Akash K Singh / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 6, November- December 2012, pp.585-619

Trust and Trust Management Models for Ecommerce & Sensor Network

Akash K Singh, PhD
IBM Corporation Sacramento, USA

Abstract

Service oriented cloud technologies are emerging as next computing platform for social media. SOA stack development and deployment undergoes architecture principles to improve service identification, service realization and service orchestration in Cloud Fabrics. Distributed services are composed and serves highly complex computing environment. In Mobile world service deployment and service access are primarily dependent upon the service subscriber and telecom provider. Thus, a reliable service fabric is highly required for the mobility computing. This paper proposes to achieve the reliable service orchestration and service fabrics along with mobility platform and the localization of the service operators and subscribers. Between the randomness and chaos communication channels there are higher chances of uncertainty. Occurrence of multiple chaos events increases the uncertainty in mobile service subscriber and provider communication channel and service availability.

Keywords- SOA, Mobility, Localization, Entropy, Randomness and Chaos Trust management Trust levels, Authentication and Access Control, Web Service Federation, Federated Identity Management

I. INTRODUCTION

Web services technologies make distributed computing components to be easily integrated across business boundaries and computing platforms. On the other hand, the web services technologies introduce a high degree of complexity of runtime operations. In web services, different kinds of business partners could be involved, and it may be possible for web services to require other services offered by third parties; the providers of web services may belong to different security domains; and the users of web services may not be predetermined. Undoubtedly, security is a key area to be addressed for delivering integrated, interoperable solutions under web services architecture. There have been many technologies that focus on building blocks and specific aspects of a broad range of security issues [1]. However it is still lacking an integrated solution and architecture that can address access control and related trust management for web services in a consistent manner. In our previous work, we have proposed a comprehensive trust management solution that covers both the analysis/modeling of trust relationships and the development of trust management systems [3, 4, 5]. Employing our previous results as a foundation, we propose a trust management approach for web services in this paper. The remainder of this paper is organized as follows. Section 2 overviews the taxonomy framework of trust. Section 3 discusses trust relationships in web services. Section 4 proposes trust management architecture of web services. Web services architecture layers provides concluding remarks for this paper. Next generations distributed cyberspace technologies, to include cloud computing, social networking, and mobile applications, coupled with the explosion in storage and processing power, will enhance services' ubiquity, availability and mobility while drastically reducing the cost of computing and communications. Such advances are expected to evolve a global marketplace for cyber resources and services. In such a largescale marketplace, users are largely autonomous with vastly diverse requirements, capabilities and trust profiles. Users' requirements may include service quality levels and fees needed. Their capabilities may also include assets owned or outsourced. while their trust profiles may include what is promised and commitments to keep these promises. Trusting services and service compositions in this marketplace is a challenging endeavor. We hypothesize the need for a generic personalized trust management system for the wide scale adoption of such marketplace. However, most existing trust management systems are oblivious to the diversity in users' trust requirements. In addition, their trust as well as trust-based decision support computations and methodologies are not personalized and are generally hardwired and not reconfigurable. Moreover, their trust management operations are tightly coupled. Such coupling exposes trust data to all trust management operations, resulting in potential violation of trust data privacy and vulnerabilities that may violate trust data confidentially and integrity. In this paper we propose a model for personalized trust management. We focus on service-to-service based environment where users of different roles (consumer, broker and provider) are trading services while satisfying their own trust requirements. In the model, users can play any of the three roles, consumer, broker or provider. Requirements of each role are expressed using trust definition language

(TDL) and are satisfied either by automatically selecting what is suitable among trust computation methodologies or enable roles to individually and manually define their computation methodology. Our proposed trust management model comprises a number of reconfigurable components that can be used to implement any trust management system according to users' trust requirements. These components represent generic operations of trust management which includes decision, expectation, analysis, data management and monitoring. Separation of these operations supports data privacy, confidentially and integrity, where data can be kept at their sources and accessed only on a need to know basis. The model builds trust using the four parameters intent, integrity, capability and results. Intent constitutes information about declared agendas (what parties promise to provide through their services), integrity constitutes information about honesty (if parties deliver what they promised), capability constitutes information about owned or outsourced resources (what assets parties have or can secure), and results constitute information about products (what products they are specialized in). Based on that model, we develop a personalized autonomic trust management system for P2P networks as a case study. The system includes the autonomic aspects of self-configuring and self-optimizing. Self-configuring includes automatic selection of suitable trust computation methodology according to user trust requirements. Self-optimizing includes accumulating knowledge from users experience to refine selection of computation methodologies. The main contributions of our work are:

- A unified model for trust management, which provides a number of reconfigurable components for implementing any trust management system according to user trust requirements.
- Defining and quantifying trust in terms of the four parameters intent, integrity, capability and results.
- Separation of concern among different trust management operations decision, expectation, analysis data management and monitoring.
- User centric trust management, where user-trust can play any of the three roles: consumer, provider and broker.

II. WIRELESS SENSOR NETWORK SECURITY

A. Wireless Sensor Network

AWIRELESS sensor network (WSN) is usually composed of a large number of spatially distributed autonomous sensor nodes (SNs) to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. A SN deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing. While SNs have popularly used for various monitoring purposes such as wild animals, weather, or environments for battlefield surveillance, they also have severely restricted resources such as energy, memory, and computational power. Further, wireless environments give more design challenges due to inherently unreliable communication. A more serious issue is that nodes may be compromised and perform malicious attacks such as packet dropping or packet modifications to disrupt normal operations of a WSN wherein SNs usually perform unattended operations. A large number of SNs deployed in the WSN also require a scalable algorithm for highly reconfigurable communication operations. In this work, we propose a hierarchical trust management protocol leveraging clustering to cope with a large number of heterogeneous SNs for scalability and reconfigurability, as well as to cope with selfish or malicious SNs for survivability and intrusion tolerance. We address the key design issues of trust management including trust composition (i.e., what trust components are considered), trust aggregation (i.e., how information is aggregated for each trust component), and trust formation (i.e., how trust is formed from individual trust components). The scientific contributions of the paper are as follows:

1) Unlike most existing reputation and trust management schemes in the literature [1], we consider not only quality of service (QoS) trust derived from communication networks, but also social trust derived from social networks [2] to judge if a node is trustworthy to deal with selfish (uncooperative) or malicious nodes.

2) Untreated in the literature, we design and validate a hierarchical trust management protocol that can dynamically learn from past experiences and adapt to changing environment conditions (e.g., increasing hostility or misbehaving node population) to maximize application performance and enhance operation agility. This is achieved by addressing critical issues of hierarchical trust management, namely, trust composition, aggregation, and formation. For trust composition, we explore novel social and QoS trust components. For trust aggregation, we identify the best way to aggregate trust (direct vs. indirect trust evaluation) and propagate trust (trust data collection, dissemination and analysis) for each individual trust component, and ascertain protocol accuracy by means of a novel model-based analysis methodology. For trust formation, we identify the best way to form trust out of social and QoS trust properties depending on application requirements to maximize application performance. Dynamic trust management is achieved by first determining the best trust formation model, given a set of model parameters specifying the environment conditions (e.g., increasing hostility) and then at runtime by learning and adapting to changing environment conditions

using the best trust formation model identified from static analysis.

3) To achieve the goals of identifying the best trust composition, trust aggregation and trust formation for WSN applications, we develop a novel model-based analysis methodology for analyzing and validating protocol design. The novelty lies in the new design notion of objective trust derived from global knowledge or ground truth derived from the mathematical model against which subjective trust obtained as a result of executing the trust management protocol may be compared and validated. This requires a mathematical model based on Stochastic Petri Net (SPN) techniques [3] and an iteration solution technique be developed to faithfully describe a large number of heterogeneous entities with a variety of QoS and social behaviors to yield global knowledge or ground truth of node status, thus providing objective trust against which subjective trust from protocol execution can be validated. The end product is a model-based analysis tool for evaluation of hierarchical trust management protocol designs applicable to a wide range of WSN applications, allowing trust composition, trust aggregation, and trust formation designs to be incorporated, tested and validated.

4) Untreated in the literature, we explore and validate a new design concept of application-level trust optimization in response to changing conditions to maximize application performance or best satisfy application requirements. To demonstrate the utility of the hierarchical trust management protocol, we apply it to trust-based geographic routing [4], [5] and trust-based intrusion detection. For the trust-based geographic routing application, we identify the best trust formation model to optimize application performance in delivery ratio or message delay in the presence of misbehaving nodes. For the trust-based intrusion detection application, we identify the best trust formation model as well as the best application-level drop-dead trust threshold below which a node is considered misbehaving to optimize application performance in false alarm probability. The rest of the paper is organized as follows. The emergence of wireless networks and rapid proliferation of mobile portable devices have stimulated a general trend towards extending P2P characteristics to wireless communication environments. As a result, the P2P paradigm has migrated to pervasive computing scenarios. Many P2P systems do not have the central administration and peers are autonomous, making them inherently insecure and untrustworthy [2, 20]. To handle the trustworthiness issues of these systems in open and decentralized environments, many trust and reputation schemes have been proposed to establish trust among peers in P2P systems. In a trust and reputation system, the historical behaviors and activities are recorded for each entity. The statistics of these behaviors and activities are used to predict how the entity is likely to behave in the future [11]. Many studies [3]-[23], have recently developed the decentralized trust and reputation systems and addressed various issues of trust and reputation management, such as GossipTrust – a gossip-based aggregation scheme [23], FIRE - a decentralized trust model [7], H-Trust – a selective aggregation scheme [21], FuzzyTrust [15] and a reputation based trust management system [14]. Moreover, several studies [10], [18] have contributed to the framework design and middleware architecture for trust management. Mobile P2P systems pose greater challenges in trust management due to the frequent changes in the network topology. To deploy a mobile P2P system a straight forward approach is to mount a P2P system over Mobile Ad hoc Networks (MANETs) [20]. MANETs are wireless networks where the transitory sets of mobile nodes dynamically establish their own network on the fly. Nodes in a MANET are constrained by a limited amount of energy, storage, bandwidth and computational power. These limitations prove to be a hindrance in seamless connectivity with other peers and thus deteriorating the effectiveness of many trust and reputation systems. Since a reputation-based system requires trust ratings from other peers to evaluate or update trust scores, it is imperative that the trust management system should be decentralized and can effectively aggregate trust ratings despite of delays, connection loss and malicious behavior from peers [24, 25]. Moreover, as it is impossible to establish the global trust ratings for peers, any trust management scheme must take into account trust ratings at a local level and build the reputation of peers based on accumulated ratings. To study trustworthiness in mobile P2P trust management systems, we first investigate the effectiveness of various decentralized and distributed trust ratings aggregation schemes on MANETs. Specifically, the popular trust schemes including the received ratings aggregation [9], weighted average of ratings [7], Bellman- Ford based algorithm [22], total and ultimate trust schemes [1] are thoroughly investigated and compared. Based on the analytical results, we propose an efficient, accurate, robust and scalable light weight trust ratings aggregation scheme, referred to as M-trust, for mobile P2P networks. We further propose a trust ratings aggregation algorithm that acquires trust ratings not only from direct recommendations but also from recommendations from distant nodes. Results obtained from extensive simulations show that this proposed scheme can decrease the time required to compute the list of trust ratings and reduce the required storage space. The comparison to other schemes shows that M-trust possesses the excellent overall performance in terms of accuracy, reliability, convergence speed, rate of detecting malicious peers under various constraints of mobility, trust threshold and network out-degree.

The rest of this paper is organized as follows; Section 2 presents and compares the typical trust ratings aggregation schemes. Section 3 describes the proposed scheme followed by the detailed analysis and comparison of performance results in Section 4. Section 5 concludes this work.

We consider the following anycast field equations defined over an open bounded piece of network and /or feature space $\Omega \subset R^d$. They describe the dynamics of the mean anycast of each of p node populations.

$$\begin{cases} (\frac{d}{dt}+l_i)V_i(t,r) = \sum_{j=1}^{p}\int_{\Omega} J_{ij}(r,\bar{r})S[(V_j(t-\tau_{ij}(r,\bar{r}),\bar{r})-h_{ij})]d\bar{r} \\ \qquad\qquad + I_i^{ext}(r,t), \qquad t \geq 0, 1 \leq i \leq p, \\ V_i(t,r) = \phi_i(t,r) \qquad\qquad t \in [-T,0] \end{cases} \quad (1)$$

We give an interpretation of the various parameters and functions that appear in (1), Ω is finite piece of nodes and/or feature space and is represented as an open bounded set of R^d . The vector r and $\bar{r}$ represent points in Ω . The function $S: R \to (0,1)$ is the normalized sigmoid function:

$$S(z) = \frac{1}{1+e^{-z}} \qquad (2)$$

It describes the relation between the input rate v_i of population i as a function of the packets potential, for example, $V_i = v_i = S[\sigma_i(V_i - h_i)]$. We note V the $p-$ dimensional vector $(V_1,...,V_p)$. The p function $\phi_i, i = 1,..., p,$ represent the initial conditions, see below. We note ϕ the $p-$ dimensional vector $(\phi_1,...,\phi_p)$. The p function $I_i^{ext}, i = 1,..., p,$ represent external factors from other network areas. We note I^{ext} the $p-$ dimensional vector $(I_1^{ext},...,I_p^{ext})$. The $p \times p$ matrix of functions $J = \{J_{ij}\}_{i,j=1,...,p}$ represents the connectivity between populations i and j, see below. The p real values $h_i, i = 1,..., p,$ determine the threshold of activity for each population, that is, the value of the nodes potential corresponding to 50% of the maximal activity. The p real positive values $\sigma_i, i = 1,..., p,$ determine the slopes of the sigmoids at the origin. Finally the p real positive values $l_i, i = 1,..., p,$ determine the speed at which each anycast node potential decreases exponentially toward its real value. We also introduce the function $S: R^p \to R^p$, defined by $S(x) = [S(\sigma_1(x_1 - h_1)),..., S(\sigma_p - h_p))]$, and the diagonal $p \times p$ matrix $L_0 = diag(l_1,...,l_p)$. Is the intrinsic dynamics of the population given by the linear response of data transfer. $(\frac{d}{dt}+l_i)$ is replaced by $(\frac{d}{dt}+l_i)^2$ to use the alpha function response. We use $(\frac{d}{dt}+l_i)$ for simplicity although our analysis applies to more general intrinsic dynamics. For the sake, of generality, the propagation delays are not assumed to be identical for all populations, hence they are described by a matrix $\tau(r,\bar{r})$ whose element $\tau_{ij}(r,\bar{r})$ is the propagation delay between population j at $\bar{r}$ and population i at r. The reason for this assumption is that it is still unclear from anycast if propagation delays are independent of the populations. We assume for technical reasons that τ is continuous, that is $\tau \in C^0(\bar{\Omega}^2, R_+^{p \times p})$. Moreover packet data indicate that τ is not a symmetric function i.e., $\tau_{ij}(r,\bar{r}) \neq \tau_{ij}(\bar{r},r)$, thus no assumption is made about this symmetry unless otherwise stated. In order to compute the righthand side of (1), we need to know the node potential factor V on interval $[-T,0]$. The value of T is obtained by considering the maximal delay:

$$\tau_m = \max_{i,j(r,r \in \bar{\Omega} \times \bar{\Omega})} \tau_{i,j}(r,\bar{r}) \qquad (3)$$

Hence we choose $T = \tau_m$

B. Mobile AdHoc Network (MANET)

A delay tolerant network (DTN) provides interoperable communications through mobile nodes with the characteristics of high end-to-end path latency, frequent disconnection, limited resources (e.g., battery, computational power, bandwidth), and unreliable wireless transmission. Further, for DTNs in mobile ad hoc network (MANET) environments, we also face additional challenges due to a lack of centralized trust entity and this increases security vulnerability [5]. For a sparse MANET DTN, mobility-assisted routing based on store-carry-and-forward method has been used. That is, a message carrier forwards a message to an encountered node until the message reaches a destination node. In MANET DTN environments, it is important to select a trustable node as a next message carrier among all encountered nodes to minimize delay for a message to reach a destination node as well as to maximize the message delivery ratio. In this paper, we consider a MANET DTN in the presence of selfish and malicious nodes and propose a family of trust

management protocols for encounter-based routing to select a highly trustworthy next message carrier with the goals of maximizing the message delivery ratio without incurring a high delay or a high message overhead. In the literature, DTN routing based on encounter patterns has been investigated [2, 10, 11]. However, if the predicted encounter does not happen, then messages would be lost for single-copy routing, or flooded for multi-copy routing. Moreover, these approaches could not guarantee reliable message delivery due to the presence of selfish or malicious nodes. The vulnerability of DTN routing to node selfishness was well studied in [7]. Several recent studies [12, 14, 15] considered using reputation in selecting message carriers among encountered nodes for DTNs. Nevertheless, [12, 14] assumed that a centralized entity exists for credit management, and [15] merely used reputation to judge if the system should switch from reputation-based routing to multipath routing when many selfish nodes exist. There is very little research to date on the social aspect of trust management for DTN routing. Social relationship and social networking were considered as criteria to select message carriers in a MANET DTN [6,8]. However, no consideration was given to the presence of malicious or selfish nodes. Very recently, [9] considered routing by socially selfish nodes in DTNs, taking into consideration the willingness of a socially selfish node to forward messages to the destination node because of social ties. Unlike prior work cited above, in this paper, we combine the notion of social trust and QoS trust into a composite trust metric for determining the best node among the new encounters for message forwarding. We consider honesty and unselfishness for social trust to account for node trustworthiness for message delivery, and connectivity for QoS trust to account for node capability to quickly deliver the message to the destination node. By assigning various weights associated with these QoS and social trust properties, we form a class of DTN routing protocols, from which we examine two versions of the trust management protocol in this paper: an equal-weight QoS and social trust management protocol (called trust-based routing for short) and a QoS trust only management protocol (call connectivity-based routing for short). We analyze and compare the performance characteristics of trust-based routing and connectivity-based routing protocols with epidemic routing [13] for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. The results indicate that our trust-based routing protocol approaches the ideal performance of epidemic routing in delivery ratio, while connectivity-based routing approaches the ideal performance of epidemic routing in message delay, as the percentage of selfish and malicious nodes present in the DTN system increases. All DTN routing protocols in the class significantly outperform epidemic routing in message overhead. IN AN INCREASINGLY networked world, increased connectivity could lead to improved information sharing, facilitate collaboration, and enable distributed decision making, which is the underlying concept in Network Centric Operations. In mobile ad hoc networks (MANETs), the distributed decision making should take into account trust in the elements: the sources of information, the processors of information, the elements of the communications network across which the information is transmitted, etc. This trust must often be derived under time-critical conditions, and in a distributed way.

C. Mathematical Framework

A convenient functional setting for the non-delayed packet field equations is to use the space $F = L^2(\Omega, R^p)$ which is a Hilbert space endowed with the usual inner product:

$$\langle V, U \rangle_F = \sum_{i=1}^{p} \int_\Omega V_i(r) U_i(r) dr \qquad (1)$$

To give a meaning to (1), we defined the history space $C = C^0([-\tau_m, 0], F)$ with $\|\phi\| = \sup_{t\in[-\tau_m,0]} \|\phi(t)\| F$, which is the Banach phase space associated with equation (3). Using the notation $V_t(\theta) = V(t+\theta), \theta \in [-\tau_m, 0]$, we write (1) as

$$\begin{cases} \dot{V}(t) = -L_0 V(t) + L_1 S(V_t) + I^{ext}(t), \\ V_0 = \phi \in C, \end{cases} \qquad (2)$$

Where

$$\begin{cases} L_1 : C \to F, \\ \phi \to \int_\Omega J(.,\bar{r}) \phi(\bar{r}, -\tau(.,\bar{r})) d\bar{r} \end{cases}$$

Is the linear continuous operator satisfying $\|L_1\| \le \|J\|_{L^2(\Omega^2, R^{p\times p})}$. Notice that most of the papers on this subject assume Ω infinite, hence requiring $\tau_m = \infty$.

Proposition 1.0 If the following assumptions are satisfied.

1. $J \in L^2(\Omega^2, R^{p\times p})$,
2. The external current $I^{ext} \in C^0(R, F)$,
3. $\tau \in C^0(\overline{\Omega^2}, R_+^{p\times p}), \sup_{\overline{\Omega^2}} \tau \le \tau_m$.

Then for any $\phi \in C$, there exists a unique solution $V \in C^1([0,\infty), F) \cap C^0([-\tau_m, \infty, F)$ to (3)

Notice that this result gives existence on R_+, finite-time explosion is impossible for this delayed differential equation. Nevertheless, a particular

solution could grow indefinitely, we now prove that this cannot happen.

D. Boundedness of Solutions

A valid model of neural networks should only feature bounded packet node potentials.

Theorem 1.0 All the trajectories are ultimately bounded by the same constant R if $I \equiv \max_{t\in R^+} \|I^{ext}(t)\|_F < \infty.$

Proof :Let us defined $f : R\times C \to R^+$ as

$$f(t,V_t) \overset{def}{=} \langle -L_0 V_t(0) + L_1 S(V_t) + I^{ext}(t), V(t)\rangle_F = \frac{1}{2}\frac{d\|V\|_F^2}{dt}$$

We note $l = \min_{i=1,\dots p} l_i$

$$f(t,V_t) \le -l\|V(t)\|_F^2 + (\sqrt{p|\Omega|}\,\|J\|_F + I)\|V(t)\|_F$$

Thus, if

$$\|V(t)\|_F \ge 2\frac{\sqrt{p|\Omega|}.\|J\|_F + I}{l} \overset{def}{=} R,\ f(t,V_t) \le -\frac{lR^2}{2} \overset{def}{=} -\delta < 0$$

Let us show that the open route of F of center 0 and radius R, B_R, is stable under the dynamics of equation. We know that $V(t)$ is defined for all $t \ge 0s$ and that $f < 0$ on ∂B_R, the boundary of B_R. We consider three cases for the initial condition V_0. If $\|V_0\|_C < R$ and set $T = \sup\{t \mid \forall s \in [0,t], V(s) \in \overline{B_R}\}.$ Suppose that $T \in R,$ then $V(T)$ is defined and belongs to $\overline{B_R}$, the closure of B_R, because $\overline{B_R}$ is closed, in effect to ∂B_R, we also have $\frac{d}{dt}\|V\|_F^2 |_{t=T} = f(T,V_T) \le -\delta < 0$ because $V(T) \in \partial B_R$. Thus we deduce that for $\varepsilon > 0$ and small enough, $V(T+\varepsilon) \in \overline{B_R}$ which contradicts the definition of T. Thus $T \notin R$ and $\overline{B_R}$ is stable.

Because f<0 on $\partial B_R, V(0) \in \partial B_R$ implies that $\forall t > 0, V(t) \in B_R$. Finally we consider the case $V(0) \in C\overline{B_R}$. Suppose that $\forall t > 0, V(t) \notin \overline{B_R},$ then $\forall t > 0, \frac{d}{dt}\|V\|_F^2 \le -2\delta,$ thus $\|V(t)\|_F$ is monotonically decreasing and reaches the value of R in finite time when $V(t)$ reaches ∂B_R. This contradicts our assumption. Thus $\exists T > 0 \,|\, V(T) \in B_R.$

Proposition 1.1 : Let s and t be measured simple functions on X. for $E\varepsilon M,$ define

$$\phi(E) = \int_E s\, d\mu \qquad (1)$$

Then ϕ is a measure on M.

$$\int_X (s+t)d\mu = \int_X s\, d\mu + \int_X t d\mu \qquad (2)$$

Proof : If s and if $E_1, E_2, \dots$ are disjoint members of M whose union is $E,$ the countable additivity of μ shows that

$$\phi(E) = \sum_{i=1}^{n} \alpha_i \mu(A_i \cap E) = \sum_{i=1}^{n} \alpha_i \sum_{r=1}^{\infty} \mu(A_i \cap E_r)$$
$$= \sum_{r=1}^{\infty}\sum_{i=1}^{n} \alpha_i \mu(A_i \cap E_r) = \sum_{r=1}^{\infty} \phi(E_r)$$

Also, $\varphi(\phi) = 0,$ so that φ is not identically ∞.

Next, let s be as before, let $\beta_1, \dots, \beta_m$ be the distinct values of t,and let $B_j = \{x : t(x) = \beta_j\}$ If $E_{ij} = A_i \cap B_j,$ the $\int_{E_{ij}} (s+t)d\mu = (\alpha_i + \beta_j)\mu(E_{ij})$

and $\int_{E_{ij}} sd\mu + \int_{E_{ij}} td\mu = \alpha_i \mu(E_{ij}) + \beta_j \mu(E_{ij})$

Thus (2) holds with E_{ij} in place of X. Since X is the disjoint union of the sets E_{ij} $(1 \le i \le n, 1 \le j \le m),$ the first half of our proposition implies that (2) holds.

Theorem 1.1: If K is a compact set in the plane whose complement is connected, if f is a continuous complex function on K which is holomorphic in the interior of , and if $\varepsilon > 0,$ then there exists a polynomial P such that $|f(z) = P(z)| < \varepsilon$ for all $z\varepsilon K$. If the interior of K is empty, then part of the hypothesis is vacuously satisfied, and the conclusion holds for every $f\varepsilon C(K)$. Note that K need to be connected.

Proof: By Tietze's theorem, f can be extended to a continuous function in the plane, with compact

support. We fix one such extension and denote it again by f. For any $\delta > 0$, let $\omega(\delta)$ be the supremum of the numbers $|f(z_2) - f(z_1)|$ Where z_1 and z_2 are subject to the condition $|z_2 - z_1| \le \delta$. Since f is uniformly continous, we have $\lim_{\delta \to 0} \omega(\delta) = 0$ (1) From now on, δ will be fixed. We shall prove that there is a polynomial P such that

$$|f(z) - P(z)| < 10{,}000\ \omega(\delta) \quad (z \varepsilon K) \qquad (2)$$

By (1), this proves the theorem. Our first objective is the construction of a function $\Phi \varepsilon C_c^{'}(R^2)$, such that for all z

$$|f(z) - \Phi(z)| \le \omega(\delta), \qquad (3)$$

$$|(\partial\Phi)(z)| < \frac{2\omega(\delta)}{\delta}, \qquad (4)$$

And

$$\Phi(z) = -\frac{1}{\pi}\iint_X \frac{(\partial\Phi)(\zeta)}{\zeta - z} d\zeta d\eta \qquad (\zeta = \xi + i\eta), \qquad (5)$$

Where X is the set of all points in the support of Φ whose distance from the complement of K does not δ. (Thus X contains no point which is "far within" K.) We construct Φ as the convolution of f with a smoothing function A. Put $a(r) = 0$ if $r > \delta$, put

$$a(r) = \frac{3}{\pi\delta^2}\left(1 - \frac{r^2}{\delta^2}\right)^2 \qquad (0 \le r \le \delta), \qquad (6)$$

And define

$$A(z) = a(|z|) \qquad (7)$$

For all complex z. It is clear that $A \varepsilon C_c^{'}(R^2)$. We claim that

$$\iint_{R^s} A = 1, \qquad (8)$$

$$\iint_{R^2} \partial A = 0, \qquad (9)$$

$$\iint_{R^3} |\partial A| = \frac{24}{15\delta} < \frac{2}{\delta}, \qquad (10)$$

The constants are so adjusted in (6) that (8) holds. (Compute the integral in polar coordinates), (9) holds simply because A has compact support. To compute (10), express ∂A in polar coordinates, and note that $\partial A / \partial\theta = 0$,

$$\partial A / \partial r = -a^{'},$$

Now define

$$\Phi(z) = \iint_{R^2} f(z-\zeta) A d\xi d\eta = \iint_{R^2} A(z-\zeta) f(\zeta) d\xi d\eta \qquad (11)$$

Since f and A have compact support, so does Φ. Since

$$\Phi(z) - f(z) = \iint_{R^2} [f(z-\zeta) - f(z)] A(\xi) d\xi d\eta \qquad (12)$$

And $A(\zeta) = 0$ if $|\zeta| > \delta$, (3) follows from (8). The difference quotients of A converge boundedly to the corresponding partial derivatives, since $A \varepsilon C_c^{'}(R^2)$. Hence the last expression in (11) may be differentiated under the integral sign, and we obtain

$$\begin{aligned}(\partial\Phi)(z) &= \iint_{R^2} (\overline{\partial A})(z-\zeta) f(\zeta) d\xi d\eta \\ &= \iint_{R^2} f(z-\zeta)(\partial A)(\zeta) d\xi d\eta \\ &= \iint_{R^2} [f(z-\zeta) - f(z)](\partial A)(\zeta) d\xi d\eta \qquad (13)\end{aligned}$$

The last equality depends on (9). Now (10) and (13) give (4). If we write (13) with Φ_x and Φ_y in place of $\partial\Phi$, we see that Φ has continuous partial derivatives, if we can show that $\partial\Phi = 0$ in G, where G is the set of all $z \varepsilon K$ whose distance from the complement of K exceeds δ. We shall do this by showing that

$$\Phi(z) = f(z) \qquad (z \varepsilon G); \qquad (14)$$

Note that $\partial f = 0$ in G, since f is holomorphic there. Now if $z \varepsilon G$, then $z - \zeta$ is in the interior of K for all ζ with $|\zeta| < \delta$. The mean value property for harmonic functions therefore gives, by the first equation in (11),

$$\begin{aligned}\Phi(z) &= \int_0^{\delta} a(r) r dr \int_0^{2\pi} f(z - re^{i\theta}) d\theta \\ &= 2\pi f(z) \int_0^{\delta} a(r) r dr = f(z) \iint_{R^2} A = f(z) \qquad (15)\end{aligned}$$

For all $z\ \varepsilon\ G$, we have now proved (3), (4), and (5) The definition of X shows that X is compact and that X can be covered by finitely many open discs $D_1, \ldots, D_n$, of radius 2δ, whose centers are not in K. Since $S^2 - K$ is connected,

the center of each D_j can be joined to ∞ by a polygonal path in $S^2 - K$. It follows that each D_j contains a compact connected set E_j, of diameter at least 2δ, so that $S^2 - E_j$ is connected and so that $K \cap E_j = \phi$. with $r = 2\delta$. There are functions $g_j \varepsilon H(S^2 - E_j)$ and constants b_j so that the inequalities.

$$\left|Q_j(\zeta, z)\right| < \frac{50}{\delta}, \qquad (16)$$

$$\left|Q_j(\zeta, z) - \frac{1}{z-\zeta}\right| < \frac{4,000\delta^2}{\left|z-\zeta\right|^2} \qquad (17)$$

Hold for $z \notin E_j$ and $\zeta \in D_j$, if

$$Q_j(\zeta, z) = g_j(z) + (\zeta - b_j) g_j^2(z) \qquad (18)$$

Let Ω be the complement of $E_1 \cup ... \cup E_n$. Then Ω is an open set which contains K. Put $X_1 = X \cap D_1$ and $X_j = (X \cap D_j) - (X_1 \cup ... \cup X_{j-1})$, for $2 \le j \le n$,

Define

$$R(\zeta, z) = Q_j(\zeta, z) \qquad (\zeta \varepsilon X_j, z \varepsilon \Omega) \qquad (19)$$

And

$$F(z) = \frac{1}{\pi} \iint_X (\partial\Phi)(\zeta) R(\zeta, z) d\zeta d\eta \qquad (20)$$

$(z \ \varepsilon \ \Omega)$

Since,

$$F(z) = \sum_{j=1} \frac{1}{\pi} \iint_{X_i} (\partial\Phi)(\zeta) Q_j(\zeta, z) d\xi d\eta, \qquad (21)$$

(18) shows that F is a finite linear combination of the functions g_j and g_j^2. Hence $F \varepsilon H(\Omega)$. By (20), (4), and (5) we have

$$\left|F(z) - \Phi(z)\right| < \frac{2\omega(\delta)}{\pi\delta} \iint_X \left| R(\zeta, z) - \frac{1}{z-\zeta} \right| d\xi d\eta \quad (z \ \varepsilon \ \Omega) \quad (22)$$

Observe that the inequalities (16) and (17) are valid with R in place of Q_j if $\zeta \ \varepsilon \ X$ and $z \ \varepsilon \ \Omega$. Now fix $z \ \varepsilon \ \Omega$., put $\zeta = z + \rho e^{i\theta}$, and estimate the integrand in (22) by (16) if $\rho < 4\delta$, by (17) if $4\delta \le \rho$. The integral in (22) is then seen to be less than the sum of

$$2\pi \int_0^{4\delta} \left(\frac{50}{\delta} + \frac{1}{\rho} \right) \rho d\rho = 808\pi\delta \qquad (23)$$

And

$$2\pi \int_{4\delta}^{\infty} \frac{4,000\delta^2}{\rho^2} \rho d\rho = 2,000\pi\delta. \qquad (24)$$

Hence (22) yields

$$\left|F(z) - \Phi(z)\right| < 6,000\omega(\delta) \qquad (z \ \varepsilon \ \Omega) \qquad (25)$$

Since $F \ \varepsilon \ H(\Omega)$, $K \subset \Omega$, and $S^2 - K$ is connected, Runge's theorem shows that F can be uniformly approximated on K by polynomials. Hence (3) and (25) show that (2) can be satisfied. This completes the proof.

Lemma 1.0 : Suppose $f \varepsilon C_c^{'}(R^2)$, the space of all continuously differentiable functions in the plane, with compact support. Put

$$\partial = \frac{1}{2} \left(\frac{\partial}{\partial x} + i \frac{\partial}{\partial y} \right) \qquad (1)$$

Then the following "Cauchy formula" holds:

$$f(z) = -\frac{1}{\pi} \iint_{R^2} \frac{(\partial f)(\zeta)}{\zeta - z} d\xi d\eta$$

$$(\zeta = \xi + i\eta) \qquad (2)$$

Proof: This may be deduced from Green's theorem. However, here is a simple direct proof:

Put $\varphi(r, \theta) = f(z + re^{i\theta})$, $r > 0$, θ real

If $\zeta = z + re^{i\theta}$, the chain rule gives

$$(\partial f)(\zeta) = \frac{1}{2} e^{i\theta} \left[\frac{\partial}{\partial r} + \frac{i}{r} \frac{\partial}{\partial \theta} \right] \varphi(r, \theta) \qquad (3)$$

The right side of (2) is therefore equal to the limit, as $\varepsilon \to 0$, of

$$-\frac{1}{2} \int_{\varepsilon}^{\infty} \int_0^{2\pi} \left(\frac{\partial \varphi}{\partial r} + \frac{i}{r} \frac{\partial \varphi}{\partial \theta} \right) d\theta dr \qquad (4)$$

For each $r > 0, \varphi$ is periodic in θ, with period 2π. The integral of $\partial\varphi / \partial\theta$ is therefore 0, and (4) becomes

$$-\frac{1}{2\pi} \int_0^{2\pi} d\theta \int_{\varepsilon}^{\infty} \frac{\partial \varphi}{\partial r} dr = \frac{1}{2\pi} \int_0^{2\pi} \varphi(\varepsilon, \theta) d\theta \qquad (5)$$

As $\varepsilon \to 0$, $\varphi(\varepsilon, \theta) \to f(z)$ uniformly. This gives (2)

If $X^\alpha \in a$ and $X^\beta \in k[X_1,...X_n]$, then $X^\alpha X^\beta = X^{\alpha+\beta} \in a$, and so A satisfies $(*)$. Conversely,

$$(\sum_{\alpha\in A} c_\alpha X^\alpha)(\sum_{\beta\in \square^n} d_\beta X^\beta) = \sum_{\alpha,\beta} c_\alpha d_\beta X^{\alpha+\beta} \quad (\textit{finite sums}),$$

and so if A satisfies $(*)$, then the subspace generated by the monomials $X^\alpha, \alpha \in a$, is an ideal. The proposition gives a classification of the monomial ideals in $k[X_1,...X_n]$: they are in one to one correspondence with the subsets A of $\square^n$ satisfying $(*)$. For example, the monomial ideals in $k[X]$ are exactly the ideals (X^n), $n \geq 1$, and the zero ideal (corresponding to the empty set A). We write $\langle X^\alpha \mid \alpha \in A\rangle$ for the ideal corresponding to A (subspace generated by the $X^\alpha, \alpha \in a$).

LEMMA 1.1. Let S be a subset of $\square^n$. The the ideal a generated by $X^\alpha, \alpha \in S$ is the monomial ideal corresponding to

$$A \underset{df}{=} \{\beta \in \square^n \mid \beta - \alpha \in \square^n, \quad some\ \alpha \in S\}$$

Thus, a monomial is in a if and only if it is divisible by one of the $X^\alpha, \alpha \in| S$

PROOF. Clearly A satisfies $(*)$, and $a \subset \langle X^\beta \mid \beta \in A\rangle$. Conversely, if $\beta \in A$, then $\beta - \alpha \in \square^n$ for some $\alpha \in S$, and $X^\beta = X^\alpha X^{\beta-\alpha} \in a$. The last statement follows from the fact that $X^\alpha \mid X^\beta \Leftrightarrow \beta - \alpha \in \square^n$. Let $A \subset \square^n$ satisfy $(*)$. From the geometry of A, it is clear that there is a finite set of elements $S = \{\alpha_1,...\alpha_s\}$ of A such that

$$A = \{\beta \in \square^n \mid \beta - \alpha_i \in \square^2, \ some\ \alpha_i \in S\}$$

(The α_i's are the corners of A) Moreover, $a \underset{df}{=} \langle X^\alpha \mid \alpha \in A\rangle$ is generated by the monomials $X^{\alpha_i}, \alpha_i \in S$.

DEFINITION 1.0. For a nonzero ideal a in $k[X_1,...,X_n]$, we let $(LT(a))$ be the ideal generated by

$$\{LT(f) \mid f \in a\}$$

LEMMA 1.2 Let a be a nonzero ideal in $k[X_1,...,X_n]$; then $(LT(a))$ is a monomial ideal, and it equals $(LT(g_1),...,LT(g_n))$ for some $g_1,...,g_n \in a$.

PROOF. Since $(LT(a))$ can also be described as the ideal generated by the leading monomials (rather than the leading terms) of elements of a.

THEOREM 1.2. Every *ideal* a in $k[X_1,...,X_n]$ is finitely generated; more precisely, $a = (g_1,...,g_s)$ where $g_1,...,g_s$ are any elements of a whose leading terms generate $LT(a)$

PROOF. Let $f \in a$. On applying the division algorithm, we find

$$f = a_1g_1 + ... + a_sg_s + r, \qquad a_i, r \in k[X_1,...,X_n]$$

, where either $r = 0$ or no monomial occurring in it is divisible by any $LT(g_i)$. But $r = f - \sum a_i g_i \in a$, and therefore $LT(r) \in LT(a) = (LT(g_1),...,LT(g_s))$, implies that every monomial occurring in r is divisible by one in $LT(g_i)$. Thus $r = 0$, and $g \in (g_1,...,g_s)$.

DEFINITION 1.1. A finite subset $S = \{g_1,|...,g_s\}$ of an ideal a is a standard ($(Gr\ddot{o}bner)$ bases for a if $(LT(g_1),...,LT(g_s)) = LT(a)$. In other words, S is a standard basis if the leading term of every element of a is divisible by at least one of the leading terms of the g_i.

THEOREM 1.3 *The ring* $k[X_1,...,X_n]$ *is Noetherian i.e., every ideal is finitely generated.*

PROOF. For $n = 1$, $k[X]$ is a principal ideal domain, which means that every ideal is generated by single element. We shall prove the theorem by induction on n. Note that the obvious map $k[X_1,...X_{n-1}][X_n] \to k[X_1,...X_n]$ is an isomorphism – this simply says that every polynomial f in n variables $X_1,...X_n$ can be

expressed uniquely as a polynomial in X_n with coefficients in $k[X_1,...,X_n]$:

$$f(X_1,...X_n) = a_0(X_1,...X_{n-1})X_n^r + ... + a_r(X_1,...X_{n-1})$$

Thus the next lemma will complete the proof

LEMMA 1.3. If A is Noetherian, then so also is $A[X]$

PROOF. For a polynomial

$$f(X) = a_0X^r + a_1X^{r-1} + ... + a_r, \quad a_i \in A, \quad a_0 \neq 0,$$

r is called the degree of f, and a_0 is its leading coefficient. We call 0 the leading coefficient of the polynomial 0. Let a be an ideal in $A[X]$. The leading coefficients of the polynomials in a form an ideal a' in A, and since A is Noetherian, a' will be finitely generated. Let $g_1,...,g_m$ be elements of a whose leading coefficients generate a', and let r be the maximum degree of g_i. Now let $f \in a$, and suppose f has degree $s > r$, say, $f = aX^s + ...$ Then $a \in a'$, and so we can write

$$a = \sum b_i a_i, \qquad b_i \in A,$$

a_i = *leading coefficient of* g_i

Now

$f - \sum b_i g_i X^{s-r_i}$, $r_i = \deg(g_i)$, has degree $< \deg(f)$. By continuing in this way, we find that $f \equiv f_t \mod(g_1,...g_m)$ With f_t a polynomial of degree $t < r$. For each $d < r$, let a_d be the subset of A consisting of 0 and the leading coefficients of all polynomials in a of degree d; it is again an ideal in A. Let $g_{d,1},...,g_{d,m_d}$ be polynomials of degree d whose leading coefficients generate a_d. Then the same argument as above shows that any polynomial f_d in a of degree d can be written $f_d \equiv f_{d-1} \mod(g_{d,1},...g_{d,m_d})$ With f_{d-1} of degree $\leq d-1$. On applying this remark repeatedly we find that $f_t \in (g_{r-1,1},...g_{r-1,m_{r-1}},...g_{0,1},...g_{0,m_0})$ Hence

$$f_t \in (g_1,...g_m g_{r-1,1},...g_{r-1,m_{r-1}},...,g_{0,1},...,g_{0,m_0})$$

and so the polynomials $g_1,...,g_{0,m_0}$ generate a

III. DESIGN CHALLENGES

A. Design Challenges in Mobile AdHoc Network (MANET)Protocol

A mobile ad hoc network [1] consists of wireless mobile nodes forming a temporary network without the help of centralized infrastructure, and where nodes communicate through multi-hops. Security protocol designers for MANETs face technical challenges due to severe resource constraints in bandwidth, memory size, battery life, computational power, and unique wireless characteristics such as openness to eavesdropping, lack of specific ingress and exit points, high security threats, vulnerability, unreliable communication, and rapid changes in topologies or memberships because of user mobility or node failure [1][2][3]. In addition, compared with designing security protocols for civilian MANETs, designing security protocols for military MANETs requires additional caution, since battlefield communication networks must cope with hostile environments, node heterogeneity, often stringent performance constraints, node subversion, high tempo operations leading to rapid changes in network topology and service requirements, and dynamically formed communities of interest wherein participants may not have predefined trust relationships [4]. To cope with these dynamics, networks must be able to reconfigure seamlessly, via low-complexity distributed network management schemes [3]. Security in a tactical network includes notions of communication security which can be easily quantified as opposed to the perception of security which is hard to quantify.

One of the great successes of category theory in computer science has been the development of a "unified theory" of the constructions underlying denotational semantics. In the untyped λ-calculus, any term may appear in the function position of an application. This means that a model D of the λ-calculus must have the property that given a term t whose interpretation is $d \in D$, Also, the interpretation of a functional abstraction like $\lambda x.x$ is most conveniently defined as a function from $D \text{ to } D$, which must then be regarded as an element of *D*. Let $\psi : [D \to D] \to D$ be the function that picks out elements of *D* to represent elements of $[D \to D]$ and $\phi : D \to [D \to D]$ be the function that maps elements of *D* to functions of *D*. Since $\psi(f)$ is intended to represent the function f as an element of *D*, it makes sense to require that $\phi(\psi(f)) = f$, that is, $\psi o \psi = id_{[D \to D]}$ Furthermore, we often

want to view every element of *D* as representing some function from *D to D* and require that elements representing the same function be equal – that is

$$\psi(\varphi(d)) = d$$

or

$$\psi \, o \, \phi = id_D$$

The latter condition is called extensionality. These conditions together imply that $\phi \, and \, \psi$ are inverses--- that is, *D* is isomorphic to the space of functions from *D to D* that can be the interpretations of functional abstractions: $D \cong [D \to D]$ .Let us suppose we are working with the untyped $\lambda - calculus$, we need a solution ot the equation $D \cong A + [D \to D]$, where A is some predetermined domain containing interpretations for elements of *C*. Each element of *D* corresponds to either an element of *A* or an element of $[D \to D]$, with a tag. This equation can be solved by finding least fixed points of the function $F(X) = A + [X \to X]$ from domains to domains --- that is, finding domains *X* such that $X \cong A + [X \to X]$, and such that for any domain *Y* also satisfying this equation, there is an embedding of *X* to *Y* --- a pair of maps

$$X \underset{f^R}{\overset{f}{\rightleftarrows}} Y$$

Such that

$$f^R \, o \, f = id_X$$

$$f \, o \, f^R \subseteq id_Y$$

Where $f \subseteq g$ means that $f \; approximates \; g$ in some ordering representing their information content. The key shift of perspective from the domain-theoretic to the more general category-theoretic approach lies in considering *F* not as a function on domains, but as a *functor* on a category of domains. Instead of a least fixed point of the function, *F*.

Definition 1.3: Let ***K*** be a category and $F : K \to K$ as a functor. A fixed point of *F* is a pair (A,a), where A is a ***K-object*** and $a : F(A) \to A$ is an isomorphism. A prefixed point of F is a pair (A,a), where A is a ***K-object*** and a is any arrow from F(A) to A

Definition 1.4 : An $\omega - chain$ in a category ***K*** is a diagram of the following form:

$$\Delta = D_o \xrightarrow{f_o} D_1 \xrightarrow{f_1} D_2 \xrightarrow{f_2} .....$$

Recall that a cocone μ of an $\omega - chain \; \Delta$ is a *K*-object *X* and a collection of K –*arrows* $\{\mu_i : D_i \to X \mid i \geq 0\}$ such that $\mu_i = \mu_{i+1} o \, f_i$ for all $i \geq 0$. We sometimes write $\mu : \Delta \to X$ as a reminder of the arrangement of $\mu's$ components Similarly, a colimit $\mu : \Delta \to X$ is a cocone with the property that if $\nu : \Delta \to X^{'}$ is also a cocone then there exists a unique mediating arrow $k : X \to X^{'}$ such that for all $i \geq 0,, \; \nu_i = k \, o \, \mu_i$. Colimits of $\omega - chains$ are sometimes referred to as $\omega - colimits$. Dually, an $\omega^{op} - chain$ in ***K*** is a diagram of the following form:

$$\Delta = D_o \xleftarrow{f_o} D_1 \xleftarrow{f_1} D_2 \xleftarrow{f_2} .....$$

A cone $\mu : X \to \Delta$ of an $\omega^{op} - chain \; \Delta$ is a ***K***-object X and a collection of **K**-arrows $\{\mu_i : D_i \mid i \geq 0\}$ such that for all $i \geq 0, \; \mu_i = f_i \, o \, \mu_{i+1}$. An ω^{op} -limit of an $\omega^{op} - chain$ Δ is a cone $\mu : X \to \Delta$ with the property that if $\nu : X^{'} \to \Delta$ is also a cone, then there exists a unique mediating arrow $k : X^{'} \to X$ such that for all $i \geq 0, \mu_i \, o \, k = \nu_i$. We write $\perp_k$ (or just $\perp$) for the distinguish initial object of ***K,*** when it has one, and $\perp \to A$ for the unique arrow from $\perp$ to each ***K***-object A. It is also convenient to write $\Delta^{-} = D_1 \xrightarrow{f_1} D_2 \xrightarrow{f_2} .....$ to denote all of Δ except D_o and f_0. By analogy, μ^{-} is $\{\mu_i \mid i \geq 1\}$. For the images of Δ and μ under ***F*** we write

$$F(\Delta) = F(D_o) \xrightarrow{F(f_o)} F(D_1) \xrightarrow{F(f_1)} F(D_2) \xrightarrow{F(f_2)} .....$$

and $F(\mu) = \{F(\mu_i) \mid i \geq 0\}$

We write F^i for the ***i***-fold iterated composition of ***F*** – that is, $F^o(f) = f, F^1(f) = F(f), F^2(f) = F(F(f))$,etc. With these definitions we can state that every monitonic function on a complete lattice has a least fixed point:

Lemma 1.4. Let ***K*** be a category with initial object $\perp$ and let $F : K \to K$ be a functor. Define the $\omega - chain \, \Delta$ by

$$\Delta = \perp \xrightarrow{!\perp \to F(\perp)} F(\perp) \xrightarrow{F(!\perp \to F(\perp))} F^2(\perp) \xrightarrow{F^2(!\perp \to F(\perp))} .....$$

If both $\mu : \Delta \to D$ and $F(\mu) : F(\Delta) \to F(D)$ are colimits, then (D,d) is an intial F-algebra, where

$d : F(D) \to D$ is the mediating arrow from $F(\mu)$ to the cocone μ^-

Theorem 1.4 Let a DAG G given in which each node is a random variable, and let a discrete conditional probability distribution of each node given values of its parents in G be specified. Then the product of these conditional distributions yields a joint probability distribution P of the variables, and (G,P) satisfies the Markov condition.

Proof. Order the nodes according to an ancestral ordering. Let $X_1, X_2, ...X_n$ be the resultant ordering. Next define.

$$P(x_1, x_2, ...x_n) = P(x_n \mid pa_n) P(x_{n-1} \mid Pa_{n-1}) ...$$
$$..P(x_2 \mid pa_2) P(x_1 \mid pa_1),$$

Where PA_i is the set of parents of X_i of in G and $P(x_i \mid pa_i)$ is the specified conditional probability distribution. First we show this does indeed yield a joint probability distribution. Clearly, $0 \le P(x_1, x_2, ...x_n) \le 1$ for all values of the variables. Therefore, to show we have a joint distribution, as the variables range through all their possible values, is equal to one. To that end, Specified conditional distributions are the conditional distributions they notationally represent in the joint distribution. Finally, we show the Markov condition is satisfied. To do this, we need show for $1 \le k \le n$ that
whenever

$$P(pa_k) \ne 0, if \;\; P(nd_k \mid pa_k) \ne 0$$
$$and \;\; P(x_k \mid pa_k) \ne 0$$
$$then \; P(x_k \mid nd_k, pa_k) = P(x_k \mid pa_k),$$

Where ND_k is the set of nondescendents of X_k of in G. Since $PA_k \subseteq ND_k$, we need only show $P(x_k \mid nd_k) = P(x_k \mid pa_k)$. First for a given k, order the nodes so that all and only nondescendents of X_k precede X_k in the ordering. Note that this ordering depends on k, whereas the ordering in the first part of the proof does not. Clearly then

$$ND_k = \{X_1, X_2, ...X_{k-1}\}$$
$$Let$$
$$D_k = \{X_{k+1}, X_{k+2}, ...X_n\}$$

follows $\sum_{d_k}$

We define the m^{th} *cyclotomic field to be the field* $Q[x]/(\Phi_m(x))$ Where $\Phi_m(x)$ is the m^{th} cyclotomic polynomial. $Q[x]/(\Phi_m(x))$ $\Phi_m(x)$ *has degree* $\varphi(m)$ *over* Q *since* $\Phi_m(x)$ has degree $\varphi(m)$. *The roots of* $\Phi_m(x)$ are just the primitive m^{th} roots of unity, so the complex embeddings of $Q[x]/(\Phi_m(x))$ *are simply the* $\varphi(m)$ *maps*

$$\sigma_k : Q[x]/(\Phi_m(x)) \mapsto C,$$
$$1 \le k \prec m, (k, m) = 1, \quad where$$
$$\sigma_k(x) = \xi_m^k,$$

ξ_m being our fixed choice of primitive m^{th} root of unity. Note that $\xi_m^k \in Q(\xi_m)$ for every k; it follows that $Q(\xi_m) = Q(\xi_m^k)$ for all k relatively prime to m. In particular, the images of the σ_i coincide, so $Q[x]/(\Phi_m(x))$ *is Galois over* Q. *This means that we can write* $Q(\xi_m)$ *for* $Q[x]/(\Phi_m(x))$ *without much fear of ambiguity; we will do so from now on, the identification being* $\xi_m \mapsto x$. *One advantage of this is that one can easily talk about cyclotomic fields being extensions of one another,or intersections or compositums; all of these things take place considering them as subfield of* C. We now investigate some basic properties of cyclotomic fields. The first issue is whether or not they are all distinct; to determine this, we need to know which roots of unity lie in $Q(\xi_m)$.Note, for example, that if m is odd, then $-\xi_m$ is a $2m^{th}$ root of unity. We will show that this is the only way in which one can obtain any non-m^{th} roots of unity.

LEMMA 1.5 If m divides n, then $Q(\xi_m)$ *is contained in* $Q(\xi_n)$

PROOF. Since $\xi^{n/m} = \xi_m$, *we have* $\xi_m \in Q(\xi_n)$, *so the result is clear*

LEMMA 1.6 If m and n are relatively prime, then

$$Q(\xi_m, \xi_n) = Q(\xi_{nm})$$

and

$$Q(\xi_m) \cap Q(\xi_n) = Q$$

(Recall the $Q(\xi_m, \xi_n)$ is the compositum of $Q(\xi_m)$ *and* $Q(\xi_n)$)

PROOF. One checks easily that $\xi_m\xi_n$ is a primitive mn^{th} root of unity, so that

$$Q(\xi_{mn}) \subseteq Q(\xi_m, \xi_n)$$
$$[Q(\xi_m, \xi_n) : Q] \le [Q(\xi_m) : Q][Q(\xi_n : Q]$$
$$= \varphi(m)\varphi(n) = \varphi(mn);$$

Since $[Q(\xi_{mn}) : Q] = \varphi(mn);$ this implies that $Q(\xi_m, \xi_n) = Q(\xi_{nm})$ We know that $Q(\xi_m, \xi_n)$ has degree $\varphi(mn)$ over Q, so we must have

$$[Q(\xi_m, \xi_n) : Q(\xi_m)] = \varphi(n)$$

and

$$[Q(\xi_m, \xi_n) : Q(\xi_m)] = \varphi(m)$$

$$[Q(\xi_m) : Q(\xi_m) \cap Q(\xi_n)] \ge \varphi(m)$$

And thus that $Q(\xi_m) \cap Q(\xi_n) = Q$

PROPOSITION 1.2 For any m and n

$$Q(\xi_m, \xi_n) = Q(\xi_{[m,n]})$$

And

$$Q(\xi_m) \cap Q(\xi_n) = Q(\xi_{(m,n)});$$

here $[m,n]$ and (m,n) denote the least common multiple and the greatest common divisor of m and n, respectively.

PROOF. Write $m = p_1^{e_1} \ldots\ldots p_k^{e_k}$ *and* $p_1^{f_1} \ldots . p_k^{f_k}$ where the p_i are distinct primes. (We allow e_i *or* f_i to be zero)

$$Q(\xi_m) = Q(\xi_{p_1^{e_1}})Q(\xi_{p_2^{e_2}}) \ldots Q(\xi_{p_k^{e_k}})$$

and

$$Q(\xi_n) = Q(\xi_{p_1^{f_1}})Q(\xi_{p_2^{f_2}}) \ldots Q(\xi_{p_k^{f_k}})$$

Thus

$$Q(\xi_m, \xi_n) = Q(\xi_{p_1^{e_1}}) \ldots\ldots\ldots Q(\xi_{p_2^{e_k}})Q(\xi_{p_1^{f_1}}) \ldots Q(\xi_{p_k^{f_k}})$$
$$= Q(\xi_{p_1^{e_1}})Q(\xi_{p_1^{f_1}}) \ldots Q(\xi_{p_k^{e_k}})Q(\xi_{p_k^{f_k}})$$
$$= Q(\xi_{p_1^{\max(e_1, f_1)}}) \ldots\ldots\ldots Q(\xi_{p_1^{\max(e_k, f_k)}})$$
$$= Q(\xi_{p_1^{\max(e_1, f_1)} \ldots\ldots\ldots p_1^{\max(e_k, f_k)}})$$
$$= Q(\xi_{[m,n]});$$

An entirely similar computation shows that $Q(\xi_m) \cap Q(\xi_n) = Q(\xi_{(m,n)})$

Mutual information measures the information transferred when x_i is sent and y_i is received, and is defined as

$$I(x_i, y_i) = \log_2 \frac{P(x_i / y_i)}{P(x_i)} \; bits \qquad (1)$$

In a noise-free channel, **each** y_i is uniquely connected to the corresponding x_i, and so they constitute an input –output pair (x_i, y_i) for which

$$P(x_i / y_j) = 1 \; and \; I(x_i, y_j) = \log_2 \frac{1}{P(x_i)} \; \text{bits;}$$

that is, the transferred information is equal to the self-information that corresponds to the input x_i In a very noisy channel, the output y_i and input x_i would be completely uncorrelated, and so $P(x_i / y_j) = P(x_i)$ and also $I(x_i, y_j) = 0;$ that is, there is no transference of information. In general, a given channel will operate between these two extremes. The mutual information is defined between the input and the output of a given channel. An average of the calculation of the mutual information for all input-output pairs of a given channel is the average mutual information:

$$I(X,Y) = \sum_{i.j} P(x_i, y_j) I(x_i, y_j) = \sum_{i.j} P(x_i, y_j) \log_2 \left[\frac{P(x_i / y_j)}{P(x_i)} \right]$$

bits per symbol . This calculation is done over the input and output alphabets. The average mutual information. The following expressions are useful for modifying the mutual information expression:

$$P(x_i, y_j) = P(x_i / y_j)P(y_j) = P(y_j / x_i)P(x_i)$$

$$P(y_j) = \sum_i P(y_j / x_i)P(x_i)$$

$$P(x_i) = \sum_i P(x_i / y_j)P(y_j)$$

Then

$$I(X,Y)=\sum_{i.j}P(x_i,y_j)$$

$$=\sum_{i.j}P(x_i,y_j)\log_2\left[\frac{1}{P(x_i)}\right]$$

$$-\sum_{i.j}P(x_i,y_j)\log_2\left[\frac{1}{P(x_i/y_j)}\right]$$

$$\sum_{i.j}P(x_i,y_j)\log_2\left[\frac{1}{P(x_i)}\right]$$

$$=\sum_{i}\left[P(x_i/y_j)P(y_j)\right]\log_2\frac{1}{P(x_i)}$$

$$\sum_{i}P(x_i)\log_2\frac{1}{P(x_i)}=H(X)$$

$$I(X,Y)=H(X)-H(X/Y)$$

Where $H(X/Y)=\sum_{i,j}P(x_i,y_j)\log_2\frac{1}{P(x_i/y_j)}$ is usually called the equivocation. In a sense, the equivocation can be seen as the information lost in the noisy channel, and is a function of the backward conditional probability. The observation of an output symbol y_j provides $H(X)-H(X/Y)$ bits of information. This difference is the mutual information of the channel. *Mutual Information: Properties* Since

$$P(x_i/y_j)P(y_j)=P(y_j/x_i)P(x_i)$$

The mutual information fits the condition

$$I(X,Y)=I(Y,X)$$

And by interchanging input and output it is also true that

$$I(X,Y)=H(Y)-H(Y/X)$$

Where

$$H(Y)=\sum_{j}P(y_j)\log_2\frac{1}{P(y_j)}$$

This last entropy is usually called the noise entropy. Thus, the information transferred through the channel is the difference between the output entropy and the noise entropy. Alternatively, it can be said that the channel mutual information is the difference between the number of bits needed for determining a given input symbol before knowing the corresponding output symbol, and the number of bits needed for determining a given input symbol after knowing the corresponding output symbol

$$I(X,Y)=H(X)-H(X/Y)$$

As the channel mutual information expression is a difference between two quantities, it seems that this parameter can adopt negative values. However, and is spite of the fact that for some $y_j, H(X/y_j)$ can be larger than $H(X)$, this is not possible for the average value calculated over all the outputs:

$$\sum_{i,j}P(x_i,y_j)\log_2\frac{P(x_i/y_j)}{P(x_i)}=\sum_{i,j}P(x_i,y_j)\log_2\frac{P(x_i,y_j)}{P(x_i)P(y_j)}$$

Then

$$-I(X,Y)=\sum_{i,j}P(x_i,y_j)\frac{P(x_i)P(y_j)}{P(x_i,y_j)}\le 0$$

Because this expression is of the form

$$\sum_{i=1}^{M}P_i\log_2(\frac{Q_i}{P_i})\le 0$$

The above expression can be applied due to the factor $P(x_i)P(y_j)$, which is the product of two probabilities, so that it behaves as the quantity Q_i, which in this expression is a dummy variable that fits the condition $\sum_i Q_i \le 1$. It can be concluded that the average mutual information is a non-negative number. It can also be equal to zero, when the input and the output are independent of each other. A related entropy called the joint entropy is defined as

$$H(X,Y)=\sum_{i,j}P(x_i,y_j)\log_2\frac{1}{P(x_i,y_j)}$$

$$=\sum_{i,j}P(x_i,y_j)\log_2\frac{P(x_i)P(y_j)}{P(x_i,y_j)}$$

$$+\sum_{i,j}P(x_i,y_j)\log_2\frac{1}{P(x_i)P(y_j)}$$

Theorem 1.5: Entropies of the binary erasure channel (BEC) The BEC is defined with an alphabet of two inputs and three outputs, with symbol probabilities.

$P(x_1)=\alpha$ *and* $P(x_2)=1-\alpha$, and transition probabilities

$P(y_3/x_2)=1-p$ *and* $P(y_2/x_1)=0$,

and $P(y_3/x_1)=0$

and $P(y_1/x_2)=p$

and $P(y_3/x_2)=1-p$

Lemma 1.7. Given an arbitrary restricted time-discrete, amplitude-continuous channel whose

restrictions are determined by sets F_n and whose density functions exhibit no dependence on the state s, let n be a fixed positive integer, and $p(x)$ an arbitrary probability density function on Euclidean n-space. $p(y \mid x)$ for the density $p_n(y_1,...,y_n \mid x_1,...x_n)$ and F *for* F_n. For any real number a, let

$$A=\left\{(x,y):\log\frac{p(y\mid x)}{p(y)}>a\right\} \qquad (1)$$

Then for each positive integer u, there is a code (u,n,λ) such that

$$\lambda \le ue^{-a}+P\{(X,Y)\notin A\}+P\{X\notin F\} \qquad (2)$$

Where

$$P\{(X,Y)\in A\}=\int_A\cdots\int p(x,y)dxdy, \qquad p(x,y)=p(x)p(y\mid x)$$

and

$$P\{X\in F\}=\int_F\cdots\int p(x)dx$$

Proof: A sequence $x^{(1)}\in F$ *such that*

$$P\left\{Y\in A_{x^1}\mid X=x^{(1)}\right\}\ge 1-\varepsilon$$

$$where\ A_x=\{y:(x,y)\varepsilon A\};$$

Choose the decoding set B_1 to be $A_{x^{(1)}}$. Having chosen $x^{(1)},.....,x^{(k-1)}$ and $B_1,...,B_{k-1}$, select $x^k\in F$ such that

$$P\left\{Y\in A_{x^{(k)}}-\bigcup_{i=1}^{k-1}B_i\mid X=x^{(k)}\right\}\ge 1-\varepsilon;$$

Set $B_k=A_{x^{(k)}}-\bigcup_{i=1}^{k-1}B_i$, If the process does not terminate in a finite number of steps, then the sequences $x^{(i)}$ and decoding sets B_i, $i=1,2,...,u,$ form the desired code. Thus assume that the process terminates after t steps. (Conceivably $t=0$). We will show $t\ge u$ by showing that $\varepsilon\le te^{-a}+P\{(X,Y)\notin A\}+P\{X\notin F\}$. We proceed as follows.

Let

$$B=\bigcup_{j=1}^{t}B_j.\quad (If\ \ t=0,\ take\ \ B=\phi).\ Then$$

$$P\{(X,Y)\in A\}=\int_{(x,y)\in A}p(x,y)dx\,dy$$

$$=\int_x p(x)\int_{y\in A_x}p(y\mid x)dy\,dx$$

$$=\int_x p(x)\int_{y\in B\cap A_x}p(y\mid x)dy\,dx+\int_x p(x)$$

IV. EXPERIMENTAL DESIGN

We evaluate the performance of our scheme and study various "what-if" scenarios through detailed simulation experiments. We compare our scheme against existing alternatives of using a least recently used (LRU) or a least frequently used (LFU) cache replacement strategy.

A. Algorithms

Ideals. Let A be a ring. Recall that an *ideal a* in A is a subset such that a is subgroup of A regarded as a group under addition;

$$a\in a, r\in A\Rightarrow ra\in A$$

The ideal generated by a subset S of A is the intersection of all ideals A containing a ----- it is easy to verify that this is in fact an ideal, and that it consist of all finite sums of the form $\sum r_i s_i$ with $r_i\in A, s_i\in S$. When $S=\{s_1,.....,s_m\}$, we shall write $(s_1,.....,s_m)$ for the ideal it generates.

Let a and b be ideals in A. The set $\{a+b\mid a\in a,b\in b\}$ is an ideal, denoted by $a+b$. The ideal generated by $\{ab\mid a\in a,b\in b\}$ is denoted by ab. Note that $ab\subset a\cap b$. Clearly ab consists of all finite sums $\sum a_i b_i$ with $a_i\in a$ and $b_i\in b$, and if $a=(a_1,...,a_m)$ and $b=(b_1,...,b_n)$, then $ab=(a_1b_1,...,a_ib_j,...,a_mb_n)$ .Let a be an ideal of A. The set of cosets of a in A forms a ring A/a, and $a\mapsto a+a$ is a homomorphism $\phi: A\mapsto A/a$. The map $b\mapsto\phi^{-1}(b)$ is a one to one correspondence between the ideals of A/a and the ideals of A containing a An ideal p if *prime* if $p\ne A$ and $ab\in p\Rightarrow a\in p$ or $b\in p$. Thus p is prime if and only if A/p is nonzero and has the property that $ab=0,\quad b\ne 0\Rightarrow a=0,$ i.e., A/p is an integral domain. An ideal m is

maximal if $m \neq | A$ and there does not exist an ideal n contained strictly between m and A. Thus m is maximal if and only if A/m has no proper nonzero ideals, and so is a field. Note that m maximal $\Rightarrow$ m prime. The ideals of $A \times B$ are all of the form $a \times b$, with a and b ideals in A and B. To see this, note that if c is an ideal in $A \times B$ and $(a,b) \in c$, then $(a,0) = (a,b)(1,0) \in c$ and $(0,b) = (a,b)(0,1) \in c$. This shows that $c = a \times b$ with

$$a = \{a \mid (a,b) \in c \ \ some \ \ b \in b\}$$

and

$$b = \{b \mid (a,b) \in c \ \ some \ \ a \in a\}$$

Let A be a ring. An A-algebra is a ring B together with a homomorphism $i_B : A \to B$. A *homomorphism of* A -algebra $B \to C$ is a homomorphism of rings $\varphi : B \to C$ such that $\varphi(i_B(a)) = i_C(a)$ for all $a \in A$. An A-algebra B is said to be *finitely generated* (or of *finite-type* over A) if there exist elements $x_1, ..., x_n \in B$ such that every element of B can be expressed as a polynomial in the x_i with coefficients in $i(A)$, i.e., such that the homomorphism $A[X_1, ..., X_n] \to B$ sending X_i to x_i is surjective. A ring homomorphism $A \to B$ is *finite*, and B is finitely generated as an A-module. Let k be a field, and let A be a k -algebra. If $1 \neq 0$ in A, then the map $k \to A$ is injective, we can identify k with its image, i.e., we can regard k as a subring of A. If 1=0 in a ring R, the R is the zero ring, i.e., $R = \{0\}$. **Polynomial rings.** Let k be a field. A *monomial* in $X_1, ..., X_n$ is an expression of the form $X_1^{a_1} ... X_n^{a_n}$, $a_j \in N$. The *total degree* of the monomial is $\sum a_i$. We sometimes abbreviate it by X^{α}, $\alpha = (a_1, ..., a_n) \in \square^n$. The elements of the polynomial ring $k[X_1, ..., X_n]$ are finite sums $\sum c_{a_1 ... a_n} X_1^{a_1} ... X_n^{a_n}$, $c_{a_1 ... a_n} \in k$, $a_j \in \square$ With the obvious notions of equality, addition and multiplication. Thus the monomials from basis for $k[X_1, ..., X_n]$ as a k -vector space. The ring $k[X_1, ..., X_n]$ is an integral domain, and the only units in it are the nonzero constant polynomials. A polynomial $f(X_1, ..., X_n)$ is *irreducible* if it is nonconstant and has only the obvious factorizations, i.e., $f = gh \Rightarrow g$ or h is constant. **Division in** $k[X]$. The division algorithm allows us to divide a nonzero polynomial into another: let f and g be polynomials in $k[X]$ with $g \neq 0$; then there exist unique polynomials $q, r \in k[X]$ such that $f = qg + r$ with either $r = 0$ or $\deg r < \deg g$. Moreover, there is an algorithm for deciding whether $f \in (g)$, namely, find r and check whether it is zero. Moreover, the Euclidean algorithm allows to pass from finite set of generators for an ideal in $k[X]$ to a single generator by successively replacing each pair of generators with their greatest common divisor.

(Pure) ***lexicographic*** *ordering (lex).* Here monomials are ordered by lexicographic(dictionary) order. More precisely, let $\alpha = (a_1, ...a_n)$ and $\beta = (b_1, ...b_n)$ be two elements of $\square^n$; then $\alpha > \beta$ *and* $X^{\alpha} > X^{\beta}$ (lexicographic ordering) if, in the vector difference $\alpha - \beta \in \square$, the left most nonzero entry is positive. For example, $XY^2 > Y^3Z^4$; $X^3Y^2Z^4 > X^3Y^2Z$. Note that this isn't quite how the dictionary would order them: it would put $XXXYYZZZZ$ after $XXXYYZ$. *Graded reverse lexicographic order (grevlex).* Here monomials are ordered by total degree, with ties broken by reverse lexicographic ordering. Thus, $\alpha > \beta$ if $\sum a_i > \sum b_i$, or $\sum a_i = \sum b_i$ and in $\alpha - \beta$ the right most nonzero entry is negative. For example:

$X^4Y^4Z^7 > X^5Y^5Z^4$ *(total degree greater)*

$XY^5Z^2 > X^4YZ^3$, $X^5YZ > X^4YZ^2$.

Orderings on $k[X_1, ...X_n]$. Fix an ordering on the monomials in $k[X_1, ...X_n]$. Then we can write an element f of $k[X_1, ...X_n]$ in a canonical fashion, by re-ordering its elements in decreasing order. For example, we would write

$$f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$$

as

$$f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2 \quad (lex)$$

or

$$f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2 \quad (grevlex)$$

Let $\sum a_\alpha X^\alpha \in k[X_1,...,X_n]$, in decreasing order:

$$f = a_{\alpha_0} X^{\alpha_0} + a_{\alpha_1} X^{\alpha_1} + ..., \quad \alpha_0 > \alpha_1 > ..., \quad \alpha_0 \neq 0$$

Then we define.

- The *multidegree* of f to be multdeg(f)= α_0 ;
- The *leading coefficient of* f to be *LC*(f)= a_{α_0} ;
- The *leading monomial of* f to be *LM*(f) = X^{α_0} ;
- The *leading term of* f to be *LT*(f) = $a_{\alpha_0} X^{\alpha_0}$

For the polynomial $f = 4XY^2Z + ...$, the multidegree is (1,2,1), the leading coefficient is 4, the leading monomial is XY^2Z , and the leading term is $4XY^2Z$. **The division algorithm in** $k[X_1,...X_n]$. Fix a monomial ordering in $\mathbb{N}^2$. Suppose given a polynomial f and an ordered set $(g_1,...g_s)$ of polynomials; the division algorithm then constructs polynomials $a_1,...a_s$ and r such that $f = a_1g_1 + ... + a_sg_s + r$ Where either $r = 0$ or no monomial in r is divisible by any of $LT(g_1),...,LT(g_s)$ **Step 1:** If $LT(g_1) \mid LT(f)$, divide g_1 into f to get

$$f = a_1g_1 + h, \quad a_1 = \frac{LT(f)}{LT(g_1)} \in k[X_1,...,X_n]$$

If $LT(g_1) \mid LT(h)$, repeat the process until $f = a_1g_1 + f_1$ (different a_1) with $LT(f_1)$ not divisible by $LT(g_1)$. Now divide g_2 into f_1, and so on, until $f = a_1g_1 + ... + a_sg_s + r_1$ With $LT(r_1)$ not divisible by any $LT(g_1),...LT(g_s)$

Step 2: Rewrite $r_1 = LT(r_1) + r_2$, and repeat Step 1 with r_2 for f : $f = a_1g_1 + ... + a_sg_s + LT(r_1) + r_3$ (different a_i's) **Monomial ideals.** In general, an ideal a will contain a polynomial without containing the individual terms of the polynomial; for example, the ideal $a = (Y^2 - X^3)$ contains $Y^2 - X^3$ but not Y^2 or X^3.

DEFINITION 1.5. An ideal a is *monomial* if $\sum c_\alpha X^\alpha \in a \Rightarrow X^\alpha \in a$ all α with $c_\alpha \neq 0$.

PROPOSITION 1.3. Let a be a *monomial ideal*, and let $A = \{\alpha \mid X^\alpha \in a\}$. Then A satisfies the condition $\alpha \in A, \ \beta \in \mathbb{N}^n \Rightarrow \alpha + \beta \in$ (*) And a is the k -subspace of $k[X_1,...,X_n]$ generated by the $X^\alpha, \alpha \in A$. Conversely, of A is a subset of $\mathbb{N}^n$ satisfying $(*)$, then the k-subspace a of $k[X_1,...,X_n]$ generated by $\{X^\alpha \mid \alpha \in A\}$ is a monomial ideal.

PROOF. It is clear from its definition that a monomial ideal a is the k -subspace of $k[X_1,...,X_n]$ generated by the set of monomials it contains. If $X^\alpha \in a$ and $X^\beta \in k[X_1,...,X_n]$.

If a permutation is chosen uniformly and at random from the $n!$ possible permutations in S_n, then the counts $C_j^{(n)}$ of cycles of length j are dependent random variables. The joint distribution of $C^{(n)} = (C_1^{(n)},...,C_n^{(n)})$ follows from Cauchy's formula, and is given by

$$P[C^{(n)} = c] = \frac{1}{n!} N(n,c) = 1\left\{\sum_{j=1}^n jc_j = n\right\} \prod_{j=1}^n \left(\frac{1}{j}\right)^{c_j} \frac{1}{c_j!}, \qquad (1.1)$$

for $c \in \mathbb{N}_+^n$.

Lemma1.7 For nonnegative integers $m_1,...,m_n$,

$$E\left(\prod_{j=1}^n (C_j^{(n)})^{[m_j]}\right) = \left(\prod_{j=1}^n \left(\frac{1}{j}\right)^{m_j}\right) 1\left\{\sum_{j=1}^n jm_j \le n\right\} \qquad (1.4)$$

Proof. This can be established directly by exploiting cancellation of the form $c_j^{[m_j]} / c_j^! = 1/(c_j - m_j)!$ when $c_j \ge m_j$, which occurs between the ingredients in Cauchy's formula and the falling factorials in the moments. Write $m = \sum jm_j$. Then, with the first sum indexed by $c = (c_1,...c_n) \in \mathbb{N}_+^n$ and the last sum indexed by $d = (d_1,...,d_n) \in \mathbb{N}_+^n$ via the correspondence $d_j = c_j - m_j$, we have

$$E\left(\prod_{j=1}^{n}(C_j^{(n)})^{[m_j]}\right)=\sum_c P[C^{(n)}=c]\prod_{j=1}^{n}(c_j)^{[m_j]}$$

$$=\sum_{c:c_j\geq m_j \text{ for all } j} 1\left\{\sum_{j=1}^{n} jc_j=n\right\}\prod_{j=1}^{n}\frac{(c_j)^{[m_j]}}{j^{c_j}c_j!}$$

$$=\prod_{j=1}^{n}\frac{1}{j^{m_j}}\sum_d 1\left\{\sum_{j=1}^{n} jd_j=n-m\right\}\prod_{j=1}^{n}\frac{1}{j^{d_j}(d_j)!}$$

This last sum simplifies to the indicator $1(m\leq n),$ corresponding to the fact that if $n-m\geq 0,$ then $d_j=0$ for $j>n-m,$ and a random permutation in S_{n-m} must have some cycle structure $(d_1,...,d_{n-m})$. The moments of $C_j^{(n)}$ follow immediately as

$$E(C_j^{(n)})^{[r]}=j^{-r}1\{jr\leq n\} \qquad (1.2)$$

We note for future reference that (1.4) can also be written in the form

$$E\left(\prod_{j=1}^{n}(C_j^{(n)})^{[m_j]}\right)=E\left(\prod_{j=1}^{n}Z_j^{[m_j]}\right)1\left\{\sum_{j=1}^{n} jm_j\leq n\right\}, \qquad (1.3)$$

Where the Z_j are independent Poisson-distribution random variables that satisfy $E(Z_j)=1/j$

The marginal distribution of cycle counts provides a formula for the joint distribution of the cycle counts C_j^n, we find the distribution of C_j^n using a combinatorial approach combined with the inclusion-exclusion formula.

Lemma 1.8. For $1\leq j\leq n,$

$$P[C_j^{(n)}=k]=\frac{j^{-k}}{k!}\sum_{l=0}^{[n/j]-k}(-1)^l\frac{j^{-l}}{l!} \qquad (1.1)$$

Proof. Consider the set I of all possible cycles of length $j,$ formed with elements chosen from $\{1,2,...n\},$ so that $|I|=n^{[j]/j}$. For each $\alpha\in I,$ consider the "property" G_α of having $\alpha;$ that is, G_α is the set of permutations $\pi\in S_n$ such that α is one of the cycles of π. We then have $|G_\alpha|=(n-j)!,$ since the elements of $\{1,2,...,n\}$ not in α must be permuted among themselves. To use the inclusion-exclusion formula we need to calculate the term $S_r,$ which is the sum of the probabilities of the r-fold intersection of properties, summing over all sets of r distinct properties. There are two cases to consider. If the r properties are indexed by r cycles having no elements in common, then the intersection specifies how rj elements are moved by the permutation, and there are $(n-rj)!1(rj\leq n)$ permutations in the intersection. There are $n^{[rj]}/(j^r r!)$ such intersections. For the other case, some two distinct properties name some element in common, so no permutation can have both these properties, and the r-fold intersection is empty. Thus

$$S_r=(n-rj)!1(rj\leq n)$$

$$\times\frac{n^{[rj]}}{j^r r!}\frac{1}{n!}=1(rj\leq n)\frac{1}{j^r r!}$$

Finally, the inclusion-exclusion series for the number of permutations having exactly k properties is

$$\sum_{l\geq 0}(-1)^l\binom{k+l}{l}S_{k+l},$$

Which simplifies to (1.1) Returning to the original hat-check problem, we substitute j=1 in (1.1) to obtain the distribution of the number of fixed points of a random permutation. For $k=0,1,...,n,$

$$P[C_1^{(n)}=k]=\frac{1}{k!}\sum_{l=0}^{n-k}(-1)^l\frac{1}{l!}, \qquad (1.2)$$

and the moments of $C_1^{(n)}$ follow from (1.2) with $j=1.$ In particular, for $n\geq 2,$ the mean and variance of $C_1^{(n)}$ are both equal to 1. The joint distribution of $(C_1^{(n)},...,C_b^{(n)})$ for any $1\leq b\leq n$ has an expression similar to (1.7); this too can be derived by inclusion-exclusion. For any $c=(c_1,...,c_b)\in\square_+^b$ with $m=\sum ic_i,$

$$P[(C_1^{(n)},...,C_b^{(n)})=c]$$

$$=\left\{\prod_{i=1}^{b}\left(\frac{1}{i}\right)^{c_i}\frac{1}{c_i!}\right\}\sum_{\substack{l\geq 0 \text{ with}\\ \sum il_i\leq n-m}}(-1)^{l_1+...+l_b}\prod_{i=1}^{b}\left(\frac{1}{i}\right)^{l_i}\frac{1}{l_i!} \qquad (1.3)$$

The joint moments of the first b counts $C_1^{(n)},...,C_b^{(n)}$ can be obtained directly from (1.2) and (1.3) by setting $m_{b+1}=...=m_n=0$

The limit distribution of cycle counts

It follows immediately from Lemma 1.2 that for each fixed $j,$ as $n\to\infty,$

$$P[C_j^{(n)}=k]\to\frac{j^{-k}}{k!}e^{-1/j}, \quad k=0,1,2,...,$$

So that $C_j^{(n)}$ converges in distribution to a random variable Z_j having a Poisson distribution with mean $1/j;$ we use the notation $C_j^{(n)}\to_d Z_j$

where $Z_j \sim P_o(1/j)$ to describe this. Infact, the limit random variables are independent.

Theorem 1.6 The process of cycle counts converges in distribution to a Poisson process of $\sim$ with intensity j^{-1}. That is, as $n \to \infty$,

$$(C_1^{(n)}, C_2^{(n)}, ...) \to_d (Z_1, Z_2, ...) \quad (1.1)$$

Where the $Z_j, j = 1, 2, ...,$ are independent Poisson-distributed random variables with $E(Z_j) = \frac{1}{j}$

Proof. To establish the converges in distribution one shows that for each fixed $b \geq 1$, as $n \to \infty$,

$$P[(C_1^{(n)}, ..., C_b^{(n)}) = c] \to P[(Z_1, ..., Z_b) = c]$$

Error rates

The proof of Theorem says nothing about the rate of convergence. Elementary analysis can be used to estimate this rate when $b = 1$. Using properties of alternating series with decreasing terms, for $k = 0, 1, ..., n$,

$$\frac{1}{k!}\left(\frac{1}{(n-k+1)!} - \frac{1}{(n-k+2)!}\right) \leq \left|P[C_1^{(n)} = k] - P[Z_1 = k]\right| \leq \frac{1}{k!(n-k+1)!}$$

It follows that

$$\frac{2^{n+1}}{(n+1)!}\frac{n}{n+2} \leq \sum_{k=0}^{n}\left|P[C_1^{(n)} = k] - P[Z_1 = k]\right| \leq \frac{2^{n+1}-1}{(n+1)!} \quad (1.11)$$

Since

$$P[Z_1 > n] = \frac{e^{-1}}{(n+1)!}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + ...\right) < \frac{1}{(n+1)!},$$

We see from (1.11) that the total variation distance between the distribution $L(C_1^{(n)})$ of $C_1^{(n)}$ and the distribution $L(Z_1)$ of Z_1

B. Motivation for Trust Management in Mobile AdHoc Network (MANET)

The concept of "Trust" originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [5]. Blaze et al. [6] first introduced the term "Trust Management" and identified it as a separate component of security services in networks and clarified that "Trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships." Trust management in MANETs is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Examples would be in building initial trust bootstrapping [7], coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone [8]. In addition, trust management has diverse applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes. Trust management, including trust establishment, trust update, and trust revocation, in MANETs is also much more challenging than in traditional centralized environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. The dynamic nature and characteristics of MANETs result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time [8] [9]. Despite a couple of surveys of trust management [10] [11] [12], a comprehensive survey of trust management in MANETs does not exist and is the main aim of this paper. A short version of this paper was presented at ICCRTS 2009 [13]. The contributions of this paper are: (1) to give a clear definition of trust in the communication and networking field, drawing upon definitions from different disciplines; (2) to extensively survey the existing trust management schemes developed for MANETs and investigate their general trends; and (3) to discuss future research areas based on the concept of social and cognitive networks. The rest of this paper is organized as follows. In Section 2, we discuss the concept of trust in diverse disciplines, give a clear distinction between trust and trustworthiness, and discuss the relationship between trust and risk. We also introduce the main properties of trust in MANETs. Section 3 surveys generally accepted classifications of trust management, attacks considered in existing trust management schemes for MANETs, and metrics used to measure the performance of existing MANET trust management schemes. Section 4 surveys trust management schemes that have been developed for specific purposes, including secure routing, authentication, intrusion detection, access control, key management, and trust evidence distribution and evaluation. In Section 5, we discuss design concepts that designers of MANET trust management systems should keep in mind and suggest trust metrics based on the concepts of social trust and quality-of-service (QoS) trust. Section 6 concludes this paper. In recent years, there has been an increasing interest in providing security for multiagent systems. One of the major concerns in multiagent systems security is access control management. This is due to the social

nature of multiagent systems, where individual agents work together either in cooperative or competitive manner to solve problems that are beyond the capabilities and knowledge of each individual agent. The obvious and direct solution to maintain access control for multiagent systems is to reuse and extend the current well known access control mechanisms applicable to distributed systems. Unfortunately, those access control mechanisms do not scale adequately or provide the increased flexibility required by multiagent systems [1, 2]. In order to provide an effective, yet flexible access control management for multiagent systems, there are some requirements that should be taken into consideration. First, it should be distributed with no central control in order to be scalable and able to cope with the highly distributed and decentralized nature of multiagent systems. Second, it should be automated to cope with the dynamics of multiagent systems. This is because agents are frequently changing their roles which require a corresponding dynamic change in their access control information. Third, it shouldn't depend on agents' identities, because knowing the true identities of agents is considered to be uninformative in multiagent systems simply due to the open nature of multiagent systems, where agents can appear and disappear at anytime, thus the interacting agents may not know each other a priori. Finally, it should consider the heterogeneous nature of multiagent systems; hence, access control information should be represented using a syntax and semantics interoperable terminology. Fortunately all those requirements can be met by applying trust management model for access control [1, 2]. Trust Management is an emerging field of research that provides a promising framework for access control decentralization. It enables communicating agents to make access control decisions based on agents' attributes and other trust-related factors rather than agents' identities. There are two well known trust management approaches that well suit multiagent systems; policy-based approach and reputation-based approach. Policy-based trust management approach (also called credential-based trust management) is basically founded on signed digital credentials that enclose agents' non subjective properties, and policies encoded in logical rules with well defined semantics [3]. Thus, it provides a strong verification and analysis support. In general, policy-based trust is intended for systems with strong protection requirements, and for systems whose behavior is guided by complex rules that could be easily changeable. However, in some application domains, holding credentials does not necessarily imply that the user is trustworthy. Furthermore, policy-based trust management provides a static form of trust given the same credentials, and this is not sufficient for some applications as agents may change their attitudes according to their self-interest. Finally, policy-based trust results only in binary trust values, implying that an agent either is completely trusted or distrusted. Conversely in some applications, entities need to express partial trust in other peers. Reputation-based trust management approach basically depends on computing reputation measures that are intimately related to perceptions on earlier direct interactions, or indirect interactions where an agent relies on recommendations (i.e. feedbacks from other agents) [4]. This approach provides a trust value that have continuous range (e.g. [0,1]) or a group of discrete values (e.g. high, medium, low). It also provides a dynamic form of trust, where the trust value increases or decreases based on new interactions or new recommendations. However, unfortunately, reputation-based trust management using interactions approach offers a malicious agent the opportunity to manipulate recommendations to its best interests. Another problem with reputation-based trust management using interactions is that newcomers to the systems face a problem because they have no previous interactions with any agent in the system. It becomes clear that each trust management approach has its strengths and weaknesses, and hence through integration they can effectively complement each other and provide a more reliable and accurate measure of trust. Moreover, an integrated approach becomes suitable for being applied to diverse set of applications. For instance, in some applications policy-based model alone or reputation-based model alone cannot guarantee a satisfactory level of trust. As the case in applying for a loan from a bank; in order for the bank to take a decision whether or not to guarantee the applicant the loan, the bank requires not only some credentials (e.g. proof of income, identification proof, age proof, address proof, etc.), but also it has to make some investigations about past transactions of the applicant either with this bank or with other banks (which this bank trusts). For example, the bank may ask other banks about the reputation of the applicant concerning cheques' returns. It may also ask about the reputation of the applicant regarding the applicant's commitment in paying periodic payments of previous loans, if any. Obviously, the bank is integrating between a policy-based approach and a reputation-based approach for trust management. In the light of this, we propose DiReCT, Dirichlet-based Reputation and Credential Trust, a trust management-based decentralized access control framework for multiagent systems that integrates between policy-based and reputation-based trust management approaches. Unlike other reputation computation approaches such as simple summation or average, which are considered primitive and therefore provide a poor picture for the reputation values, DiReCT employs a probabilistic approach for reputation evaluation by adopting Bayesian systems using Dirichlet reputation system which is based on the Dirichlet probability distribution [5]. Dirichlet reputation systems are initially introduced by Audun

Jøsang [6]. However, Audun had applied Dirichlet reputation systems using a centralized approach not suitable for multiagent systems. Bayesian systems have a solid mathematical foundations and therefore they provide a theoretically sound basis for computing reputation values [7]. DiReCT also uses a semantically enriched rule-based policy specification and management by adopting the standard Semantic Web Rule Language (SWRL) [8].Using a semantic web language provides syntax and semantics interoperability between agents. Furthermore, SWRL is considerably more powerful than both OWL-DL or Horn clause rules alone, and thus it has a lot of potentials that make it capable of representing trust management policies for multiagent systems. The remainder of the paper is organized as follows. The next section presents the related work. Section 3 presents an overview of DiReCT. DiReCT reputation model and DiReCT policy model are presented in Sections 4 and 5 respectively. Implementation details are presented in Section 6, while a case study is presented in Section 7. Finally, Section 8 concludes this paper and outlines the future work. With the pervasiveness of Internet, more and more people and enterprises are involved in e-commerce. For example, Taobao, the largest online shopping site in China, had a total of 98 million registered users by the end of 2008. However, the openness of Internet brings serious challenge to e-commerce transaction security. To ensure secure online transaction, security technologies including network security, information encryption, identify authentication and security protocol for ecommerce are studied and applied extensively. However, problems due to asymmetric information and lacking of effective credit evaluation system and punishment mechanism for losing credit have limited the further development of ecommerce. Therefore it is necessary to establish trust recommendation mechanism and make the transaction entities (buyers and sellers) know their potential transaction partners' reputation from global and local perspectives. It is well known that effective trust mechanism is essential to foster trustworthy e-commerce environment. The rest of this paper is organized as follows. The concepts of trust and trust management, several typical trust management models for e-commerce are given in Section 2. In Section 3, the trust attributes of the transaction entity in ecommerce are identified, and trust feature vector is defined. Then a trust fuzzy clustering-based management model for ecommerce is established; corresponding trust calculation algorithm is described in detail. The effectiveness of trust management model and trust calculation algorithm.

Establish the asymptotics of $\mathrm{P}\left[A_n(C^{(n)})\right]$ under conditions (A_0) and (B_{01}), where

$$A_n(C^{(n)}) = \bigcap_{1\le i\le n} \bigcap_{r_i'+1\le j\le r_i} \left\{C_{ij}^{(n)} = 0\right\},$$

and $\zeta_i = (r_i'/r_{id}) - 1 = O(i^{-g'})$ as $i \to \infty$, for some $g' > 0$. We start with the expression

$$P[A_n(C^{(n)})] = \frac{P[T_{0m}(Z') = n]}{P[T_{0m}(Z) = n]}$$

$$\prod_{\substack{1\le i\le n \\ r_i'+1\le j\le r_i}} \left\{1 - \frac{\theta}{ir_i}(1+E_{i0})\right\} \qquad (1.1)$$

$$P[T_{0n}(Z') = n]$$

$$= \frac{\theta d}{n} \exp\left\{\sum_{i\ge 1}[\log(1+i^{-1}\theta d) - i^{-1}\theta d]\right\}$$

$$\left\{1 + O(n^{-1}\varphi'_{\{1,2,7\}}(n))\right\} \qquad (1.2)$$

and

$$P[T_{0n}(Z') = n]$$

$$= \frac{\theta d}{n} \exp\left\{\sum_{i\ge 1}[\log(1+i^{-1}\theta d) - i^{-1}\theta d]\right\}$$

$$\left\{1 + O(n^{-1}\varphi_{\{1,2,7\}}(n))\right\} \qquad (1.3)$$

Where $\varphi'_{\{1,2,7\}}(n)$ refers to the quantity derived from Z'. It thus follows that $P[A_n(C^{(n)})] \sim Kn^{-\theta(1-d)}$ for a constant K, depending on Z and the r_i' and computable explicitly from (1.1) – (1.3), if Conditions (A_0) and (B_{01}) are satisfied and if $\zeta_i^* = O(i^{-g'})$ from some $g' > 0$, since, under these circumstances, both $n^{-1}\varphi'_{\{1,2,7\}}(n)$ and $n^{-1}\varphi_{\{1,2,7\}}(n)$ tend to zero as $n \to \infty$. In particular, for polynomials and square free polynomials, the relative error in this asymptotic approximation is of order n^{-1} if $g' > 1$.

For $0 \le b \le n/8$ and $n \ge n_0$, with n_0

$$d_{TV}(L(C[1,b]), L(Z[1,b]))$$

$$\le d_{TV}(L(\tilde{C}[1,b]), L(\tilde{Z}[1,b]))$$

$$\le \varepsilon_{\{7,7\}}(n,b),$$

Where $\varepsilon_{\{7,7\}}(n,b) = O(b/n)$ under Conditions $(A_0), (D_1)$ and (B_{11}) Since, by the Conditioning Relation,

$$L(\tilde{C}[1,b]\,|\,T_{0b}(C)=l)=L(\tilde{Z}[1,b]\,|\,T_{0b}(Z)=l),$$

It follows by direct calculation that

$$d_{TV}(L(\tilde{C}[1,b]),L(\tilde{Z}[1,b]))$$
$$=d_{TV}(L(T_{0b}(C)),L(T_{0b}(Z)))$$
$$=\max_{A}\sum_{r\in A}P[T_{0b}(Z)=r]$$
$$\left\{1-\frac{P[T_{bn}(Z)=n-r]}{P[T_{0n}(Z)=n]}\right\} \qquad (1.4)$$

Suppressing the argument Z from now on, we thus obtain

$$d_{TV}(L(\tilde{C}[1,b]),L(\tilde{Z}[1,b]))$$
$$=\sum_{r\geq 0}P[T_{0b}=r]\left\{1-\frac{P[T_{bn}=n-r]}{P[T_{0n}=n]}\right\}_{+}$$
$$\leq\sum_{r>n/2}P[T_{0b}=r]+\sum_{r=0}^{[n/2]}\frac{P[T_{0b}=r]}{P[T_{0b}=n]}$$
$$\times\left\{\sum_{s=0}^{n}P[T_{0b}=s](P[T_{bn}=n-s]-P[T_{bn}=n-r]\right\}_{+}$$
$$\leq\sum_{r>n/2}P[T_{0b}=r]+\sum_{r=0}^{[n/2]}P[T_{0b}=r]$$
$$\times\sum_{s=0}^{[n/2]}P[T_{0b}=s]\frac{\{P[T_{bn}=n-s]-P[T_{bn}=n-r]\}}{P[T_{0n}=n]}$$
$$+\sum_{s=0}^{[n/2]}P[T_{0b}=r]\sum_{s=[n/2]+1}^{n}P[T=s]P[T_{bn}=n-s]/P[T_{0n}=n]$$

The first sum is at most $2n^{-1}ET_{0b}$; the third is bound by

$$(\max_{n/2<s\leq n}P[T_{0b}=s])/P[T_{0n}=n]$$
$$\leq\frac{2\varepsilon_{\{10.5(1)\}}(n/2,b)}{n}\frac{3n}{\theta P_{\theta}[0,1]},$$
$$\frac{3n}{\theta P_{\theta}[0,1]}4n^{-2}\phi^{*}_{\{10.8\}}(n)\sum_{r=0}^{[n/2]}P[T_{0b}=r]\sum_{s=0}^{[n/2]}P[T_{0b}=s]\frac{1}{2}|r-s|$$
$$\leq\frac{12\phi^{*}_{\{10.8\}}(n)}{\theta P_{\theta}[0,1]}\frac{ET_{0b}}{n}$$

Hence we may take

$$\varepsilon_{\{7,7\}}(n,b)=2n^{-1}ET_{0b}(Z)\left\{1+\frac{6\phi^{*}_{\{10.8\}}(n)}{\theta P_{\theta}[0,1]}\right\}P$$
$$+\frac{6}{\theta P_{\theta}[0,1]}\varepsilon_{\{10.5(1)\}}(n/2,b) \qquad (1.5)$$

Required order under Conditions $(A_0),(D_1)$ and (B_{11}), if $S(\infty)<\infty$. If not, $\phi^{*}_{\{10.8\}}(n)$ can be replaced by $\phi^{*}_{\{10.11\}}(n)$ in the above, which has the required order, without the restriction on the r_i implied by $S(\infty)<\infty$. Examining the Conditions $(A_0),(D_1)$ and (B_{11}), it is perhaps surprising to find that (B_{11}) is required instead of just (B_{01}); that is, that we should need $\sum_{l\geq 2}l\varepsilon_{il}=O(i^{-a_1})$ to hold for some $a_1>1$. A first observation is that a similar problem arises with the rate of decay of ε_{i1} as well. For this reason, n_1 is replaced by $\tilde{n}_1$. This makes it possible to replace condition (A_1) by the weaker pair of conditions (A_0) and (D_1) in the eventual assumptions needed for $\varepsilon_{\{7,7\}}(n,b)$ to be of order $O(b/n)$; the decay rate requirement of order $i^{-1-\gamma}$ is shifted from ε_{i1} itself to its first difference. This is needed to obtain the right approximation error for the random mappings example. However, since all the classical applications make far more stringent assumptions about the $\varepsilon_{i1}, l\geq 2$, than are made in (B_{11}). The critical point of the proof is seen where the initial estimate of the difference $P[T^{(m)}_{bn}=s]-P[T^{(m)}_{bn}=s+1]$. The factor $\varepsilon_{\{10.10\}}(n)$, which should be small, contains a far tail element from $\tilde{n}_1$ of the form $\phi^{\theta}_{1}(n)+u^{*}_{1}(n)$, which is only small if $a_1>1$, being otherwise of order $O(n^{1-a_1+\delta})$ for any $\delta>0$, since $a_2>1$ is in any case assumed. For $s\geq n/2$, this gives rise to a contribution of order $O(n^{-1-a_1+\delta})$ in the estimate of the difference $P[T_{bn}=s]-P[T_{bn}=s+1]$, which, in the remainder of the proof, is translated into a contribution of order $O(tn^{-1-a_1+\delta})$ for differences of the form $P[T_{bn}=s]-P[T_{bn}=s+1]$, finally leading to a contribution of order $bn^{-a_1+\delta}$ for any $\delta>0$ in $\varepsilon_{\{7.7\}}(n,b)$. Some improvement would seem to be possible, defining the function g by $g(w)=1_{\{w=s\}}-1_{\{w=s+t\}}$, differences that are of the form $P[T_{bn}=s]-P[T_{bn}=s+t]$ can be

directly estimated, at a cost of only a single contribution of the form $\phi_1^{\theta}(n)+u_1^*(n)$. Then, iterating the cycle, in which one estimate of a difference in point probabilities is improved to an estimate of smaller order, a bound of the form

$$\left|P[T_{bn}=s]-P[T_{bn}=s+t]\right|=O(n^{-2}t+n^{-1-a_1+\delta})$$

for any $\delta>0$ could perhaps be attained, leading to a final error estimate in order $O(bn^{-1}+n^{-a_1+\delta})$ for any $\delta>0$, to replace $\varepsilon_{\{7.7\}}(n,b)$. This would be of the ideal order $O(b/n)$ for large enough b, but would still be coarser for small b.

With b and n as in the previous section, we wish to show that

$$\left|d_{TV}(L(C[1,b]),L(Z[1,b]))-\frac{1}{2}(n+1)^{-1}\left|1-\theta\right|E\left|T_{0b}-ET_{0b}\right|\right|$$
$$\le\varepsilon_{\{7.8\}}(n,b),$$

Where $\varepsilon_{\{7.8\}}(n,b)=O(n^{-1}b[n^{-1}b+n^{-\beta_{12}+\delta}])$ for any $\delta>0$ under Conditions $(A_0),(D_1)$ and (B_{12}), with β_{12}. The proof uses sharper estimates. As before, we begin with the formula

$$d_{TV}(L(\tilde{C}[1,b]),L(\tilde{Z}[1,b]))$$
$$=\sum_{r\ge0}P[T_{0b}=r]\left\{1-\frac{P[T_{bn}=n-r]}{P[T_{0n}=n]}\right\}_+$$

Now we observe that

$$\left|\sum_{r\ge0}P[T_{0b}=r]\left\{1-\frac{P[T_{bn}=n-r]}{P[T_{0n}=n]}\right\}_+-\sum_{r=0}^{[n/2]}\frac{P[T_{0b}=r]}{P[T_{0n}=n]}\right|$$
$$\times\left|\sum_{s=[n/2]+1}^{n}P[T_{0b}=s](P[T_{bn}=n-s]-P[T_{bn}=n-r])\right|$$
$$\le4n^{-2}ET_{0b}^2+(\max_{n/2<s\le n}P[T_{0b}=s])/P[T_{0n}=n]$$
$$+P[T_{0b}>n/2]$$
$$\le8n^{-2}ET_{0b}^2+\frac{3\varepsilon_{\{10.5(2)\}}(n/2,b)}{\theta P_\theta[0,1]},\qquad(1.1)$$

We have

$$\left|\sum_{r=0}^{[n/2]}\frac{P[T_{0b}=r]}{P[T_{0n}=n]}\right.$$
$$\times\left(\left\{\sum_{s=0}^{[n/2]}P[T_{0b}=s](P[T_{bn}=n-s]-P[T_{bn}=n-r]\right\}_+\right.$$
$$\left.\left.-\left\{\sum_{s=0}^{[n/2]}P[T_{0b}=s]\frac{(s-r)(1-\theta)}{n+1}P[T_{0n}=n]\right\}_+\right)\right|$$
$$\le\frac{1}{n^2P[T_{0n}=n]}\sum_{r\ge0}P[T_{0b}=r]\sum_{s\ge0}P[T_{0b}=s]\left|s-r\right|$$
$$\times\left\{\varepsilon_{\{10.14\}}(n,b)+2(r\vee s)\left|1-\theta\right|n^{-1}\left\{K_0\theta+4\phi^*_{\{10.8\}}(n)\right\}\right\}$$
$$\le\frac{6}{\theta nP_\theta[0,1]}ET_{0b}\varepsilon_{\{10.14\}}(n,b)$$
$$+4\left|1-\theta\right|n^{-2}ET_{0b}^2\left\{K_0\theta+4\phi^*_{\{10.8\}}(n)\right\}$$
$$\left(\frac{3}{\theta nP_\theta[0,1]}\right)\Big\},\qquad(1.2)$$

The approximation in (1.2) is further simplified by noting that

$$\sum_{r=0}^{[n/2]}P[T_{0b}=r]\left|\left\{\sum_{s=0}^{[n/2]}P[T_{0b}=s]\frac{(s-r)(1-\theta)}{n+1}\right\}_+\right.$$
$$\left.-\left\{\sum_{s=0}^{[n/2]}P[T_{0b}=s]\frac{(s-r)(1-\theta)}{n+1}\right\}_+\right|$$
$$\le\sum_{r=0}^{[n/2]}P[T_{0b}=r]\sum_{s>[n/2]}P[T_{0b}=s]\frac{(s-r)\left|1-\theta\right|}{n+1}$$
$$\le\left|1-\theta\right|n^{-1}E(T_{0b}1\{T_{0b}>n/2\})\le2\left|1-\theta\right|n^{-2}ET_{0b}^2,\qquad(1.3)$$

and then by observing that

$$\sum_{r>[n/2]}P[T_{0b}=r]\left\{\sum_{s\ge0}P[T_{0b}=s]\frac{(s-r)(1-\theta)}{n+1}\right\}$$
$$\le n^{-1}\left|1-\theta\right|(ET_{0b}P[T_{0b}>n/2]+E(T_{0b}1\{T_{0b}>n/2\}))$$
$$\le4\left|1-\theta\right|n^{-2}ET_{0b}^2\qquad(1.4)$$

Combining the contributions of (1.2) –(1.3), we thus find tha

$$\Big| \; d_{TV}(L(\bar{C}[1,b]), L(\bar{Z}[1,b]))$$

$$-(n+1)^{-1}\sum_{r\geq 0} P[T_{0b}=r]\left\{\sum_{s\geq 0} P[T_{0b}=s](s-r)(1-\theta)\right\}_{+} \Big|$$

$$\leq \varepsilon_{\{7.8\}}(n,b)$$

$$= \frac{3}{\theta P_{\theta}[0,1]}\left\{\varepsilon_{\{10.5(2)\}}(n/2,b) + 2n^{-1}ET_{0b}\varepsilon_{\{10.14\}}(n,b)\right\}$$

$$+2n^{-2}ET_{0b}^{2}\left\{4+3|1-\theta|+\frac{24|1-\theta|\phi^{*}_{\{10.8\}}(n)}{\theta P_{\theta}[0,1]}\right\} \qquad (1.5)$$

The quantity $\varepsilon_{\{7.8\}}(n,b)$ is seen to be of the order claimed under Conditions $(A_0),(D_1)$ and (B_{12}) , provided that $S(\infty)<\infty$; this supplementary condition can be removed if $\phi^{*}_{\{10.8\}}(n)$ is replaced by $\phi^{*}_{\{10.11\}}(n)$ in the definition of $\varepsilon_{\{7.8\}}(n,b)$, has the required order without the restriction on the r_i implied by assuming that $S(\infty)<\infty$. Finally, a direct calculation now shows that

$$\sum_{r\geq 0} P[T_{0b}=r]\left\{\sum_{s\geq 0} P[T_{0b}=s](s-r)(1-\theta)\right\}_{+}$$

$$= \frac{1}{2}|1-\theta|\,E\,|T_{0b}-ET_{0b}|$$

V. TRUST AND TRUST MANAGEMENT MODELS FOR ECOMMERCE

A. A Concept of Trust and Trust Management

Trust is a complex concept; it has a lot of different meanings depending on application fields. In [1] the characteristics of trust are identified as follows:

(1) Trust is multidimensional. For example, trust of the transaction entities in e-commerce may be evaluated using the trust attributes such as the quality of products, prices of products, delivery speeds, etc.

(2) Trust is field-sensitive. People engaging in different fields of work are good at different things, for example, computer experts may not be proficient at music. So it makes sense that trust is restricted in one or a few specific fields to discuss.

(3) Trust is subjective. People of different cultural backgrounds living in different environments often have different value orientation and judgment criterion. And different people may have different opinions on whether someone is trustworthy.

(4) Trust is dynamically changeable and non-monotonous. For example, a customer's degree of trust in a specific seller is dynamically adjusted with the change of the seller's performance and service quality.

B. Research and Application of Trust Management Model for ECommerce

The trust model is mainly concerned with trust representation, trust measurement and trust evaluation. Trust evaluation is the core of the trust model, so trust model is also referred to as trust evaluation model [5]. The trust model based on the perspective of consumers, reputation-based trust model and the trust model combined direct trust with recommendation trust for e-commerce are briefly introduced in the following. Trust models for e-commerce based on the perspective of consumers are two-dimensional. Although come from different fields such as psychology, sociology, management etc. these models can provide convincing explanation for the problems of transaction trust in e-commerce [6]. However, these models are from consumers' perspective; don't consider the transaction entities' global (comprehensive) trust provided by the ecommerce platform as the third party. Reputation-based trust management originated from ecommerce field, in which eBay and Taobao trust management models are well-know. Trust model based on reputation evaluates the transaction entities according to users' own direct experience, other users' opinions, recommendation or synthesis results combined direct experience with recommendation [1]. For example, after a transaction is completed, the buyer and seller on eBay can leave feedback each other. The feedback includes a short comment and a rating. The rating is used to determine the feedback score (namely credit) of the feedback receiver who receives +1 point for each positive rating, no points for each neutral rating, -1 point for each negative rating. The users' credit is divided into 11 levels [7]. Taobao adopts similar rules for credit evaluation, that is, "+1" point for each positive rating, no points for each neural rating, "-1" point for each negative rating. According to the score accumulated, the transaction entity's trust level is identified. In Taobao, sellers' trust is divided into 20 levels [8]. The transaction-related factors such as the number of transactions, the amount of transactions, etc. haven't been considered in these reputation based trust management systems. Chinese scholar Cao TianJie thinks that if the transaction entities' global (comprehensive) trust is considered, while their direct (local) trust is not considered, there are shortcomings in such a kind of trust evaluation method. For example, buyer b always breaks faith with seller s, but b's global trust may be good if he conducts transactions honestly with other trading partners. A new seller may be misled by b's global trust. To avoid such problems, Cao presented a trust computing model combining direct trust with global recommendation trust [9]. Trust in e-commerce is

based on faith in essence, which is fuzzy, cannot be accurately described and validated [10]. In order to reflect various and complex trust attributes of transaction entities as far as possible, the mathematical methods should be discovered which reflect ambiguity of trust in e-commerce, also quantitatively describe trust model for ecommerce. In 1966, fuzzy clustering method is proposed by Bellman and Zadeh [11], which provides a theoretical basis for research on fuzzy object recognition. In fuzzy clustering, objects with similar properties are grouped into a cluster using specified clustering principles and fuzzy judgment standards. In [12] the trust problems between the nodes in open network environment are analyzed. The nodes' attributes are described from four aspects including reputation, social identity, social status, and violation. Based on fuzzy set theory, the fuzziness of subjective trust is described by the membership degree. However, in e-commerce system, it is difficult to obtain the social identity and social status of the transaction entities (buyers or sellers), but various transaction-related data such as the amount of transactions, the number of transactions, etc. which directly relates to the transaction entities' trust on the ecommerce platform, can be obtained dynamically. The paper study the trust management model for ecommerce based on fuzzy clustering method. The three trust attributes related to transaction in the model, can be directly obtained from system. For each transaction entity, considering global (comprehensive) trust on e-commerce platform provides reference for the potential transaction partners. On the other hand, according to transaction history-direct experience, all transaction partners who transact with entity based on trust level are grouped into clusters, which provides reference basis for new transaction decision.

Example 1.0. Consider the point $O=(0,...,0)\in \mathbb{R}^n$. For an arbitrary vector r, the coordinates of the point $x=O+r$ are equal to the respective coordinates of the vector $r: x=(x^1,...x^n)$ and $r=(x^1,...,x^n)$. The vector r such as in the example is called the position vector or the radius vector of the point x. (Or, in greater detail: r is the radius-vector of x w.r.t an origin O). Points are frequently specified by their radius-vectors. This presupposes the choice of O as the "standard origin". Let us summarize. We have considered $\mathbb{R}^n$ and interpreted its elements in two ways: as points and as vectors. Hence we may say that we leading with the two copies of $\mathbb{R}^n$: $\mathbb{R}^n$ = {points}, $\mathbb{R}^n$ = {vectors}

Operations with vectors: multiplication by a number, addition. Operations with points and vectors: adding a vector to a point (giving a point), subtracting two points (giving a vector). $\mathbb{R}^n$ treated in this way is called an *n-dimensional affine space*. (An "abstract" affine space is a pair of sets , the set of points and the set of vectors so that the operations as above are defined axiomatically). Notice that vectors in an affine space are also known as "free vectors". Intuitively, they are not fixed at points and "float freely" in space. From $\mathbb{R}^n$ considered as an affine space we can precede in two opposite directions: $\mathbb{R}^n$ as an Euclidean space $\Leftarrow$ $\mathbb{R}^n$ as an affine space $\Rightarrow$ $\mathbb{R}^n$ as a manifold.Going to the left means introducing some extra structure which will make the geometry richer. Going to the right means forgetting about part of the affine structure; going further in this direction will lead us to the so-called "smooth (or differentiable) manifolds". The theory of differential forms does not require any extra geometry. So our natural direction is to the right. The Euclidean structure, however, is useful for examples and applications. So let us say a few words about it:

Remark 1.0. *Euclidean geometry.* In $\mathbb{R}^n$ considered as an affine space we can already do a good deal of geometry. For example, we can consider lines and planes, and quadric surfaces like an ellipsoid. However, we cannot discuss such things as "lengths", "angles" or "areas" and "volumes". To be able to do so, we have to introduce some more definitions, making $\mathbb{R}^n$ a Euclidean space. Namely, we define the length of a vector $a=(a^1,...,a^n)$ to be

$$|a|:=\sqrt{(a^1)^2+...+(a^n)^2} \qquad (1)$$

After that we can also define distances between points as follows:

$$d(A,B):=\left|\overrightarrow{AB}\right| \qquad (2)$$

One can check that the distance so defined possesses natural properties that we expect: is it always non-negative and equals zero only for coinciding points; the distance from A to B is the same as that from B to A (symmetry); also, for three points, A, B and C, we have $d(A,B)\le d(A,C)+d(C,B)$ (the "triangle inequality"). To define angles, we first introduce the scalar product of two vectors

$$(a,b):=a^1b^1+...+a^nb^n \qquad (3)$$

Thus $|a|=\sqrt{(a,a)}$. The scalar product is also denote by dot: $a.b=(a,b)$, and hence is often referred to as the "dot product". Now, for nonzero vectors, we define the angle between them by the equality

$$\cos\alpha:=\frac{(a,b)}{|a||b|} \qquad (4)$$

The angle itself is defined up to an integral multiple of 2π . For this definition to be consistent we have to ensure that the r.h.s. of (4) does not exceed 1 by the absolute value. This follows from the inequality

$$(a,b)^2 \le |a|^2 |b|^2 \qquad (5)$$

known as the Cauchy–Bunyakovsky–Schwarz inequality (various combinations of these three names are applied in different books). One of the ways of proving (5) is to consider the scalar square of the linear combination $a+tb,$ where $t \in R$. As $(a+tb, a+tb) \ge 0$ is a quadratic polynomial in t which is never negative, its discriminant must be less or equal zero. Writing this explicitly yields (5). The triangle inequality for distances also follows from the inequality (5).

Example 1.1. Consider the function $f(x) = x^i$ (the i-th coordinate). The linear function dx^i (the differential of x^i) applied to an arbitrary vector h is simply h^i .From these examples follows that we can rewrite df as

$$df = \frac{\partial f}{\partial x^1} dx^1 + \ldots + \frac{\partial f}{\partial x^n} dx^n, \qquad (1)$$

which is the standard form. Once again: the partial derivatives in (1) are just the coefficients (depending on x); $dx^1, dx^2, \ldots$ are linear functions giving on an arbitrary vector h its coordinates $h^1, h^2, \ldots,$ respectively. Hence

$$df(x)(h) = \partial_{hf(x)} = \frac{\partial f}{\partial x^1} h^1 + \ldots + \frac{\partial f}{\partial x^n} h^n, \qquad (2)$$

Theorem 1.7. Suppose we have a parametrized curve $t \mapsto x(t)$ passing through $x_0 \in \mathbb{R}^n$ at $t = t_0$ and with the velocity vector $x(t_0) = \upsilon$ Then

$$\frac{df(x(t))}{dt}(t_0) = \partial_\upsilon f(x_0) = df(x_0)(\upsilon) \qquad (1)$$

Proof. Indeed, consider a small increment of the parameter $t : t_0 \mapsto t_0 + \Delta t$, Where $\Delta t \mapsto 0$. On the other hand, we have $f(x_0 + h) - f(x_0) = df(x_0)(h) + \beta(h)|h|$ for an arbitrary vector h , where $\beta(h) \to 0$ when $h \to 0$. Combining it together, for the increment of $f(x(t))$ we obtain

$$\begin{aligned} & f(x(t_0 + \Delta t) - f(x_0) \\ &= df(x_0)(\upsilon.\Delta t + \alpha(\Delta t)\Delta t) \\ &+ \beta(\upsilon.\Delta t + \alpha(\Delta t)\Delta t).|\upsilon\Delta t + \alpha(\Delta t)\Delta t| \\ &= df(x_0)(\upsilon).\Delta t + \gamma(\Delta t)\Delta t \end{aligned}$$

For a certain $\gamma(\Delta t)$ such that $\gamma(\Delta t) \to 0$ when $\Delta t \to 0$ (we used the linearity of $df(x_0)$). By the definition, this means that the derivative of $f(x(t))$ at $t = t_0$ is exactly $df(x_0)(\upsilon)$. The statement of the theorem can be expressed by a simple formula:

$$\frac{df(x(t))}{dt} = \frac{\partial f}{\partial x^1} x^1 + \ldots + \frac{\partial f}{\partial x^n} x^n \qquad (2)$$

To calculate the value Of df at a point x_0 on a given vector υ one can take an arbitrary curve passing Through x_0 at t_0 with υ as the velocity vector at t_0 and calculate the usual derivative of $f(x(t))$ at $t = t_0$.

Theorem 1.8. For functions $f, g : U \to \mathbb{R}$, $U \subset \mathbb{R}^n$,

$$d(f+g) = df + dg \qquad (1)$$

$$d(fg) = df.g + f.dg \qquad (2)$$

Proof. Consider an arbitrary point x_0 and an arbitrary vector υ stretching from it. Let a curve $x(t)$ be such that $x(t_0) = x_0$ and $x(t_0) = \upsilon$. Hence

$$d(f+g)(x_0)(\upsilon) = \frac{d}{dt}(f(x(t)) + g(x(t)))$$

at $t = t_0$ and

$$d(fg)(x_0)(\upsilon) = \frac{d}{dt}(f(x(t))g(x(t)))$$

at $t = t_0$ Formulae (1) and (2) then immediately follow from the corresponding formulae for the usual derivative Now, almost without change the theory generalizes to functions taking values in $\mathbb{R}^m$ instead of $\mathbb{R}$. The only difference is that now the differential of a map $F : U \to \mathbb{R}^m$ at a point x will be a linear function taking vectors in $\mathbb{R}^n$ to vectors in $\mathbb{R}^m$ (instead of $\mathbb{R}$) . For an arbitrary vector $h \in \mathbb{R}^n$,

$$F(x+h)=F(x)+dF(x)(h)$$
$$+\beta(h)|h| \qquad (3)$$

Where $\beta(h)\to 0$ when $h\to 0$. We have $dF=(dF^1,...,dF^m)$ and

$$dF=\frac{\partial F}{\partial x^1}dx^1+...+\frac{\partial F}{\partial x^n}dx^n$$

$$=\begin{pmatrix}\frac{\partial F^1}{\partial x^1}&\cdots&\frac{\partial F^1}{\partial x^n}\\ \cdots&\cdots&\cdots\\ \frac{\partial F^m}{\partial x^1}&\cdots&\frac{\partial F^m}{\partial x^n}\end{pmatrix}\begin{pmatrix}dx^1\\ \cdots\\ dx^n\end{pmatrix} \qquad (4)$$

In this matrix notation we have to write vectors as vector-columns.

Theorem 1.9. For an arbitrary parametrized curve $x(t)$ in $\mathbb{R}^n$, the differential of a map $F:U\to\mathbb{R}^m$ (where $U\subset\mathbb{R}^n$) maps the velocity vector $\dot{x}(t)$ to the velocity vector of the curve $F(x(t))$ in $\mathbb{R}^m$:

$$\frac{dF(x(t))}{dt}=dF(x(t))(\dot{x}(t)) \qquad (1)$$

Proof. By the definition of the velocity vector,

$$x(t+\Delta t)=x(t)+\dot{x}(t).\Delta t+\alpha(\Delta t)\Delta t \qquad (2)$$

Where $\alpha(\Delta t)\to 0$ when $\Delta t\to 0$. By the definition of the differential,

$$F(x+h)=F(x)+dF(x)(h)+\beta(h)|h \qquad (3)$$

Where $\beta(h)\to 0$ when $h\to 0$. we obtain

$$F(x(t+\Delta t))=F(x+\underbrace{\dot{x}(t).\Delta t+\alpha(\Delta t)\Delta t}_{h})$$

$$=F(x)+dF(x)(\dot{x}(t)\Delta t+\alpha(\Delta t)\Delta t)+$$

$$\beta(\dot{x}(t)\Delta t+\alpha(\Delta t)\Delta t).|\dot{x}(t)\Delta t+\alpha(\Delta t)\Delta t|$$

$$=F(x)+dF(x)(\dot{x}(t)\Delta t+\gamma(\Delta t)\Delta t$$

For some $\gamma(\Delta t)\to 0$ when $\Delta t\to 0$. This precisely means that $dF(x)\dot{x}(t)$ is the velocity vector of $F(x)$. As every vector attached to a point can be viewed as the velocity vector of some curve passing through this point, this theorem gives a clear geometric picture of dF as a linear map on vectors.

Theorem 1.10 Suppose we have two maps $F:U\to V$ and $G:V\to W$, where $U\subset\mathbb{R}^n, V\subset\mathbb{R}^m, W\subset\mathbb{R}^p$ (open domains). Let $F:x\mapsto y=F(x)$. Then the differential of the composite map $GoF:U\to W$ is the composition of the differentials of F and G:

$$d(GoF)(x)=dG(y)odF(x) \qquad (4)$$

Proof. We can use the description of the differential .Consider a curve $x(t)$ in $\mathbb{R}^n$ with the velocity vector $\dot{x}$. Basically, we need to know to which vector in $\mathbb{R}^p$ it is taken by $d(GoF)$. the curve $(GoF)(x(t)=G(F(x(t))$. By the same theorem, it equals the image under dG of the Anycast Flow vector to the curve $F(x(t))$ in $\mathbb{R}^m$. Applying the theorem once again, we see that the velocity vector to the curve $F(x(t))$ is the image under dF of the vector $\dot{x}(t)$. Hence $d(GoF)(\dot{x})=dG(dF(\dot{x}))$ for an arbitrary vector $\dot{x}$.

Corollary 1.0. If we denote coordinates in $\mathbb{R}^n$ by $(x^1,...,x^n)$ and in $\mathbb{R}^m$ by $(y^1,...,y^m)$, and write

$$dF=\frac{\partial F}{\partial x^1}dx^1+...+\frac{\partial F}{\partial x^n}dx^n \qquad (1)$$

$$dG=\frac{\partial G}{\partial y^1}dy^1+...+\frac{\partial G}{\partial y^n}dy^n, \qquad (2)$$

Then the chain rule can be expressed as follows:

$$d(GoF)=\frac{\partial G}{\partial y^1}dF^1+...+\frac{\partial G}{\partial y^m}dF^m, \qquad (3)$$

Where dF^i are taken from (1). In other words, to get $d(GoF)$ we have to substitute into (2) the expression for $dy^i=dF^i$ from (3). This can also be expressed by the following matrix formula:

$$d(GoF)=\begin{pmatrix}\frac{\partial G^1}{\partial y^1}&\cdots&\frac{\partial G^1}{\partial y^m}\\ \cdots&\cdots&\cdots\\ \frac{\partial G^p}{\partial y^1}&\cdots&\frac{\partial G^p}{\partial y^m}\end{pmatrix}\begin{pmatrix}\frac{\partial F^1}{\partial x^1}&\cdots&\frac{\partial F^1}{\partial x^n}\\ \cdots&\cdots&\cdots\\ \frac{\partial F^m}{\partial x^1}&\cdots&\frac{\partial F^m}{\partial x^n}\end{pmatrix}\begin{pmatrix}dx^1\\ \cdots\\ dx^n\end{pmatrix} \qquad (4)$$

i.e., if dG and dF are expressed by matrices of partial derivatives, then $d(GoF)$ is expressed by the product of these matrices. This is often written as

$$\begin{pmatrix} \frac{\partial z^1}{\partial x^1} \cdots \frac{\partial z^1}{\partial x^n} \\ \cdots \quad \cdots \quad \cdots \\ \frac{\partial z^p}{\partial x^1} \cdots \frac{\partial z^p}{\partial x^n} \end{pmatrix} = \begin{pmatrix} \frac{\partial z^1}{\partial y^1} \cdots \frac{\partial z^1}{\partial y^m} \\ \cdots \quad \cdots \quad \cdots \\ \frac{\partial z^p}{\partial y^1} \cdots \frac{\partial z^p}{\partial y^m} \end{pmatrix}$$

$$\begin{pmatrix} \frac{\partial y^1}{\partial x^1} \cdots \frac{\partial y^1}{\partial x^n} \\ \cdots \quad \cdots \quad \cdots \\ \frac{\partial y^m}{\partial x^1} \cdots \frac{\partial y^m}{\partial x^n} \end{pmatrix}, \qquad (5)$$

Or

$$\frac{\partial z^\mu}{\partial x^a} = \sum_{i=1}^{m} \frac{\partial z^\mu}{\partial y^i} \frac{\partial y^i}{\partial x^a}, \qquad (6)$$

Where it is assumed that the dependence of $y \in \mathbb{R}^m$ on $x \in \mathbb{R}^n$ is given by the map F, the dependence of $z \in \mathbb{R}^p$ on $y \in \mathbb{R}^m$ is given by the map G, and the dependence of $z \in \mathbb{R}^p$ on $x \in \mathbb{R}^n$ is given by the composition GoF.

Definition 1.6. Consider an open domain $U \subset \mathbb{R}^n$. Consider also another copy of $\mathbb{R}^n$, denoted for distinction $\mathbb{R}^n_y$, with the standard coordinates $(y^1 \ldots y^n)$. A system of coordinates in the open domain U is given by a map $F: V \to U$, where $V \subset \mathbb{R}^n_y$ is an open domain of $\mathbb{R}^n_y$, such that the following three conditions are satisfied :

(1) F is smooth;
(2) F is invertible;
(3) $F^{-1}: U \to V$ is also smooth

The coordinates of a point $x \in U$ in this system are the standard coordinates of $F^{-1}(x) \in \mathbb{R}^n_y$

In other words,

$$F: (y^1 \ldots, y^n) \mapsto x = x(y^1 \ldots, y^n) \qquad (1)$$

Here the variables $(y^1 \ldots, y^n)$ are the "new" coordinates of the point x

Example 1.2. Consider a curve in $\mathbb{R}^2$ specified in polar coordinates as

$$x(t): r = r(t), \varphi = \varphi(t) \qquad (1)$$

We can simply use the chain rule. The map $t \mapsto x(t)$ can be considered as the composition of the maps $t \mapsto (r(t), \varphi(t)), (r, \varphi) \mapsto x(r, \varphi)$. Then, by the chain rule, we have

$$\dot{x} = \frac{dx}{dt} = \frac{\partial x}{\partial r}\frac{dr}{dt} + \frac{\partial x}{\partial \varphi}\frac{d\varphi}{dt} = \frac{\partial x}{\partial r}\dot{r} + \frac{\partial x}{\partial \varphi}\dot{\varphi} \qquad (2)$$

Here $\dot{r}$ and $\dot{\varphi}$ are scalar coefficients depending on t, whence the partial derivatives $\partial x / \partial r, \partial x / \partial \varphi$ are vectors depending on point in $\mathbb{R}^2$. We can compare this with the formula in the "standard" coordinates: $\dot{x} = e_1 \dot{x} + e_2 \dot{y}$. Consider the vectors $\partial x / \partial r, \partial x / \partial \varphi$. Explicitly we have

$$\frac{\partial x}{\partial r} = (\cos\varphi, \sin\varphi) \qquad (3)$$

$$\frac{\partial x}{\partial \varphi} = (-r\sin\varphi, r\cos\varphi) \qquad (4)$$

From where it follows that these vectors make a basis at all points except for the origin (where $r = 0$). It is instructive to sketch a picture, drawing vectors corresponding to a point as starting from that point. Notice that $\partial x / \partial r, \partial x / \partial \varphi$ are, respectively, the velocity vectors for the curves $r \mapsto x(r, \varphi)$ $(\varphi = \varphi_0 \ fixed)$ and $\varphi \mapsto x(r, \varphi)$ $(r = r_0 \ fixed)$. We can conclude that for an arbitrary curve given in polar coordinates the velocity vector will have components $(\dot{r}, \dot{\varphi})$ if as a basis we take $e_r := \partial x / \partial r, e_\varphi := \partial x / \partial \varphi$:

$$\dot{x} = e_r \dot{r} + e_\varphi \dot{\varphi} \qquad (5)$$

A characteristic feature of the basis e_r, e_φ is that it is not "constant" but depends on point. Vectors "stuck to points" when we consider curvilinear coordinates.

Proposition 1.3. The velocity vector has the same appearance in all coordinate systems.

Proof. Follows directly from the chain rule and the transformation law for the basis e_i. In particular, the elements of the basis $e_i = \partial x / \partial x^i$ (originally, a formal notation) can be understood directly as the velocity vectors of the coordinate lines

$x^i \mapsto x(x^1,...,x^n)$ (all coordinates but x^i are fixed). Since we now know how to handle velocities in arbitrary coordinates, the best way to treat the differential of a map $F:\mathbb{R}^n \to \mathbb{R}^m$ is by its action on the velocity vectors. By definition, we set

$$dF(x_0): \frac{dx(t)}{dt}(t_0) \mapsto \frac{dF(x(t))}{dt}(t_0) \qquad (1)$$

Now $dF(x_0)$ is a linear map that takes vectors attached to a point $x_0 \in \mathbb{R}^n$ to vectors attached to the point $F(x) \in \mathbb{R}^m$

$$dF = \frac{\partial F}{\partial x^1}dx^1 + ... + \frac{\partial F}{\partial x^n}dx^n$$

$$(e_1,...,e_m)\begin{pmatrix} \frac{\partial F^1}{\partial x^1} & \cdots & \frac{\partial F^1}{\partial x^n} \\ \cdots & \cdots & \cdots \\ \frac{\partial F^m}{\partial x^1} & \cdots & \frac{\partial F^m}{\partial x^n} \end{pmatrix}\begin{pmatrix} dx^1 \\ \cdots \\ dx^n \end{pmatrix}, \qquad (2)$$

In particular, for the differential of a function we always have

$$df = \frac{\partial f}{\partial x^1}dx^1 + ... + \frac{\partial f}{\partial x^n}dx^n, \qquad (3)$$

Where x^i are arbitrary coordinates. The form of the differential does not change when we perform a change of coordinates.

Example 1.3 Consider a 1-form in $\mathbb{R}^2$ given in the standard coordinates:

$A = -ydx + xdy$ In the polar coordinates we will have $x = r\cos\varphi, y = r\sin\varphi$, hence

$dx = \cos\varphi dr - r\sin\varphi d\varphi$

$dy = \sin\varphi dr + r\cos\varphi d\varphi$

Substituting into A, we get

$A = -r\sin\varphi(\cos\varphi dr - r\sin\varphi d\varphi)$

$+r\cos\varphi(\sin\varphi dr + r\cos\varphi d\varphi)$

$= r^2(\sin^2\varphi + \cos^2\varphi)d\varphi = r^2 d\varphi$

Hence $A = r^2 d\varphi$ is the formula for A in the polar coordinates. In particular, we see that this is again a 1-form, a linear combination of the differentials of coordinates with functions as coefficients. Secondly, in a more conceptual way, we can define a 1-form in a domain U as a linear function on vectors at every point of U :

$$\omega(\upsilon) = \omega_1\upsilon^1 + ... + \omega_n\upsilon^n, \qquad (1)$$

If $\upsilon = \sum e_i\upsilon^i$, where $e_i = \partial x / \partial x^i$. Recall that the differentials of functions were defined as linear functions on vectors (at every point), and

$$dx^i(e_j) = dx^i\left(\frac{\partial x}{\partial x^j}\right) = \delta^i_j \qquad (2)$$

at every point x.

Theorem 1.9. For arbitrary 1-form ω and path γ, the integral $\int_\gamma \omega$ does not change if we change parametrization of γ provide the orientation remains the same.

Proof: Consider $\left\langle \omega(x(t)), \frac{dx}{dt'} \right\rangle$ and $\left\langle \omega(x(t(t'))), \frac{dx}{dt'} \right\rangle$ As

$$\left\langle \omega(x(t(t'))), \frac{dx}{dt'} \right\rangle = \left| \left\langle \omega(x(t(t'))), \frac{dx}{dt'} \right\rangle . \frac{dt}{dt'} \right|,$$

Mobile ad hoc networks (MANETs) are multi-hop wireless networks dynamically formed by mobile nodes without the help of a centralized infrastructure [11]. Group communication systems (GCSs) in MANETs, such as in military battlefields or emergency rescue operations, require teamwork and collaboration to achieve a mission that depends on trust relationships among group members [16]. Blaze et al. [6] first introduced the term trust management and identified it as a separate component of security services in networks. Since its inception in 1996 [6], trust management in MANETs has received considerable attention due to its crucial necessity and diverse applicability. Trust management in MANETs is needed where participating nodes, without any previous interactions, must establish a network with an acceptable level of trust relationships among themselves, for example, in building initial trust bootstrapping, or in battlefield coalition operations without predefined trust. In addition, trust management has wide applicability in decision making situations requiring collaboration of participating nodes with goals such as secure routing, key management, intrusion detection, authentication, and access control [8, 15]. Security protocol designers for GCSs in MANETs face unique technical challenges due to the unique characteristics of MANETs such as resource-constraints (e.g., bandwidth, memory, energy, computational power), openness to eavesdropping, high security threats or vulnerability, inherently unreliable wireless communication medium, and rapid changes in topologies or memberships due to user mobility or node failure [11]. Compared with

designing security protocols for civilian MANETs, designing security protocols for mission driven GCSs in military MANETs requires additional caution because of demanding battlefield situations such as hostile environments, privacy, distinctively prioritized quality-of service (QoS), performance, compromised nodes, rapid tempo, lifetime of nodes, reliability, seamless self-organizing reconfigurability, coalition operation without predefined trust relationships, and heterogeneous node components. In order to construct trustable collaborative environments based on the unique characteristics of MANETs, many researchers [6, 9, 15,16, 24] have adopted various trust concepts to evaluate the relationships among group members. In the social science fields, trust is defined as the degree of a subjective belief about the behaviors of a particular entity [12]. Despite the subjective aspect of trust, the trust concept has been very attractive to security protocol designers because of its diverse applicability as a decision making mechanism. In developing trust management in MANETs, researchers have focused heavily on developing secure ad hoc routing based on trust with the aim of isolating malicious or selfish nodes for improving system throughput (e.g., end-to-end packet delivery ratio) [24]. However, no prior work exists on trust management in MANETs that can properly account for the various dynamically changing conditions, including topology changes, membership changes, energy depletion, node heterogeneity (e.g., different energy levels of nodes), selfishness, healthiness, and frequency of interactions over time. Our work takes into account these dynamically changing conditions. Our aim is to design and evaluate a trust management protocol for cognitive mission driven GCSs in MANETs and discover conditions under which the trust level among peers in the network may be maximized to facilitate trust-based collaboration. Specifically, peers collaborate by establishing a trust chain. We aim to identify the optimal length of the trust chain such that the trust level for peers on the trust chain is maximized. This is to be achieved for peers who may be selfish, possibly in a bootstrap mode, and in the presence of security threats, including insider and outsider attacks. The contributions of this work are as follows. First, we develop and evaluate a trust metric that not only reflects unique characteristics of cognitive GCSs in MANET environments but also meets the trust demand of mission-driven military situations (e.g., subjectivity, asymmetry, transitivity, dynamicity, context dependency). Second, we develop a mathematical model based on stochastic Petri net (SPN) techniques to evaluate the design tradeoff between the trust space (e.g., establishing trust levels of peers that are more than 1-hop away) and the decay of trust levels as a trust chain becomes longer, and the decay over time. In particular, we develop a hierarchical modeling technique to avoid state explosion problems in an SPN and to efficiently calculate the trust levels of a large number of nodes. Third, we incorporate design concepts of cognitive and social networks inspired by theories from social sciences to model cognitive trust-based GCSs in MANETs. We model the social behavior of a node in the social network by its social trust viewed by other peers in the network. Fourth, we identify the optimal length of a trust chain among peers that would maximize the trust level of peers on the chain with the goal of efficiently establishing trust relationships among participating nodes that have had no prior interactions. Our research has its roots in model-based quantitative modeling [21]. We use SPN as our mathematical model for performance analysis. An SPN model is essentially a concise representation of a Markov or semi-Markov model, capable of accommodating a large number of states. It can also accommodate general time distributions other than the commonly used exponential time distributions for modeling system events. In the literature on trust management in MANETs, little has been done using quantitative modeling techniques [15, 19]. Our work is unique in that we model and analyze the behavior of a cognitive GCS in MANETs in the presence of selfish nodes and insider attackers, incorporating trust management concepts derived from social and cognitive networks. However, formalizing or even defining trust is a hard task since it is a subjective concept. Trust Management (TM) was introduced in order to cope with this hardness. Blaze and al. [1] first introduced the term ”Trust Management” and identified it as a separate component of security services in networks and they clarified that ”Trust management provides a unified approach for specifying and interpreting security policies and relationships.” Some works dealt with TM. In [1], a management scheme for IPsec based on TM was introduced. More precisely, this proposition is based on the use of KeyNote which is a unified approach for specifying and interpreting security policies and credentials that allows direct authorization of security-critical actions. In [2], authors extended routing protocol with a trust model based on reputation. More precisely, they proposed to monitor the behavior of nodes’ neighbors and then to compute the nodes reputation based on the information collected by the monitoring. However, their mechanism allows only malicious packet dropping detection without any proposition to discard involved malicious nodes. In [3], Sun and al. proposed a framework to quantitatively measure trust, model trust propagation and defend trust evaluation systems against malicious attacks. According to these works, three TM models emerged: policy based, social based and reputation based models. Policy based models such as KeyNote [1] are used for systems access control where peers use credential verification to establish a trust

relationship. Let's note that according to this model, trust is unilateral i.e. only the resource-owner request to establish trust. Social based systems such as Regret [4], are based on social relationships between peers when computing trust and reputation values. They form conclusions about peers through analyzing a social network. Reputation based systems such as EigenRep [5], are based on measuring reputation: they evaluate the trust in the peer and the trust in the reliability of the resource. In this paper, we propose to benefit from these approaches and mainly the policy based and reputation based in order to obtain a new generic model capturing the essence of a TM system. More precisely, we propose to build this model over three activities constituting the basic steps of any system lifecycle: trust establishment, trust update and trust revocation. In order to establish a trust relation, we propose two schemas. In the first scheme, trust request is evaluated and a trust level is affected to the established relation. This evaluation is based on reputation computing and maintaining. In the second scheme, recommendations are used in order to assure trust transitivity and a recommendation level is affected to the established relation. Update activity concerns the modification of the considered relation i.e. trust level, recommendation level and reputation. Revocation activity concerns the removal of a trust relation.

RFID technology is a revolutionary method to identify and track human and products in applications such as SCM, retails, and healthcare, pharmaceutical and vehicle management [4, 16]. The use of EPC (Electronic Product Code) tags to eliminate counterfeiting is mainly because of two techniques: First, RFID allows for new, automated and secure ways to efficiently authenticate physical items. Second, as many companies invest in networked RFID technology for SCM, the item-level data collection and visibility now becomes possible [17]. Despite of the advantages of visibility and fast identification provided by RFID, the security and privacy threats attributed by limited hardware storage and memory in the RFID tag imposed an issue of counterfeiting [16]. The weakness of RFID technology in this study is considered in SCM only. There are four challenges of applying RFID technology in SCM: (1) tag security, (2) privacy and security of communication channel, (3) automatic transition of tag ownership, and (4) data integration issues [1, 7].Since the cost of tags decrease with the price close to $0.01 (1cent) each, the storage and memory capabilities on a tag are reduced. As a result, no strong and ultimate security mechanism can be installed on tags [2]. The vulnerability of RFID tags and communication channel increases the risk of security threats such as eavesdropping, skimming, and manin- the-middle, DOS, and physical attacks [15]. Single attack or a combination of threats contributes to cloning and frauds attacks, which are the main counterfeiting problems in SCM. Consequently, the above security and privacy problems decrease the human trust and confidence in the adoption and implementation ofRFID technology [9]. In a typical open network such as SCM, trust counts in selecting partners, software and hardware infrastructure used, and even in the information transmission within a communication system. Together with the list of challenges and vulnerability regarding RFID discussed earlier, public acceptance in RFID implications systems is still an open question. The major question is how can open RFID networks be secured through trust? And how do we derive the existing trust notion to fit into the RFID system and solve the security and privacy issues discussed earlier? Thus the relationship of trust and RFID in the nature of business indicates an interesting research problem, which is to be addressed in this paper. In our previous work [8], we proposed a novel seven-layer trust framework. Our trust framework provides functions for the trustworthiness of large scale RFID global tracking systems and the usefulness of RFID systems. Our trust framework also functions as a preventive and detective mechanism for security attacks. Based on [9], an RFID cloning and fraud attack is able to be handled with a better data sharing and exchange mechanism. For exchanging information, the need for authorization policies is a must. Hence, the aim of this paper is to construct a Computational Trust Management (CTM) system for our seven-layer trust framework in designing a better data sharing. Our objective is to employ our trust framework for assigning policies for a secure and visible data sharing. The second aim is to show how CTM can be used for RFID based wine counterfeiting handling. Even though our work is concentrated on RFID cloning and fraud attacks, our trust framework and the CTM solution can also be employed for other RFID security attacks.

Let p be a rational prime and let $K = \mathbb{Q}(\zeta_p)$. We write ζ for ζ_p or this section. Recall that K has degree $\varphi(p) = p-1$ over $\mathbb{Q}$. We wish to show that $O_K = \mathbb{Z}[\zeta]$. Note that ζ is a root of $x^p - 1$, and thus is an algebraic integer; since O_K is a ring we have that $\mathbb{Z}[\zeta] \subseteq O_K$. We give a proof without assuming unique factorization of ideals. We begin with some norm and trace computations. Let j be an integer. If j is not divisible by p, then ζ^j is a primitive p^{th} root of unity, and thus its conjugates are $\zeta, \zeta^2, ..., \zeta^{p-1}$. Therefore

$$Tr_{K/\mathbb{Q}}(\zeta^j) = \zeta + \zeta^2 + \ldots + \zeta^{p-1} = \Phi_p(\zeta) - 1 = -1$$

If p does divide j, then $\zeta^j = 1$, so it has only the one conjugate 1, and $Tr_{K/\mathbb{Q}}(\zeta^j) = p - 1$ By linearity of the trace, we find that

$$Tr_{K/\mathbb{Q}}(1-\zeta) = Tr_{K/\mathbb{Q}}(1-\zeta^2) = \ldots$$
$$= Tr_{K/\mathbb{Q}}(1-\zeta^{p-1}) = p$$

We also need to compute the norm of $1-\zeta$. For this, we use the factorization

$$x^{p-1} + x^{p-2} + \ldots + 1 = \Phi_p(x)$$
$$= (x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{p-1});$$

Plugging in $x = 1$ shows that

$$p = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{p-1})$$

Since the $(1-\zeta^j)$ are the conjugates of $(1-\zeta)$, this shows that $N_{K/\mathbb{Q}}(1-\zeta) = p$ The key result for determining the ring of integers O_K is the following.

LEMMA 1.9

$$(1-\zeta)O_K \cap \mathbb{Z} = p\mathbb{Z}$$

Proof. We saw above that p is a multiple of $(1-\zeta)$ in O_K, so the inclusion $(1-\zeta)O_K \cap \mathbb{Z} \supseteq p\mathbb{Z}$ is immediate. Suppose now that the inclusion is strict. Since $(1-\zeta)O_K \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ containing $p\mathbb{Z}$ and $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, we must have $(1-\zeta)O_K \cap \mathbb{Z} = \mathbb{Z}$ Thus we can write

$$1 = \alpha(1-\zeta)$$

For some $\alpha \in O_K$. That is, $1-\zeta$ is a unit in O_K.

COROLLARY 1.1 For any $\alpha \in O_K$, $Tr_{K/\mathbb{Q}}((1-\zeta)\alpha) \in p\mathbb{Z}$

PROOF. We have

$$Tr_{K/\mathbb{Q}}((1-\zeta)\alpha) = \sigma_1((1-\zeta)\alpha) + \ldots + \sigma_{p-1}((1-\zeta)\alpha)$$
$$= \sigma_1(1-\zeta)\sigma_1(\alpha) + \ldots + \sigma_{p-1}(1-\zeta)\sigma_{p-1}(\alpha)$$
$$= (1-\zeta)\sigma_1(\alpha) + \ldots + (1-\zeta^{p-1})\sigma_{p-1}(\alpha)$$

Where the σ_i are the complex embeddings of K (which we are really viewing as automorphisms of K) with the usual ordering. Furthermore, $1-\zeta^j$ is a multiple of $1-\zeta$ in O_K for every $j \neq 0$. Thus $Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) \in (1-\zeta)O_K$ Since the trace is also a rational integer.

PROPOSITION 1.4 Let p be a prime number and let $K = \mathbb{Q}(\zeta_p)$ be the p^{th} cyclotomic field. Then $O_K = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(\Phi_p(x))$; Thus $1, \zeta_p, \ldots, \zeta_p^{p-2}$ is an integral basis for O_K.

PROOF. Let $\alpha \in O_K$ and write

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$$ With $a_i \in \mathbb{Q}$.

Then

$$\alpha(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \ldots$$
$$+ a_{p-2}(\zeta^{p-2} - \zeta^{p-1})$$

By the linearity of the trace and our above calculations we find that $Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) = pa_0$ We also have $Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) \in p\mathbb{Z}$, so $a_0 \in \mathbb{Z}$ Next consider the algebraic integer

$(\alpha - a_0)\zeta^{-1} = a_1 + a_2\zeta + \ldots + a_{p-2}\zeta^{p-3}$; This is an algebraic integer since $\zeta^{-1} = \zeta^{p-1}$ is. The same argument as above shows that $a_1 \in \mathbb{Z}$, and continuing in this way we find that all of the a_i are in $\mathbb{Z}$. This completes the proof.

Example 1.4 Let $K = \mathbb{Q}$, then the local ring $\mathbb{Z}_{(p)}$ is simply the subring of $\mathbb{Q}$ of rational numbers with denominator relatively prime to p. Note that this ring $\mathbb{Z}_{(p)}$ is not the ring $\mathbb{Z}_p$ of p-adic integers; to get $\mathbb{Z}_p$ one must complete $\mathbb{Z}_{(p)}$. The usefulness of $O_{K,p}$ comes from the fact that it has a particularly simple ideal structure. Let a be any proper ideal of $O_{K,p}$ and consider the ideal $a \cap O_K$ of O_K. We claim that $a = (a \cap O_K)O_{K,p}$; That is, that a is generated by the elements of a in $a \cap O_K$. It is clear from the definition of an ideal that $a \supseteq (a \cap O_K)O_{K,p}$. To prove the other inclusion, let α be any element of a. Then we can write $\alpha = \beta/\gamma$ where $\beta \in O_K$ and $\gamma \notin p$. In particular, $\beta \in a$ (since $\beta/\gamma \in a$ and a is an ideal), so $\beta \in O_K$ and $\gamma \notin p$. so $\beta \in a \cap O_K$.

Since $1/\gamma \in O_{K,p}$, this implies that $\alpha = \beta/\gamma \in (a \cap O_K)O_{K,p}$, as claimed.We can use this fact to determine all of the ideals of $O_{K,p}$. Let a be any ideal of $O_{K,p}$ and consider the ideal factorization of $a \cap O_K$ in O_K. write it as $a \cap O_K = p^n b$ For some n and some ideal b, relatively prime to p. we claim first that $bO_{K,p} = O_{K,p}$. We now find that

$$a = (a \cap O_K)O_{K,p} = p^n bO_{K,p} = p^n O_{K,p}$$

Since $bO_{K,p}$. Thus every ideal of $O_{K,p}$ has the form $p^n O_{K,p}$ for some n; it follows immediately that $O_{K,p}$ is noetherian. It is also now clear that $p^n O_{K,p}$ is the unique non-zero prime ideal in $O_{K,p}$. Furthermore, the inclusion $O_K \mapsto O_{K,p}/pO_{K,p}$ Since $pO_{K,p} \cap O_K = p$, this map is also surjection, since the residue class of $\alpha/\beta \in O_{K,p}$ (with $\alpha \in O_K$ and $\beta \notin p$) is the image of $\alpha\beta^{-1}$ in $O_{K/p}$, which makes sense since β is invertible in $O_{K/p}$. Thus the map is an isomorphism. In particular, it is now abundantly clear that every non-zero prime ideal of $O_{K,p}$ is maximal. To show that $O_{K,p}$ is a Dedekind domain, it remains to show that it is integrally closed in K. So let $\gamma \in K$ be a root of a polynomial with coefficients in $O_{K,p}$; write this polynomial as $x^m + \frac{\alpha_{m-1}}{\beta_{m-1}}x^{m-1} + \ldots + \frac{\alpha_0}{\beta_0}$ With $\alpha_i \in O_K$ and $\beta_i \in O_{K-p}$. Set $\beta = \beta_0\beta_1\ldots\beta_{m-1}$. Multiplying by β^m we find that $\beta\gamma$ is the root of a monic polynomial with coefficients in O_K. Thus $\beta\gamma \in O_K$; since $\beta \notin p$, we have $\beta\gamma/\beta = \gamma \in O_{K,p}$. Thus $O_{K,p}$ is integrally close in K.

COROLLARY 1.2. Let K be a number field of degree n and let α be in O_K then $N'_{K/\square}(\alpha O_K) = |N_{K/\square}(\alpha)|$

PROOF. We assume a bit more Galois theory than usual for this proof. Assume first that $K/\square$ is Galois. Let σ be an element of $Gal(K/\square)$. It is clear that $\sigma(O_K)/\sigma(\alpha) \cong O_{K/\alpha}$; since $\sigma(O_K) = O_K$, this shows that $N'_{K/\square}(\sigma(\alpha)O_K) = N'_{K/\square}(\alpha O_K)$. Taking the product over all $\sigma \in Gal(K/\square)$, we have $N'_{K/\square}(N_{K/\square}(\alpha)O_K) = N'_{K/\square}(\alpha O_K)^n$ Since $N_{K/\square}(\alpha)$ is a rational integer and O_K is a free $\square$ -module of rank n, $O_K/N_{K/\square}(\alpha)O_K$ Will have order $N_{K/\square}(\alpha)^n$; therefore

$$N'_{K/\square}(N_{K/\square}(\alpha)O_K) = N_{K/\square}(\alpha O_K)^n$$

This completes the proof. In the general case, let L be the Galois closure of K and set $[L:K] = m$.

E-commerce is the process of buying and selling goods and services over the Internet. One of the major advantages of e-commerce is that it provides opportunities to extend businesses to anywhere in the world. While e-commerce provides enormous opportunities, it also presents potential threats and risks due to a lack of trust. Different from traditional businesses, participants in an e-commerce environment are unable to have face to face meetings as they have no prior knowledge of each other and with no legal protection enforcement to reduce the likelihood of business risks. As a result, it is generally believed that lack of trust is one of the main reasons that business transactions in an e-commerce environment are still not living up to their full potential [8]. To mitigate such problems, many trust management systems have been developed in establishing trust between trading partners in e-commerce [5, 6, 7, 11,13]. Trust management systems compute the trust value of an entity, relying on feedback data received from participating parties [7]. It is supposed to provide ways to increase trust and assist potential buyers in making decisions on e-commerce transactions. However, due to potential manipulations by malicious players and the enormous amount of information updated everyday trust management systems still encounter considerable challenges and are incapable of supporting all different trust relationships to improve users' confidence. In this paper, we identify several desirable properties of an ideal trust management system and propose a new multilevel trust management system that fulfils all these desirable properties. The proposed new trust management framework includes a feedback data verification component to ensure the credibility of the feedback provided by the participants, and a dispute resolution mechanism to solve any dispute on feedback received.

In recent years, lots of trust management mechanisms have been designed and implemented to restrain the selfish and fraudulent behaviors in the P2P network, which are extensively applied to such fields as resource sharing, electronic commerce and P2P Grid computing, etc. However, based on the non-centric and autonomic features of peers in the P2P network, these studies pay large attention to the aspect of "soft security" in the P2P network. "Soft security" means, in terms of the subjective expectations the trustor makes to the trustee, the trustor utilizes the mathematic approach to describe how to rate the trustee, and establish the feasible trust computation models and rating scheme [1,2]. However, these researches pay less attention to the security problem confronted by its trust management. In fact, security of trust management is the key element assuring the normal running of the TMS, and is as important as any other element of the trust management. Thus, it is necessary to discuss and analyze the security mechanism of the TMS in this paper. With these research problems in mind, we analyze the security issues existing in the trust management, and make use of the public-key cryptography to design a trust information management assurance protocol, to counter the possible security threats in the TMS, such as Sybil attacks and trust information tamper attacks in transmissions, etc.

C. Authors and Affiliations

Dr Akash Singh is working with IBM Corporation as an IT Architect and has been designing Mission Critical System and Service Solutions; He has published papers in IEEE and other International Conferences and Journals.

He joined IBM in Jul 2003 as a IT Architect which conducts research and design of High Performance Smart Grid Services and Systems and design mission critical architecture for High Performance Computing Platform and Computational Intelligence and High Speed Communication systems. He is a member of IEEE (Institute for Electrical and Electronics Engineers), the AAAI (Association for the Advancement of Artificial Intelligence) and the AACR (American Association for Cancer Research). He is the recipient of numerous awards from World Congress in Computer Science, Computer Engineering and Applied Computing 2010, 2011, and IP Multimedia System 2008 and Billing and Roaming 2008. He is active research in the field of Artificial Intelligence and advancement in Medical Systems. He is in Industry for 18 Years where he performed various role to provide the Leadership in Information Technology and Cutting edge Technology.

REFERENCES

[1] Dynamics and Control of Large Electric Power Systems. Ilic, M. and Zaborszky, J. John Wiley & Sons, Inc. © 2000, p. 756.

[2] Modeling and Evaluation of Intrusion Tolerant Systems Based on Dynamic Diversity Backups. Meng, K. et al. Proceedings of the 2009 International Symposium on Information Processing (ISIP'09). Huangshan, P. R. China, August 21-23, 2009, pp. 101–104

[3] Characterizing Intrusion Tolerant Systems Using A State Transition Model. Gong, F. et al., April 24, 2010.

[4] Energy Assurance Daily, September 27, 2007. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration Division. April 25, 2010.

[5] CENTIBOTS Large Scale Robot Teams. Konoledge, Kurt et al. Artificial Intelligence Center, SRI International, Menlo Park, CA 2003.

[6] Handling Communication Restrictions and Team Formation in Congestion Games, Agogino, A. and Tumer, K. Journal of Autonomous Agents and Multi Agent Systems, 13(1):97–115, 2006.

[7] Robotics and Autonomous Systems Research, School of Mechanical, Industrial and Manufacturing Engineering, College of Engineering, Oregon State University

[8] D. Dietrich, D. Bruckner, G. Zucker, and P. Palensky, "Communication and computation in buildings: A short introduction and overview," *IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3577–3584, Nov. 2010.

[9] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Comput. Networks*, vol. 50, pp. 877–897, May 2006.

[10] S. Paudyal, C. Canizares, and K. Bhattacharya, "Optimal operation of distribution feeders in smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4495–4503, Oct. 2011.

[11] D. M. Laverty, D. J. Morrow, R. Best, and P. A. Crossley, "Telecommunications for smart grid: Backhaul solutions for the distribution network," in *Proc. IEEE Power and Energy Society General Meeting*, Jul. 25–29, 2010, pp. 1–6.

[12] L. Wenpeng, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in *Proc. IEEE PES, Transmission Distrib. Conf. Expo.*, Apr. 19–22, 2010, pp. 1–4.

[13] Y. Peizhong, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline

under WiFi interference for smart grid applications," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 110–120, Mar. 2011.

[14] C. Gezer and C. Buratti, "A ZigBee smart energy implementation for energy efficient buildings," in *Proc. IEEE 73rd Veh. Technol. Conf. (VTC Spring)*, May 15–18, 2011, pp. 1–5.

[15] R. P. Lewis, P. Igic, and Z. Zhongfu, "Assessment of communication methods for smart electricity metering in the U.K.," in *Proc. IEEE PES/IAS Conf. Sustainable Alternative Energy (SAE)*, Sep. 2009, pp. 1–4.

[16] A. Yarali, "Wireless mesh networking technology for commercial and industrial customers," in *Proc. Elect. Comput. Eng., CCECE*,May 1–4, 2008, pp. 000047–000052.

[17] M. Y. Zhai, "Transmission characteristics of low-voltage distribution networks in China under the smart grids environment," *IEEE Trans. Power Delivery*, vol. 26, no. 1, pp. 173–180, Jan. 2011.

[18] V. Paruchuri, A. Durresi, and M. Ramesh, "Securing powerline communications," in *Proc. IEEE Int. Symp. Power Line Commun. Appl., (ISPLC)*, Apr. 2–4, 2008, pp. 64–69.

[19] Q.Yang, J. A. Barria, and T. C. Green, "Communication infrastructures for distributed control of power distribution networks," *IEEE Trans. Ind. Inform.*, vol. 7, no. 2, pp. 316–327, May 2011.

[20] T. Sauter and M. Lobashov, "End-to-end communication architecture for smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1218–1228, Apr. 2011.

[21] K. Moslehi and R. Kumar, "Smart grid—A reliability perspective," *Innovative Smart Grid Technologies (ISGT)*, pp. 1–8, Jan. 19–21, 2010.

[22] Southern Company Services, Inc., "Comments request for information on smart grid communications requirements," Jul. 2010

[23] R. Bo and F. Li, "Probabilistic LMP forecasting considering load uncertainty," *IEEE Trans. Power Syst.*, vol. 24, pp. 1279–1289, Aug. 2009.

[24] *Power Line Communications*, H. Ferreira, L. Lampe, J. Newbury, and T. Swart (Editors), Eds. New York: Wiley, 2010.

[25] G. Bumiller, "Single frequency network technology for fast ad hoc communication networks over power lines," WiKu-Wissenschaftsverlag Dr. Stein 2010.

[31] G. Bumiller, L. Lampe, and H. Hrasnica, "Power line communications for large-scale control and automation systems," *IEEE Commun. Mag.*, vol. 48, no. 4, pp. 106–113, Apr. 2010.

[32] M. Biagi and L. Lampe, "Location assisted routing techniques for power line communication in smart grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 274–278.

[33] J. Sanchez, P. Ruiz, and R. Marin-Perez, "Beacon-less geographic routing made partical: Challenges, design guidelines and protocols," *IEEE Commun. Mag.*, vol. 47, no. 8, pp. 85–91, Aug. 2009.

[34] N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi, "The deployment of a smart monitoring system using wireless sensors and actuators networks," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 49–54.

[35] S. Dawson-Haggerty, A. Tavakoli, and D. Culler, "Hydro: A hybrid routing protocol for low-power and lossy networks," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 268–273.

[36] S. Goldfisher and S. J. Tanabe, "IEEE 1901 access system: An overview of its uniqueness and motivation," *IEEE Commun. Mag.*, vol. 48, no. 10, pp. 150–157, Oct. 2010.

[37] V. C. Gungor, D. Sahin, T. Kocak, and S. Ergüt, "Smart grid communications and networking," Türk Telekom, Tech. Rep. 11316-01, Apr 2011.