A Graph-based approach to address trust and reputation in ubiquitous networks

Valentina Viduto, Paul Townend, Jie Xu,
Karim Djemame,
University of Leeds
Leeds, United Kingdom
e-mail: v.viduto@leeds.ac.uk

Alexey Bochenkov
Birmingham City University
Birmingham, United Kingdom
e-mail:alexey.bochenkov@bcu.ac.uk

Abstract— The increasing popularity of virtual computing environments such as Cloud and Grid computing is helping to drive the realization of ubiquitous and pervasive computing. However, as computing becomes more entrenched in everyday life, the concepts of trust and risk become increasingly important. In this paper, we propose a new graph-based theoretical approach to address trust and reputation in complex ubiquitous networks. We formulate trust as a function of quality of a task and time required to authenticate agent-to-agent relationship based on the Zero-Common Knowledge (ZCK) authentication scheme. This initial representation applies a graph theory concept, accompanied by a mathematical formulation of trust metrics. The approach we propose increases awareness and trustworthiness to agents based on the values estimated for each requested task; we conclude by stating our plans for future work in this area.

Keywords- trust; reputation; virtual computing environment; ubiquitous computing; graph theory;

I. INTRODUCTION

Pervasive computing systems, distributed systems, and associated interoperability technologies such as virtual computing environments have enabled embedded control and information systems to be penetrated into the ordinary objects and processes surrounding us in everyday life. Such environments allow users to interact with computing systems without explicit or even unrealized instructions, decisions and natural convenience. As suggested in [1], an agent defined as a peer, network node or a server should be capable of making decisions about actions without referring to its user, in order to meet its owner's objectives and be reactive in the sense of responding to the prevailing circumstances in unpredictable computing environments. However, to achieve this, a designer is expected to define an applicable approach of coordinated interactions between agents. This then will specify how one agent will communicate with another agent under specific context. This approach is normally both technically and technologically comprehensive, and thus does not have an appropriate enough level of flexibly due to the large variations in the designs of distributed systems, as well as their accessibility, interoperability and compatibility.

The reputation, of an embedded system within a virtual computing environment (VCE) such as a Cloud tends to be considered from the very core concept where an intelligent agent – an atomic component block – delegates some tasks to a target agent, in order to achieve an ultimate goal for the benefit of the VCE. Reputation is defined as a level of trust developed over time. Agent communications can be explored from both homogeneous and heterogeneous points of view. Therefore, heterogeneous applications may consist of a number of agents extending the complexity of such interactions between them. This complexity, and the comprehensive nature of VCEs, represents a challenge how one agent discovers and accepts services from unknown agents, while considering unknown agent's interaction history as a source to build a reputation [2].

As pointed out by the authors in [3], trust is conceptually classified in dispositional, situational, structural, trusting belief and trusting intention categories, depending on the type of trust existing between two or more entities. At the same time, to shift VCEs to a new revolutionary level, trust has to be transformed into reputation, representing a more advanced level of interaction between agents. The main challenge in the VCE context is to distinguish the intentions of the participating agents, and to identify which are contributing to achieving the ultimate goal in the open pervasive environment.

Since pervasive and distributed computing technologies are already embedded into our everyday activities, we have become more and more dependent from them. The level of information processed is so high, and network communications so intensive, that it creates an unprecedented challenge to assure users about reputation level associated with a service provided by a particular agent.

Recent research and development in this area have been mainly focused on various trust models and their applications for particular environments or specific use-cases. It is notable that often, trust is being treated as a local phenomenon rather than evaluated to a reputation level where it encompasses whole systems and takes into consideration a provenance aspect. The authors in [4] make an attempt to extended trust to global phenomenon via a graph theoretic approach. However, the limitations of this approach do not allow researchers and practitioners to create a non-static model, whilst the agent interaction process is highly dynamic.

Therefore, to move the state-of-art further, we introduce trust as a function of time to authenticate, quality of a task and reputation level, as a global phenomenon. This means that a VCE will educate itself over time, and increase

artificial intelligence capability built into regular interactions. Also, we propose agent authentication, trustworthiness, and Quality of Task (QoT) based on ZCK authentication scheme, as an integrated part of the reputation scheme.

This paper is structured to allow a clear view and easy understanding of this concept. In Section 2 we discuss computational trust and reputation models, and how agents interact within the dynamic VCE in order to provide a requested service to a user. The information security aspects of ubiquitous networks as well as the ZSK authentication scheme are reviewed in Section 3. A graph-based theoretical approach to introduce trust and reputation relationship and to formulate it as a function is presented in Section 4. Our initial results to demonstrate the logic behind the approach proposed are discussed in Section 5, and Section 6 concludes our research findings.

II. Computational Trust and Reputation Models

It is a widely acknowledged fact that the pervasiveness of distributed systems raises a set of issues in relation to fundamental security aspects, such as trust, confidentiality and privacy. To address these challenges, a new field referred to as computational trust has been developed [5]. Computational trust has been inspired by the human perception of trust, and the freedom of intermediate agents to make decisions. Therefore, the reputation of these agents plays an important part in designing trust. The main sources of information used to design trust and reputation models are direct experiences and provenance information (defined as the documentation of a process that leads to a result) from a third party agent. Some authors argue that a good mechanism to increase the efficiency of trust and reputation models is to introduce a sociological aspect; it is also argued that this kind of sociological information would necessarily be more useful than just taking into account direct experiences [5].

The authors in [6] argue that many computational trust models have been proposed without clearly highlighting if they can be adopted in a particular environment. In order to address trust issues, it is necessary to analyse actual system behaviour, and software and/or hardware specifications. Computational trust and reputation models deal with the decision making often performed by computational agents in the presence of pervasive, unknown, and user uncontrollable entities. Therefore, designing trust and reputation models is hard because of the notion of trust that humans perceive from a sociological or physiological point of view. The authors in [5] propose that trust and reputation models can be characterized as:

- Cognitive. At the same time it was stressed that models based on a cognitive approach 'trust and reputation are made up of underlying beliefs and are a function of the degree of these beliefs'[7]. Therefore, in the cognitive approach, the mental states that direct to trust another agent or assign a reputation, as well as the associated mental consequences of this decision and the act of relying on another agent, are an essential part of the model.
- Game-theoretical. According to [8], trust and reputation are considered 'subjective probabilities by which an individual A expects that another individual B performs a given action on which its welfare depends'. As a consequence, trust and reputation are not the result of a mental state of the agent in a cognitive sense, but the result of a more pragmatic game with utility functions and the numerical aggregation of past interactions.

Computational models can also be classified as credential or experience based. Credential-based and experience based computational trust models are complementary, and address the same problem of establishing trust among interacting agents in distributed and decentralized VCEs. However, they have different assumptions.

Credential-based computational trust management systems are designed to manage a static trust originating from certificate authorities or by the use of digital certificates. A trust decision normally relies on policies or a set of strictly specified credentials. The first prototype of such a trust management system was PolicyMaker [3]. PolicyMaker represents a query engine that checks whether a requested action and the credentials supplied by the requested party match local security policy. A REFEREE is another trust management system, which makes access control decisions relating to web documents [9]. The associated limitations of such solutions are that they can only address a problem of dynamic trust adapting to the changing environment and situations.

Experience-based trust is developed to analyse historical behavior and also reputation gained while interacting with other agents, entities and VCEs. At the same time, probabilistic approaches have focused on probability and Bayesian theories to predict the likelihood of the interaction outcomes. A distributed reputation system proposed in [10] is based on a notion of belief theory, where an agent builds a local or total belief by interacting with other agents. Total belief is used to decide whether a correspondent is trustworthy, whilst local belief comes from direct interactions with the correspondent; this belief can be propagated upon request. The goal of probabilistic approaches is to predict the behavior of principals in future interactions while knowing their behavior in past interactions. Some other models that must be considered to create an overall picture belonging to experience-based computational trust are:

(1) TRAVOS (Trust and Reputation system for Agent Based Virtual Organisations) use probability and Bayesian theories to represent values of trust regarding future actions an agent may consider [11]. This model evaluates a reputation source based on previous experience, and a trustee is assessed based on present behavior and reputation. The trustor takes decisions based on a confidence level but not based upon a trust value - therefore, the reputation of agents is identified via a highest confidence level. If an agent cannot get enough confidence, then it searches for some evidence from a third party. In other words, such a model identifies two major information sources: the immediate experience of

a trustor and a trustee, and third party experience with a trustee supported by references from other peers.

(2) Marsh's model [12] was one of among first models to formalise the human notion of trust in computer science. Trust aspects pulled into the model were borrowed from sociology and psychology; this explains a reason why trust formalism has strong sociological foundations. Additionally, this model was based on basic linear mathematics, which provided an ideal tool for agents in making decisions about the environment they operate in.

III. ZERO COMMON-KNOWLEDGE AUTHENTICATION

Ubiquitous networks have one fundamental characteristic: ubiquitous systems can be accessed by multiple users simultaneously, formulating a group of peers sharing then same resources. This type of functionality introduces potential risks, as vulnerabilities can be presented on agents and hosts that participate in the communication network. Security in distributed, ubiquitous networks is an area of great attention where security aspects of confidentiality, integrity and availability should be addressed.

One of the attempts to address security aspects in pervasive, ad-hoc, ubiquitous networks has been to implement an authentication scheme, referred to as Zero Common-Knowledge (ZCK). In [13], the authors highlight that if there is no predefined relationship between two entities in multi-agent systems (such as VCEs), trust as a function cannot be established. The security objective is addressed in a following manner: consider that A is able to authenticate B by ZCK fashion if A is able to identify the authority that runs B, and B is able to convince A that both had some previous experience and some relationship in the past [13]. This concept clearly outlines the need for reputation when considering VCE systems. It also should be noted that within the proposed authentication scheme, the authors followed an infrastructure-less approach where there is no centralised control and ZCK authentication consists of weak peers without pre-established secrets regarding security mechanisms applied. Therefore, ZCK authentication requires only one-way hash functions, which are well suited for weak peers. The framework of trust is based on the identification of an agent relying on a previous transaction even through an insecure channel. Furthermore, the framework itself does not claim to address confidentiality or non-repudiation of multiple agents. Nevertheless, it can provide integrity through the proposed authentication mechanism, which has been proven to be computationally inexpensive with very low bandwidth and memory requirements compared to PKI and other symmetric schemes.

As suggested by the authors in [14], Peer-to-Peer (P2P) systems might compromise users' privacy, and highlights that a large number of concerns have been raised about the issue of providing authentic resources in P2P [14]. The issue with authentication lies in the concept that agents and hosts must know the identity of each other, and therefore there is no space for anonymity. That means that trust becomes a personal attribute of an agent or host, strongly linked to its identity. This fact creates an additional level of vulnerability for a system, since identity replication is a common tool being exploited to break in to systems. A possible solution to solve this issue was introduced in [14]. The authors addressed this by designing a Pseudo Trust protocol in which each peer generates an unforgettable and verifiable pseudonym using a one-way hash function. The advantage of this protocol is that trust becomes a transferable attribute, which supports anonymity. At the same time, it creates an additional issue to control that pseudonym validity. The next step in this development has been to combine the Pseudo Trust protocol with the Zero-Knowledge authentication approach to facilitate authentication of unknown agents and hosts, therefore identifying trust levels whilst maintaining anonymity for both peers.

IV. GRAPH THEORETICAL APPROACH

Graph-based theory has been widely applied to visualise, represent many computer science problems. In this paper, we use a concept of trust and reputation graph to visualise the relationship between a local human and an agent in the global network of pervasive systems. We assume that a human has got some level of trust in that agent based on previous transactions and previous experiences, and that therefore a human can delegate confidential information to an agent. Nevertheless, the agent further processes a human's query and passes it to another agent within a global network.
Let G denote a trust graph, W(G) denotes a vertex set and E(G) the edge set of the trust graph G: G(W,E).

The vertex W consists of a set of agents A, thus A = {a1, a2, ... a_n} and a human H, i.e. W = H U A. We consider agents as computerized entities that can independently on behalf of a human in the global VCE. The edge e ϵ E of a a direct trust graph G is represented as an ordered pair (k, u), where k ϵ W and u ϵ W , meaning that an agent trusts another agent based on the previous experience. k is the initial vertex and u is the destination vertex.

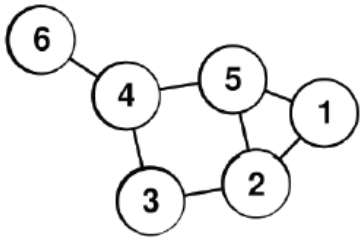

Figure 1: General representation of graph

Figure 1 represents a ubiquitous, complex environment of agents, where a vertex set

W= {1,2,3,4,5,6}

links agents, and an edge set

E = {{1,2},{1,5},{2,3},{2,5},{3,4},{4,5},{4,6}}

shows a direct link between two agents, who have gained some level of trust and reputation based on the previous experience.

Figure 2 shows a sample trust graph with a single human agent H and a set of multi-agents $A = \{a1,a2,\ldots,a_n\}$. The graph represents a delegate authority to perform a task to an agent a1, who further passes the same task to other agents within the network. At this point, we assume that agents within the global, ubiquitous environment interact with each other through transactions or tasks. Further, within the paper we will stick to using a term task. These tasks include various activities, such as retrieving information, downloading, uploading files to/from a server or any other requests initiated by the human. It should also be noted that the relationship between a human and a local agent is bi-directional, as both parties should be authenticated to each other.

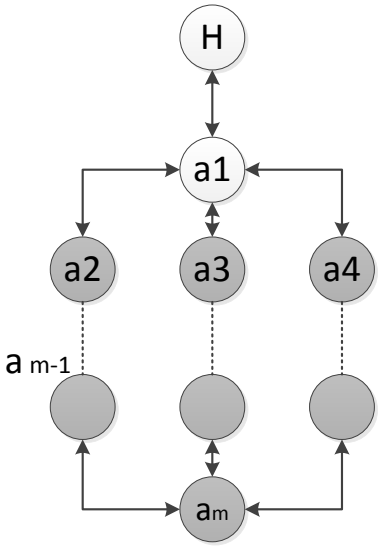

Figure 2. A graph of trust from local to global view

We consider a reputation as being an important aspect to be considered when delegating information to other agents. Therefore, we visualise two types of edge in the trust graph: firstly, task edges t_{am} to represent a request passed from one agent to another within a global network; and secondly, reputation edges R_{am}, to represent a level of reputation an agent-to-agent relationship has. The task from human H to an agent a1 contains request details, e.g. retrieve, store, upload; time a task was initiated, location, amount of data transmitted and network behavior information. In addition to the task edge, a reputation edge from H to a1 represents the reputation level, quality of service provided based on previous and current experience.

Figure 3 shows a visualised view of agent-to-agent and human-to-agent interactions, while delegating tasks and reputation from local to global view. An initial interaction starts from a human H to a local agent a1, which then passes the task (solid edges) to agent within the network knowing its reputation (dashed edges).

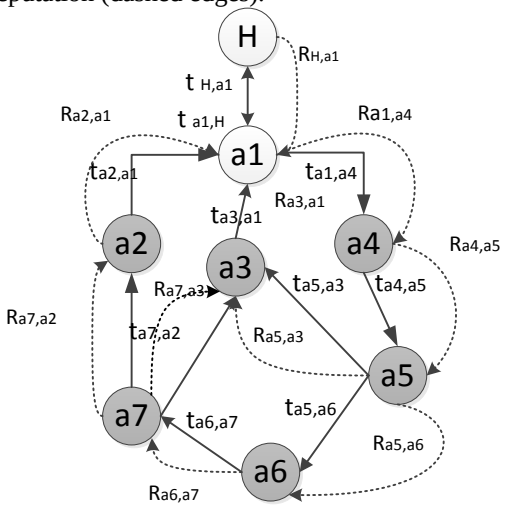

Figure 3. Example of a task, reputation edges from local to global network

V. TRUST AND REPUTATION MATHEMATICAL VIEW

Despite the fact that our model is based on a graph theoretical approach, we have mathematically expressed trust as a function of time required to authenticate each agent-to-agent and human-to agent relationship, while applying the ZCK authentication mechanism and agent experience as a reputation gained through previous experience in dealing with a task.

Therefore, we have assumed that trust in agents strongly relates to the reputation level R that a particular agent has gained while completing a requested task. Additionally, considering a reputation edge between agents we have introduced a new metric to represent a quality of completed task, defined as Quality of a Task (QoT), which contains data such as time required to respond, response messages, and feedback. These parameters are important while building reputation in an agent. Based on this metric, the system is educating itself over time and creates artificial intelligence built in regular interactions within the complex environment. Quality of a Task (QoT) can then be expressed as [0,1], where 1 is the maximum possible quality for a specific task and 0 is the quality for an unfeasible task. This certainly is possible if network conditions do not allow any communication to take place or no task is initiated. It should be noted, that the quality of a task can be affected by factors such as network conditions at a time of a request initiation, number of agents within a system or number of nodes and distance between them. The longer the distance between

nodes, the longer the response time will be recorded. Combining these metrics, the reputation R for an agent a_i regarding a particular task performed by an agent can be defined as follow:

$$R_{a_i} = \frac{QoT a_i}{T_{a_i}} \qquad (1)$$

Where $QoT_{a_i} \in [0,1]$ – is the quality of a task for a specific interaction for agent a_i, and $T_{a_i} \in [1,2 \dots n]$ is a number of authentication hops in the path between agents or host that initiates a task. Based on Eq.(1) it can be seen that the reputation of an agent can be dramatically reduced when the number of authentication hops in the network is increased. We have made an assumption that as the number of agents in the path increases, this will unavoidable reduce the reputation R of an agent performing a task. The assumption is supported by the fact that as the authentication time and the number of authentication hops present on a path increase, the possibility for a security breach, such as the one related to DoS or Brute Force attack, also increases.

Therefore, the overall trust τ a human agent places in a complex VCE system consists of a product of reputation levels between multiple agents which interact from task request to task delivery and a number of agents in a path. Thus, we have:

$$\tau_H = \frac{\prod_{i=1}^{m} R_{a_i}}{n_i} \qquad (2)$$

Additionally to the formulation above, trust can be seen from a global perspective, considering a distance between these agents/nodes/hops as the request is passed to the global system from a local network. Thus, the Eq. (2) can be transformed as follows:

$$\tau_H = \left(\frac{\prod_{i=1}^{m} R_{a_i}}{n_i}\right) - k(d) \qquad (3)$$

Where k is the distance between agents in the graph and d is some constant, n_i is the number of agents in the task path.

Further in our theoretical graph approach we have calculated the average trust τ_{avg}. An average trust τ_{avg} is important when considering an adaptive and dynamic nature in path selection or mobility of agents in and outside the domain.

This metric can provide a single value of trust for a specific task and with the task associated agent reputation based on the path, location etc. Therefore, the average trust can be mathematically expressed as follows:

$$\tau_{avg} = \frac{\prod_{i=1}^{m} R_{a_i}}{T_{a_i} \cdot n_i} \qquad (4)$$

VI. RESULTS AND FUTURE WORK

In order to demonstrate the performance of the model we randomly generate three tasks and associated quality of a task, and a number of authentication hops. Authentication time T in the graph (Figure 4) of the selected authentication scheme - ZCK - relates to the number of agents T_{ai} in the path. The longer it takes for an agent to perform a task as well as authenticate itself to another agent in the global network, the poorer the quality of this task is. Thus, the longer it takes to deliver a task to the human, the lower the reputation level is.

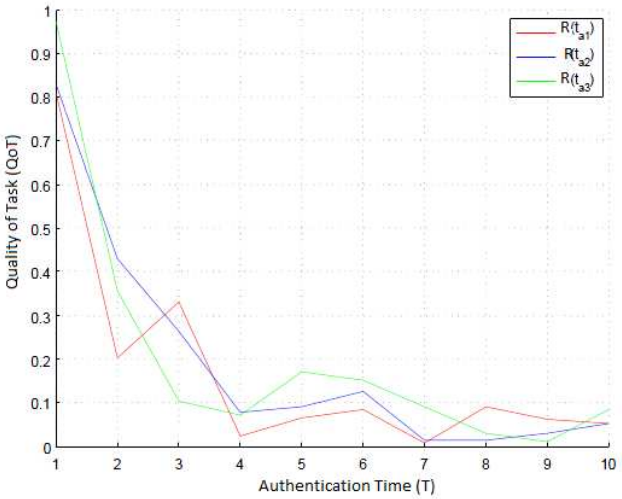

Figure 4. Reputation level for three different tasks

In this work, we have demonstrated how the graph-based approach can be used to represent trust and reputation in ubiquitous networks, and have addressed trust as a function of the reputation levels agents have gained from previous experiences and a number of authentication hops in the path. In other words, trust is seen as dependent on reputation levels between two or more agents which perform a requested task. Nevertheless, the reputation can be affected not only by the authentication time required to authenticate agent-to-agent relationships but also by other factors. These can be network conditions that may reduce the response time at a time of a resource was requested. In our future work, we plan to include additional factors, such as network influences like jitter and delay, into the trust formulation and we also intend to perform additional experiments to prove the initial trust and reputation relationship.

Despite using several assumptions while discussing the graph-based approach to address trust, this work has underlined an important aspect of trust. Using the demonstrated mathematical formulation of trust a human can obtain a trust value for each task after its completion, get information about a number of agents which dealt with the task, their level of reputation and other possible security factors that may increase or reduce trust in a particular agent set.

VII. CONCLUSION

In this paper we have presented a graph-based approach to address trust in complex ubiquitous systems, where a graph theory is used to visualise interactions between agents from a local to global perspective. In addition, within the proposed approach we have introduced new metrics to represent trust. These are: quality of a task, reputation level and average trust. Thus, trust has been formulated as a function of time required to authenticate agents in the path, using the ZCK authentication scheme, and a quality of a task, which consists of a response time, context of messages, feedback, etc. Therefore, the trust function represents a tight relationship between the reputation agents gain during their interaction within a global network, and possible factors that may reduce this level. Furthermore, the average trust can provide a trust value for a specific task based on pre-selected paths. This value provides a sound understanding of a distance between tasks performing agents.

We believe that this approach can help to encourage research in several directions, and novel trust and reputation models will be built upon the foundation given here.

REFERENCES

[1] M.He, N.R.Jennings, H.F.Leung, On agent-mediated electronic commerce. IEEE Transactions on Knowledge and Data Engineering, 2003, vol.15, pp. 985-1003

[2] G.Lu, J.Lu, S.Yao, J.Yip. A review on computation trust models for multi-agent systems. The open information science journal, 2009, 2(8),pp.18-25

[3] D.H.McKnight, V.Choudhury and J.C.Kaemar. Developig and validating trust measures for e-commerce:An integrative topology. Information Systems Research, 2002, 13(3) pp.334-359.

[4] P.Sant and C.Maple A graph theoreticc framework for trust – from local to global. In Information Visualisation (IV'2006), pp 497-503.

[5] J. Sabater and C.Sierra. 2005. Review on Computational Trust and Reputation Models. Artif. Intell. Rev. 24, 1 (September 2005), 33-60. DOI=10.1007/s10462-004-0041-5

[6] K., Krukow, M., Nielsen, and V. Sasone, (2008). Trust models in ubiquituos computing. Philosophical transactions of the royal society, 366 (1881), pp. 3781–3793.

[7] B.,. Esfandiari, , S. Chandrasekharan (2001). On How Agents Make Friends: Mechanisms for Trust Acquisition. In Proceedings of the 4th workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada, pp. 27-34.

[8] .D. Gambetta 1990, Trust: Making and breaking cooperative relations, ISBN 0631175873

[9] Y.H.Chu, J.Feigenbaum, B.A.LaMacchia, P,Resnick and M.Strauss. Referee:Trust management for web applications. Computer Networks, 1997, vol 29(8-13), pp 953-964.

[10] B.Yu and M.P.Singh. An evidential model of distributed reputation management. In AA-MAS 2002, pp 294-301.

[11] W.T. Teacy, J.Patel, N.R.Jennings and M.Luck. TRAVOS: trust and reputation in the context of inaccurate information sources. Autonomous agents and mullti-agent stsrems, 2006. Vol.12(2) pp.183-198

[12] S.P.Marsh Formalising trust as a computational concept.Technical Report 1994.

[13] A.Weimerskirch and D.Westhoff. Zero common-knowledge authentication for pervasive networks. in Proc.10th Workshop Selected Areas in Cryptography (SAC 03), pp. 73-87, 2003

[14] L. Lu, J. Han, Y. Liu, L. Hu, J.-P. Huai, L. Ni, and J. MaPseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps. IEEE Trans. Parallel Distrib. Syst. 2008. 19(10), pp. 1325-1337. .