.

[2] Blaze M., Feigenbaum J., and Ioannidis J., The role of trust manage-ment in distributed systems security, in Secure Internet Programming, Springer-Verlag (1999): 185–210.

[3] Ganeriwal S., Srivastava M. B., Reputation-based framework for high integrity sensor networks, in Proceedings of ACM Security for Ad-hoc and Sensor Networks (SASN) (2004).

[4] Hoffman K., Zage D., Nita-Rotaru C., A Survey of Attack and Defense Techniques for Reputation Systems, ACM Computing Surveys, 42 (2009): 1–31.

[5] Kavitha T., Sridharan , D., Security Vulnerabilities In Wireless Sensor Networks: A Survey, J. Inform. Assur. Secur. (2010): 31–044.

[6] Padmavathi G., Shanmugapriya D., A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, International Journal of Computer Science and Information Security 4(2) (2009).

[7] Sun Y., Han Z., Ray Liu K. J., Defense of Trust Management Vulnerabilities in Distributed Networks, IEEE Communications Magazine 46 (2008): 112–119.

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

[9] Sabater J., Sierra C., Review on Computational Trust and Reputation Models. Artificial Intelligence, Artificial Intelligence Review, 24(1) (2005): 3360.

[10] Velloso P. B., Laufer R. P., Duarte O. C. M. B., Pujolle G., A Trust Model Robust to Slander Attacks in Ad Hoc Networks, IEEE International Conf. Comput. Commun. Netw. ANC workshop (2008).

[11] Sun Y. L., Han Z., Yu W., Ray Liu K. J., A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks, Proc. IEEE INFOCOM (2006).

[12] Sun Y., Han Z., Ray Liu K. J., Defense of Trust Management Vulnerabilities in Distributed Networks, Communications Magazine, IEEE, 46(2) (2008): 112–119.

[13] Gomez Marmol F., Martnez Perez G., Security threats scenarios in trust and reputation models for distributed systems, Computers &, Security, 28(7) (2009): 545–556.

[14] Zhang L., Jiang S., Zhang J., Keong Ng W., Robustness of Trust Models and Combinations for Handling Unfair Ratings, In Proceedings of the 6th IFIP International Conference on Trust Management (IFIPTM) (2012): 36–51.

[15] Sun Y. L., Liu Y., Security of Online Reputation Systems The evolution of attacks and defenses, IEEE Signal Processing Magazine, 29(2) (2012): 87–97.

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

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

[18] Yu Y., Li K., Zhou W., Li P., Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications (2011).

[19] Srinivasany A., Teitelbaumy J., Liangz H., Wuy J., Cardei M., Reputation and Trust-based Systems for Ad Hoc and Sensor Networks, In: A. Boukerche, Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks (2009): 375–404.