The Forming of Trust Level to the Nodes in the Distributed Computer Systems

Vadym Mukhin, Anton Bidkov, Vu Duc Thinh

Abstract - **This paper described the approach to the forming of the trust level for the Distributed Computer Systems (DCS) nodes, based on the analyzing of the dynamics of the processed information value changing**.

Keywords - **Security, distributed computer systems, nodes, trust level.**

I. Introduction

The security ensuring in a distributed computing environment is a very critical issue today. One of the important problems of safety mechanisms realization consists in the fact that in this environment every node can be added or excluded from the network at any time and there is absent the central control. [1]

Today, several trust and reputation models are suggested as part of solution of this problem. Also, there are known many methods and mechanisms such as fuzzy logic, Bayesian networks or bio-inspired algorithms, which allows manage and model the trust and reputation relations in distributed systems. [1] Anyway, the trust and reputation model should provide the mechanisms, allowing react on the all possible security threats.

II. Trust and Reputation Models

Most of the current trust and reputation models follow 4 main steps [1]:

- Collect information about nodes in the environment;
- Aggregate received information and compute trust level;
- Choose the most trustworthy or reputable peers for interaction;
- Realize the permanent adjusting of the trust level to nodes or their reputation.

Fig. 1 shows the main modern trust and reputation models for distributed systems.

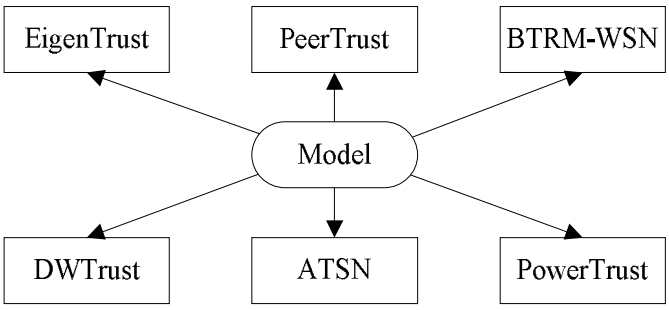

Fig. 1 The main modern trust and reputation models

Vadym Mukhin, Anton Bidkov, Vu Duc Thinh – National technical university of Ukraine "Kiev Polytechnic Institute", pr. Pobedy, 37, Kiev, 03056, UKRAINE, E-mail:mukhin@comsys.ntu-kpi.kiev.ua

III. Suggested Approach to Trust Level Forming

We suggest the approach to the forming of the trust level for the Distributed Computer Systems (DCS) nodes, based on the analyzing of the dynamics of the processed information value changing.

The trust level $Tn_i(t)$ to the i-th node taking into account the value of processed information is calculated as:

$$Tn_i(t) = Tn_0 * e^{\left(C(t)*\lg\left(\frac{N_{\lim}}{N_i(t)+1}\right)\right)} \qquad (1)$$

where: Tn_0 - the initial level of trust to the node, $C(t)$ – function-indicator of the information value on the time interval (0, t), $N_i(t)$ - the number of security incidents initiated by or associated with the i-th node at the time interval (0 , t), N_{lim} – the number of the critical incidents at the same time interval.

The information value is described as the discrete levels, for example, from 1 to 5 depending on the current requirements for the security level, and this value is changing dynamically.

The security incidents in DCS are divided into intentional and incidental. In general, the subjects of DCS and the nodes from which they are acting, can randomly performs the unintentional mis-actions, formally associated with an attempt to break the system security. The variation of N_{lim} parameter, which actually defines the maximum allowable number of the security incidents caused by accidental actions of the subjects, allows consider these cases.

So, the trust level Tn_i to i-th node during its functioning in DCS may be increased, decreased or remain constant. Thus, in the event when the number of security incidents $N_i(t)$, associated with the i-th node on the time interval (0, t) exceeds the critical number N_{lim} ($N_i(t) > N_{lim}$), then the trust level for this node is reduced, and if the number of incidents is less than N_{lim} ($N_i(t) < N_{lim}$), then the trust level to this node, on the contrary, is increased.

IV. Conclusion

The suggested approach to the forming of the trust level to nodes allows adaptively, during DCS functioning, define the most secured configuration of resources (DCS nodes) for the information processing, taking into account the dynamics of its value changing in time, thus enhancing the effectiveness of security systems for the DCS.

References

[1] F.G. Marmol, G.M. Perez, Security threats scenarios in trust and reputation models for distributed systems, *Trust and Reputation Management in Distributed and Heterogeneous Systems PhD Thesis*, pp. 98-109, April, 2010.