Initially Cognitive Computation with Self-Organization Strategy for Securely Humanized Human-Machine Interactions

Charles Z.-Z. Liu, *IEEE, Member*
Charles Laboratory, Justtide Tech Co.,Ltd.
Email: chlsl@yahoo.com

***Abstract*—This brief paper addresses the issue of human machine interaction with consideration of security and humanization both. Initially Cognitive Computation (ICC) has been proposed and described with an illustration combining with a surveillance ICC framework with its application scene and process. Considering its diversity of devices and application involved with cloud computing with sophisticated configuration for networking in pervasive computational networked system, we further consider the autonomy and security of the systematic materialization that is in need of flexible configuration and proposed a self-organization strategy with security authentication in duration of trustworthy connection establishment.**

keywords: ***human-machine interactions, initially cognitive computation, humanization, security, self-organization, cloud***

I. Introduction

With the development of pervasive computing and ubiquitous network, rapid growth of information system accompanied with its various devices leads to the wide penetration of Human-Machine Interactions (HMI). It is not surprised that interaction with ATM, Kiosk to perform financial and merchandize transaction, or PDA, smart-phone Web-browser terminal to perform commercial activity. Humanization is one of its most significant content of HMI but also primary symbol of smart functionality to embody intelligence. It is mainly reflected as that the machine or computer system is capable of adapting to habits and instinct of human—the initiative subject in interaction so as to bring the anthropomorphic experience of information exchanging to user and satisfy demand with heartfelt services. Besides aesthetic, it emphasizes more on the satisfaction of mental demand in spirit level. As a case in point, menu-driven touch screen pad with visual or voice cue would make user be inclined to be interested in the service. For a long time, works have been carrying out concentrated on graphic, model and operation to make it easier to use machine [1]–[7]. These works promote the experience of interaction and are more mode of interaction while the forms of these are traditionally classical.

Most classical HMI are relatively passive compared to human to human interaction. A typical procedure is that user to be served inputs the information in specified format according to the cue displayed by machine to perform a series of necessary operations thus completing authentications, confirmations, services in business. This passive routine process constraints the efficiency of services and limits its quality in terms of effectiveness and humanization experience. For one thing, a manifest aspect is it takes up much time during cue and input procedure in serial interaction form that triggering and responding like tennis. For another, modern computer system have provide many auxiliary functionalities such as input/output in recording procedures in service, analysis on data and visualization with marked characteristics. However, as for computer has no concept about operator so as to do not know who are interacting with and what is significant or useless for service objective. What it did is just a routine thus rendering these auxiliaries passive and stylized stereotypes. It is administration sides, including administrators, decision-makers, operators, that is not excluded when they perform task by interaction with computation system, in which mangers are in need of being suffer the same lifeless experience as users as initiative subject, even more boring. Therefore, it can be seen that passive interaction in routine limit the efficiency of service and quality of humanization experience. What is more, there exist risks with respect to information security and operation safety in this passive interaction. Due to the aforementioned blindness of machine to user, computing system fail to recognize the operator comprehensively that objects can be authenticated as legal user and be enabled to command the machine to execute operations to perform the desired tasks as long as he or she provide correct input thus rendering back door for identity theft, illegal intruder, malevolent attack and other improper operation that undermine security and stability of the system.

Thus, to our best knowledge, it is reasonable to confer machine higher ability for cognition thus providing security guarantee and humanization experience for interaction. Thus we carry out the research on initial cognition strategies and technologies and proposed a framework for human secure interactions. In this brief paper, systematic framework and relevant strategies are describe. Initial cognition Framework for secure humanized interaction and its self-organization strategy are proposed and stated in details in section 2 and section 3 respectively. In section 4, challenges for further research are identified and conclusions are drawn.

II. Initially Cognitive Computation

According to the aforementioned analysis on traditional interaction, it can be seen that one of the significant reason leads to the degrading humanization experience and security is lack of cognition to environment, operators and the relationship between the desired services and the executed operations. Thus technology that enable computational system to be capable of initially cognitive sensing is needed to perform efficient service with securely humanized interaction.

Distinguished with classical interaction, the proposed initially cognitive computation (ICC) is a smart interaction mode with active cognition and assessment carried out before the procedures in service on with advanced visual sensing, acoustic sensing and other smart measurement direct at the specific target in scene, in which recognition of object including both user as human and devices as machine, understanding implication of information with respect to sensing including vision, audition and other physics, judgement on behaviors and operations thus capturing and assessing attempts and target task are critical for humanization interaction on account of that it is accurately cognise environment and user that make it possible for machine to understand and consider the task it need to perform and is executing thus initially matching the user's demands. For one thing, it provides support of humanized experience for interaction and decision making in services. As for computational system, ICC contributes to understanding the demand of user thus delivering initial inquiry or pushing desirable or potentially required services as responding before ask rather than passive carrying out services by means of tennis like input and respondence according to displayed cues so as to make the services more socially humanized interaction than stylized stereotype of routine. For another, ICC extend and strengthen the ability of protection for system safety. With the support of ICC, computational system pre-cognises the scene and users even before carry out the task, which means the range of interaction is expanded beyond service. As a case in point, framework of ICC with surveillance support is designed and illustrated in Fig.1, in which the main process of this system can be described as following:

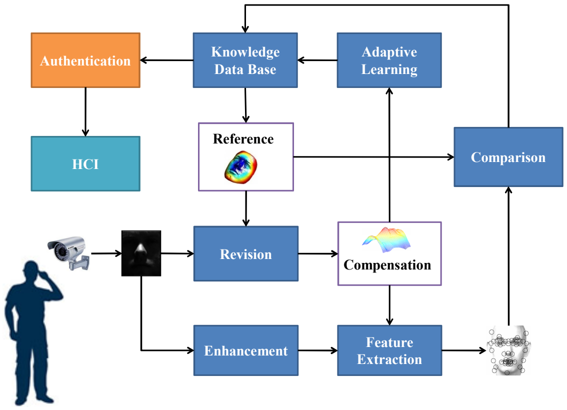

Fig. 1. A Surveillance ICC Framework

1) when a person come into valid area, system acquires information of the target by visual sensor (represented as camera in the figure);
2) the information is conveyed to the modules with respect to revision and enhancement respectively to perform preprocess refine the relevant information;
3) with the reference model and compensation, the accuracy and volume of information is fostered thus providing refined materials for feature extraction so as to abstract out the significant characteristics;
4) comparing the extraction result with reference model to perform matching and calculating the residuals;
5) convey the result of comparison to knowledge base and perform the identification authentication and behavior assessment with judgement rule in the base;
6) system makes the decision according to the authentication and assessment results so as to instruct HCI to respond;
7) each process is learned by system itself thus updating its capability and knowledge to perform the task better with the process on.

It can be seen according to the process described above, the risk of system safety has been reduced since the identification authenticating is performed once the initiative subject step into the area of system surveillance before the essential services being carried out thus anticipating and pre-judging the security the subject and possible event involved with the behaviors so as to provide foresight for preventing appearance camouflage, masquerading attack and other anomalous events rather than aware afterward in classical interaction. As for surveillance with functionality of recognition, many works has been carried out in the past [8]–[11] and the relevant details will not go further into the matter in paper with the limits of space.

An inevitable issue is system configuration. The system, especially for autonomy ones that is in need of flexible configuration and accessible networking automatically, possesses sophisticated operation. It is costly and low efficiency to perform the configuration with human effort if the system is usually needed to re-configure particularly the ones with mobile devices and uncertain service scene. Meanwhile, cloud computing is one of the efficient but low cost alternatives to perform ubiquitous service, which can provide more flexible service that updating without modification service involved with devices, infrastructures and field construction. Configuration is also needed. Thus on no account can we ignore the significance of security in system configuration especially for self-configuration, and we further study the secure self-organization strategy for ICC.

III. Secure Self-Organization Strategy

Considering the sophisticated procedures of configuration, a self-organization strategy is needed to reduce the human effort and simplify the human involvement in process, especially for those extendable cloud with access to diverse devices in need of flexible configurations and seamless joints. We consider the system as a network and configuration as networking with self-organization process. As for self-organization strategy, many related works have been doing on WSN or Ad-hoc. [12]–[16]. In these works, nodes in network were set as unified units, function or performance of each node were simple and identical, and the nodes authorities were static in a certain long work period. However, units in large scale complex network are hybrid, such as AmI or IoT, which contains quantities of smart devices. Nodes with diverse performance and function can not be set unified with same authority, let along put the changeable situation into consideration. Therefore, networking should be give weight to diversity in such difference-reserving network.

In the meanwhile, it is the security of the communication in mode of M2M (Machine to Machine) such as networking and trustworthy connection establishment that taken into consideration as well to further strengthen the guarantee of security in flexibility performance, especially for autonomous system with unattended configuration and robustness to physical anti-attack, in which the main system function can be guaranteed even if several nodes lost function.

Hypothesizing under network scene N, each node $v_i \in V(N)$ is an agent with intelligence, where $V(N)$ is node aggregate of N. We divided intelligence level into A, B, C, D four level from high to low(see TABLE 1).

TABLE 1
INTELLIGENCE CLASSIFICATION

Classification		
class	level	description
A	advanced	capacity of perceive, complex inference with complex data structure
B	medium	capacity of computation and data processing with medium data base
C	simple	capacity of data store and auto-reaction with string stack processing
D	non	simple sensing and reaction data transmit and store with simple buffer

Assume properties region of each $v_i \in N$ is close, so is X_{v_i} for states and B_{v_i} for behaviors, where

$$\begin{aligned} P_{v_i} &= \{A, B, C, D\} \\ X_{v_i} &= \{x_1, x_2, \ldots\}_{v_i} \\ B_{v_i} &= \{b_1, b_2, \ldots\}_{v_i} \end{aligned} \tag{1}$$

Define operators $\hbar_1 : P \to R$ and $\hbar_2 : B \to R$, then the image of property and behavior in real number field can be acquired as W:

$$W = \{\hbar_1(P), \hbar_2(B)\} \tag{2}$$

Assume topology T is known, then it can be acquired that:

$$X_N = f(T, X, W) \tag{3}$$

Thus the scene can be modeling to instructs the systematic design including data organization, state and task definition, system operation, etc, with respect to interaction. The interactions are formulated as follow:

- source unit according to semantics (protocol) symbolize and encapsulate the information into data;
- sink unit decode the data and read information;
- each unit performs memorization and induction by information learning and interact with information stream exchanging;
- each unit process and update knowledge-base to perform evolution;
- according to a certain rule to judge, reorganize or refine some new information;
- directs at a specific problem or index re-exchanging updated information to perform consultation

Each unit can gradually acquire and adapt to network environment by learning from each other. Knowledge about environment is formed and memorized in whole network as entirety information. Whole strategy can be divided as three main phrases:

- Phrase1: Initialization, coding and addressing;
- Phrase2: Interaction, networking and pattern recognition;
- Phrase3: Organization, alliance forming and role assignment;

Information, such as IP, location, state and intelligence level, can be acquired via parsing operation. According to specific service, assume f_κ is parsing function, $Node_i.Address$ is the address of node i, then the correspondence service ID is:

$$\{Prog : ID | ID_i = f_\kappa^{-1}(Node_i.Address, X_{v_i})\} \tag{4}$$

Each ID_i contain two main identification information: $SegmentID_i$ and $NodeID_i$. Each node encapsulates identification together with node information into a IDpacket:

$$IDpacket_i = SegmentID_i \oplus NodeID_i \oplus Signaling_i \tag{5}$$

where $Signaling_i$ is a sub-packet including the content of node information, task command and service authority.

Life-period is adopted to describe the capability of data-drive. Nodes with different level set life-period according to service need. Correspondently, timestamp is attached to each packet. Source node i sends packet with REQ terminal authentic information frame to the nodes $v_{j|j\neq i}$ around within radius σ. Then v_j replies an frame ACK together with information encapsulation. At last, if a link can be build between v_i and v_j, an AFF frame will be resent mutually to affirm the link by update in routine table of both nodes.

In the system, four main patterns can be acquired by comparing self information with the received one after unpacking, which is $Local$，$Remote$，$Loop$ and $Error$, where:

- $Local$ means two nodes are with same sub-net location and reachable within local area;
- $Remote$ means nodes are located in different area and communicate with cross-area routine;
- $Loop$ means loopback existed in area;
- $Error_{ij}$ means error take place between the link or link is unreliable or untrustworthy.

Corresponding infer compute progress is:

$$PR_i(IDpacket_j) = \begin{cases} Local & C_1 \wedge C_2 \wedge C_3 \\ Remote & C_1 \wedge \bar{C_2} \wedge C_3 \\ Loop & \bar{C_1} \wedge C_2 \wedge C_3 \\ Error_{ij} & \bar{C_1} \wedge \bar{C_2} \parallel \bar{C_3} \end{cases} \tag{6}$$

where,

$$\begin{cases} \{C_1 : NodeID_i \neq Node_j\} \\ \{C_2 : SegmentID_i = SegmentID_j\} \\ \{C_3 : Signaling_i \Longleftrightarrow Signaling_j\} \end{cases} \tag{7}$$

and $\Longleftrightarrow$ indicates that the mutual authentication process is complete and valid that authentication information in signaling of node in pair is fit with each other thus regarding the nodes involved with the connection are legal. The patterns above are basic elements in recognition. More patterns that are complex can be derived from combination. Furthering learning process can discriminate network environment via tracking the loopback or unstable routine to support works follow-up, such as role assignment and intelligent alliance self-organization. And the node had stayed in pattern of $Error$ for a certain long period will be excluded from the connection and marked as suspicious device, whatever it is physical fault or illegal planted by intruder, so as to guarantee the absolute effectiveness of the system.

Combining with the security techniques as presented in [17]–[21], the strategy of self-organization can be embedded into various protocols such as ad-hoc, WiFi or bluetooth with both security guarantee and flexible networking.

Based on pattern elements $Remote$, $Local$, $Loop$ and $Error_{ij}$, role assignment can be acquired with rule (8),

$$Role_i = \begin{cases} Member & Local \\ Crosser & Local \wedge Remote \\ Frisby & Local \wedge Loop \end{cases} \tag{8}$$

Such role assignment can provide more support on smart-networking. For example, role $Crosser$ not only tend to be router but also would help to recognize the edge of cluster, which is important for communication and scheduling.

Based on role assignment, alliance division can be acquired with different selection rule. For example, consider space factor, the rule can be formulated as:

$$\begin{aligned} Union_a = \ & (Nodes|(Node_a \in Member) \\ & \wedge(\forall Node_i \in G(V,E)) \\ & \wedge(PR_a(IDpacket_i) = Local) \end{aligned} \tag{9}$$

if further put accessibility in to consideration, the rule is:

$$Union = \{\forall Nodes|(Nodes \in Member \wedge Frisby\} \tag{10}$$

With the interaction and exchanging, routine table is tending towards stability, which makes the dynamic linkages converge to a stable topology with correspoding configuration thus completing self-organization.

IV. Conclusion

In this paper, we introduce the original idea of ICC with comparison to classical interaction and surveillance framework as a case in point to describe its positive effect on promoting security and humanization. A secure self-organization strategy for autonomous configuration is proposed with consideration of security. In future works, much weight will be given to ICC's performance involved with machine learning, information security in untrustworthy channel and its cloud computing application in SaaS, IaaS and PaaS mode.

References

[1] John M Carroll. *HCI models, theories, and frameworks: Toward a multidisciplinary science*. Morgan Kaufmann, 2003.

[2] Veysel Demir, Atef Elsherbeni, Denchai Worasawate, and Ercument Arvas. A graphical user interface (gui) for plane-wave scattering from a conducting, dielectric, or chiral sphere. *Antennas and Propagation Magazine, IEEE*, 46(5):94–99, 2004.

[3] Wade K Copeland, Vandhana Krishnan, Daniel Beck, Matt Settles, James A Foster, Kyu-Chul Cho, Mitch Day, Roxana Hickey, Ursel ME Schütte, Xia Zhou, et al. mcagui: microbial community analysis r-graphical user interface (gui). *Bioinformatics*, 28(16):2198–2199, 2012.

[4] Daniele Silvestro and Ingo Michalak. raxmlgui: a graphical front-end for raxml. *Organisms Diversity & Evolution*, 12(4):335–337, 2012.

[5] Milan Gnjatović, Marko Janev, and Vlado Delić. Focus tree: modeling attentional information in task-oriented human-machine interaction. *Applied Intelligence*, 37(3):305–320, 2012.

[6] Ishan Banerjee, Bao Nguyen, Vahid Garousi, and Atif Memon. Graphical user interface (gui) testing: Systematic mapping and repository. *Information and Software Technology*, 2013.

[7] Janna Protzak, Klas Ihme, and Thorsten Oliver Zander. A passive brain-computer interface for supporting gaze-based human-machine interaction. In *Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion*, pages 662–671. Springer, 2013.

[8] Ahmed Elgammal, Ramani Duraiswami, David Harwood, and Larry S Davis. Background and foreground modeling using nonparametric kernel density estimation for visual surveillance. *Proceedings of the IEEE*, 90(7):1151–1163, 2002.

[9] Sven Bolte and Fritz Poustka. The recognition of facial affect in autistic and schizophrenic subjects and their first-degree relatives. *Psychological medicine*, 33(5):907–915, 2003.

[10] Gabriele Sachs, Dorothea Steger-Wuchse, Ilse Kryspin-Exner, Ruben C Gur, and Heinz Katschnig. Facial recognition deficits and cognition in schizophrenia. *Schizophrenia research*, 68(1):27–35, 2004.

[11] Dimitrios Makris and Tim Ellis. Learning semantic scene models from observing activity in visual surveillance. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 35(3):397–408, 2005.

[12] S. Basagni. Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks. *Proceedings of the IEEE 50th International Vehicular Technology Conference (VTC'99)*, 2:889 – 893, 1999.

[13] G. Chen, F. Nocetti, J. Gonzalez, and I. Stojmenovic. Connectivity-based k-hop clustering in wireless networks. *in Proceeding of the 35th Annual Hawaii International Conference on System Sciences(HICSS'02)*, 2002.

[14] M. Chatterjee, S.K. Das, and D. Turgut. Wca:a weighted clustering algorithm for mobile ad hoc networks. *Cluster Computing Journal*, 5.2:193 – 204, 2002.

[15] A. Desmet, F. Naghdy, and M. Ros. Embedding distributed learning algorithms in wireless ad-hoc control networks. *Intelligent and Advanced Systems, 2007. ICIAS 2007*, pages 338 – 342, 2003.

[16] C. Muldoon, G.M.P. O'Hare, M.J. O'Grady, and R. Tynan. Agent migration and communication in wsns. *Parallel and Distributed Computing, Applications and Technologies, 2008. PDCAT 2008*, pages 425 – 430, 2008.

[17] Dirk Balfanz, Diana K Smetters, Paul Stewart, and H Chi Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *NDSS*, 2002.

[18] Srdjan Capkun, Levente Buttyán, and J-P Hubaux. Self-organized public-key management for mobile ad hoc networks. *Mobile Computing, IEEE Transactions on*, 2(1):52–64, 2003.

[19] Long Hoang Nguyen and Andrew W Roscoe. Authenticating ad hoc networks by comparison of short digests. *Information and Computation*, 206(2):250–271, 2008.

[20] Long Hoang Nguyen and Andrew William Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey. *Journal of Computer Security*, 19(1):139–201, 2011.

[21] Namakkal S Sambamurthy and Parathasarathy Krishnan. Methods and systems for securing data by providing continuous user-system binding authentication, August 8 2013. US Patent 20,130,205,410.