MACHINE TRUST MODELS

by Jan Eloff

Trust, by nature, is a human concept that relies on a way of thinking and perception. The question is:

"Can the human-to-human concept of trust be extrapolated to the concept of machine-to-machine trust?"

Fuzzy Cognitive Maps (FCMs) show potential for implementing a humanistic way of thinking about trust.

Trust is a vital ingredient of any successful interaction between individuals, among organisations and/or in society at large!

Several significant research contributions have recently been made in the field of human trust.[1,2,3,4] Important properties impacting on human trust were identified[5] it allows the reduction of complexity when decisions are made; it is measurable and evolves over time; it is dependent on a specific situation where risk is accepted when interactions occur. Furthermore it is concluded that trust in humans is based on two distinct components – knowledge and thinking.[5,6]

Amongst a myriad of other things, trust between humans and business organisations is determined by the interface between humans and the systems operated by business organisations, be they automated or manual. It is indicated in Johnston[7] that human computer interaction criteria such as aesthetic design and learnability contribute to an increased level of trust between humans and machines.

Trust relationships between organisations are, among others, influenced by culture and adherence to codes of best practices. A model of inter-organisational trust illustrates that trust is dependent on: competence, consistent positive behaviours and goodwill.[8] Machine-to-machine communications, such as in a web services environment, also influences trust relationships between organisations. This concept of machine-to-machine trust is new and has as yet not been resolved. It is hoped that some of the trust properties mentioned above can be successfully employed to improve the understanding of trust between machines.

The "Knowledge" component of trust

A comprehensive trust ontology is presented in Coetzee.[5] Three categories of concepts can be used to form trust. Firstly, a service provider (machine), must have knowledge regarding the publicly known properties of the service requester (machine) within which the trust relation needs to be established.[9] A service provider may trust others because of the knowledge that it has of the service requester. Finally, a service provider must have sufficient knowledge about itself and its own expertise. In summary, the three categories of trust knowledge as depicted in →1 constitute the foundation for the issues below that may play a role in the determination of trust between machines acting as service providers and service requesters respectively:

- Openness of the network topology used for communications between the service requester and the service provider
- Cumulative experience of previous transactions concluded between the service requester and the service provider
- Confidence of the service provider in its own operating environment
- Recommendations by and references from other entities who are trusting the service requester
- Security standards – technical and managerial standards adhered to by both the service provider and requester
- Complexity and type of service requested
- Security mechanisms implemented at the service provider.

The "Thinking" component of trust

Fuzzy logic[10] has proven itself as providing a connection between human reasoning and automated computer reasoning. Fuzzy Cognitive Maps (FCMs) show potential for implementing a humanistic way of thinking about trust.[11]

Consider →2, which depicts the Fuzzy Cognitive Map for establishing trust between a service provider (X) and a service requester (Y). Look at the relationship between C_6 and C_1. The minus 0.5 relationship between C_1 and C_6 implies, for instance, that if the Openness of the network topology was to increase, then the Trust between X and Y would decrease by 50%. If, by the same token, the Openness of the network were to decrease, then the Trust between X and Y would increase by 50%.

C_1 - Openness of the network topology used for the communications between X and Y

C_2 - Cumulative experience of transactions between X and Y

C_3 - Confidence of X in its own operating environment (platform)

C_4 - Recommendations / References – trust in entities that are supporting Y

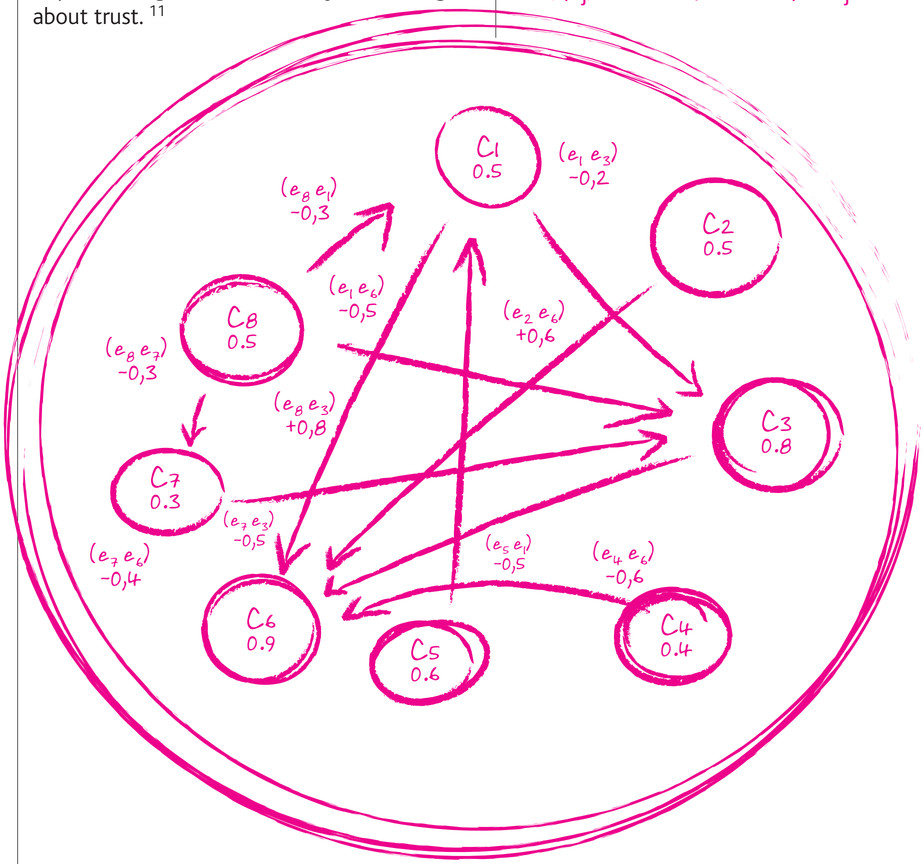
C_5 - Standards – technical and managerial standards adhered to by Y

C_6 - Trust_{xy} : machine X trusts machine Y

C_7 - Complexity and type of service at X requested by Y

C_8 - Security mechanisms implemented at X

(e_i,e_j) - Relationship between C_i and C_j



→ 2. FCM: Trust_{xy} - Service Provider X resolves it, Service Requestor Y can be trusted

In order for C_3 to occur, the incoming relationships must be aggregated to a minimum of 0.8. If, for example, a peer-to-peer network topology was used for the communications between X and Y (C_1 not triggered), if efficient security mechanisms were implemented (C_8 occurs), and if the service requested was of low complexity (C_7 not triggered), then the incoming relationship (e_8,e_3) needs to yield 0.8 in order for X to create a level of confidence in its own operating environment (C_3 occurs).

The FCM enables X to determine whether Y should be trusted. However, should X not trust Y two options exist – first, X could reject the request of Y and no further action is taken. Second, because of a potential loss in business opportunity, X may decide to make further investigations. Fuzzy dynamic systems, using edge matrixes, show the potential to assist X in determining how the causal events affect one another.

Consider the following example. What will happen if, for instance, the Service requester (Y) is able to use state-of-the-art standards that are acceptable to the Service provider (X)? This scenario is reflected in the FCM by switching event C_5 on. This input state can be represented by the state vector [0 0 0 0 1 0 0 0]. In order to model the effect of the input state I_0 = [0 0 0 0 1 0 0 0] on the FCM, the following technique[12] is used to determine the new state of each event Ci each time (t_{n+1}) an input state fires the FCM.

See below →3

This technique involves a matrix vector multiplication to transform the weighted input to each event C_i. In the above equation, S(x) is a bounded signal function that indicates whether C_i is turned off (0) or on (1). The equation (see below) is applied to the FCM with the following initial input state:

See below →4

where I_{0k} refers to the kth element in the state vector I_0 = [0 0 0 0 1 0 0 0]

e_{k1} refers to the entry in the kth row in the first column of the edge matrix E, and so forth. The above yields the following result:

$$\xrightarrow{0.5} I_1 = [0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]$$

The arrow represents a threshold operation. This means that event C_3 is turned on, indicating that the confidence that X has in its own operations should not be negatively influenced by the openness of the network. The negative impact of the openness of the network is minimised by event C_5, which signifies that the service requester (Y) is using acceptable standards, thereby reducing the risks of communications over an open network.

The next input state firing the FCM will therefore be I_1 = [0 0 1 0 1 0 0 0], followed by I_2 = [0 0 1 0 1 1 0 0], which yields I_3 = [t0 0 1 0 1 1 0 0]. Because $I_3 = I_2$, the FCM converges to a fixed point I_2 that turns on C_6 ("Trust XY").

What can be gleaned from this information? Remember that the fuzzy dynamic system is an executable component at the service provider. It was automatically determined that should the service requester adhere to improved standards, a level of trust could be established. As a direct consequence of this, the service provider can now start a process of real-time negotiation with the service requester. The service requester may be asked to use the AES standard as opposed to the DES standard.

Conclusion

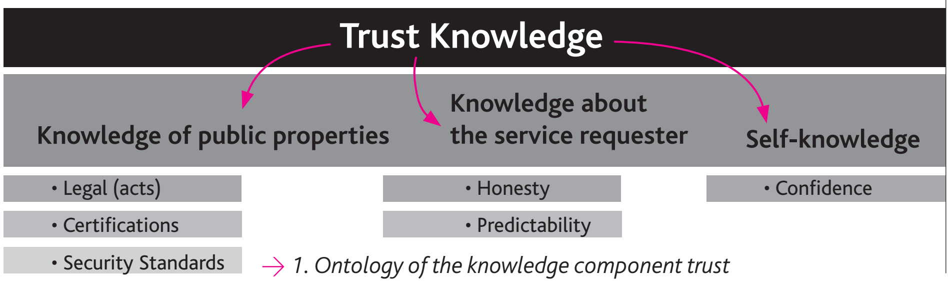
Human trust models are widely reported on in a plethora of current literature. Concepts such as experience, honesty and self-confidence have an important impact on establishing human-to-human trust. It is demonstrated in this paper that advanced human thinking on trust also has the potential to contribute to the establishment of a trust relationship between machines. Fuzzy Cognitive Map modelling provides for an elegant first attempt at implementing a trust model that balances the acts of human thinking and machine reasoning.

$$Ci(t_{n+1}) = S\Big[\sum_{k=1}^{N} e_{ki}(t_n)C_k(t_n)\Big] \text{ where N is the number of nodes in the FCM.}$$

→3

$$I_0E_c = \Big[\sum_{k=1}^{8} I_{0k}e_{k1}, \sum_{k=1}^{8} I_{0k}e_{k2}, \sum_{k=1}^{8} I_{0k}e_{k3}, \sum_{k=1}^{8} I_{0k}e_{k4}, \sum_{k=1}^{8} I_{0k}e_{k5}, \sum_{k=1}^{8} I_{0k}e_{k6}, \sum_{k=1}^{8} I_{0k}e_{k7}, \sum_{k=1}^{8} I_{0k}e_{k8}\Big]$$

→4



→ *1. Ontology of the knowledge component trust*

Bibliography

1. Marsh, S., 1994, Formalising Trust as a Computational Concept, PhD Thesis, University of Stirling, UK.

2. Deutsch, M., 1962, Cooperation and Trust: Some theoretical notes, in Nebraska Symposium on Motivation, M. R. Jones (Ed.), Nebraska University Press.

3. Luhman, N., 1979, Trust and Power, Wiley.

4. Gambetta, D., 1988, Can We Trust Trust?, chapter 13, pages 213-237. Basil Blackwell. Reprinted in electronic edition from Department of Sociology, University of Oxford.

5. Coetzee, M., Eloff, J.H.P., 2005, "Towards Web Services access control," Computers and Security, Vol. 23, No. 7, Elsevier Publishers, UK.

6. Castelfranchi, C., Falcone, R., 2004, Social Trust: "A Cognitive Approach," in Trust and Deception in Virtual Societies by Castelfranchi C. and Yao-Hua Tan (eds), Kluwer Academic Publishers, pp. 55-90.

7. Johnston, J., Eloff, Labuschagne, L., J.H.P. 2003, "Security and human computer interfaces," Computers & Security, Vol. 22, No. 8, pp. 675-684, December.

8. Ratnasingam, P.P., 2001, Interorganizational trust in Business to business e-commerce, PhD thesis, Erasmus University Rotterdam.

9. Chervany N.L. and McKnight D.H., 1996, The meanings of trust. Technical Report 94-04, Carlson School of Management, University of Minnesota.

10. Kosko, B., 1997, Fuzzy Engineering, Prentice Hall, Upper Saddle River, N.J., p. 549.

11. Falcone, R., Pezzulo, G., Castelfranchi, C., 2002, "A Fuzzy Approach to a Belief-Based Trust Computation," in Trust, Reputation and Security Theory and Practice, Bologna, Italy, July, Lecture notes in Computer Science, Vol. 2631.

12. Kosko, B., 1986, Fuzzy Cognitive Maps, International Journal of Man-Machine Studies, Vol. 24, pp. 65-75.

Further reading

Eloff, J.H.P., and Granova, A., 2003, Computer Crime Case Analysis, Computer Fraud & Security October, ISSN 1361-3723, Elsevier Advanced Technology.

Eloff, J.H.P., and Smith E., 2000, "Cognitive fuzzy modeling for enhanced risk assessment in a health care institution." IEEE Intelligent systems & their applications, Vol. 15, No. 2, pp. 69 -75. Newsweek, 2005, Indeed We Trust, February 5.

***Professor Jan Eloff**, Head: Department of Computer Science, University of Pretoria.*

jan.eloff@up.ac.za