

Towards an Analysis of Information Sharing Metrics

Sandeep Bhattaram, Seth Wilson, Henry Hexmoor
Department of Computer Science and Computer Engineering
University of Arkansas, Fayetteville, Arkansas 72701.
{sbhatta, slw08, hexmoor}@uark.edu

Abstract—Our work on sensor networks and information routing protocols has provided us with an approach to examine secure information in a trust network. In this paper we outline a couple of metrics and offer an analysis of theoretical minits allowed by our metrics. Our theories are substantiated by simulated experiments.

1. INTRODUCTION

The universal phenomenon of engaging in communication describes a modus operandi for sorting, categorizing, understanding and interpreting messages one receives from others. An information provider conveys a message to the listener. This message might be the information that is of interest to the listener or it might be shared at random without any prior request or interest. In either case, as a result of such sharing it is evident that the data or facts in the message are firstly duplicated at the recipient's end; also, the pertinent information is now shared with and disclosed to the listener, supplementing the listener's knowledge base. We term this process information sharing.

E-Business transactions that deal with sensitive data in the form of digital documents highlight the security concerns of the information sharing processes transpiring across the originator's or the organization's boundaries. Any detail that permeates these boundaries to reach a group of agents that are not desired to hold this information from the information originator's view point (i.e., agents belonging to competing organizations) might be considered as a breach in security. In open systems, participants (i.e., human users, computational agents and services) are likely interacting with others whom they may not know. The agents might enter or leave the system at any instant of time. These dynamic factors pose greater risks with regards to the leaking of information and its misuse thereafter. The more information is gathered and assimilated, the more intelligent an individual becomes in reducing any such uncertainty that may exist therein.

The necessity of information sharing is also pronounced in the context of homeland security concerns. However, the need for information to flow freely among agents in a community working across various law-enforcement agencies is at odds with the need for preserving the inherent security of such information flow. The role played by communication and sharing of information among interacting agents in dynamic and open environments thus accentuates the need for both qualitative and quantitative analysis of the process of information sharing, level of security established and metrics that quantify its overall system health.

The main focus of our continuing research from [1] is to analyze, both qualitatively and quantitatively, societies of agents and organizations for different measures of secure information sharing from a trust-based soft security perspective. There is a slow but certain paradigm shift in the field of security from the traditional models of security called *hard security* to what is termed as *soft security*. Hard security mechanisms provide security through a physical barrier; for example, the different levels of sensitivity and access based on such classification in security models such as the Onion Skin model [2] and the Bell Lapadula model. Furthermore, hard security also includes mechanisms such as user-ids and passwords, public and private keys, and certificates as security tokens. These solutions are effective, but only in centrally controlled domains. Hard security mechanisms also suffer from the atomic nature in providing security; an all-or-nothing property wherein the malicious agent can enter the system multiple times and at any instant of time after she gains access to the appropriate token. Thus, these models are not malleable and don't consider such important factors as uncertainty, time, and fluidity of the relationships in open systems. We have therefore embarked upon formulating security policies that are based on soft security mechanisms such as *inter-agent trust*.

Soft security approaches assume the existence of malicious agents in a system and restrict their participation over a period of time. This approach to security is more flexible, adaptable and applicable to myriad security concerns. Trust embodies a positive social connectivity concept. In any interaction or information exchange between two parties, there is a positive expectation in the trusted party to behave or act in a constructive manner [3]. Trust adds naturalness to the interactions and considers mutuality in beliefs, expectations and respect. The concept of trust does not

guarantee absolute security to the system; rather it provides levels and forms of security in a given social system. In the context of information sharing, sensitive information will not be shared with those insufficiently trusted. A breach of security results in a breach of trust, which is quickly and easily remedied. Perpetually untrustworthy individuals are eliminated, and in turn the overall security of the organization is maintained.

This paper is organized into the following sections: Section 2 discusses the trust-based organizational model and provides definitions of some of the key terms of our continuing work on measures of trust-based information sharing. Section 3 puts forth the qualitative and quantitative analysis of the information sharing metrics and introduces the *rehabilitation* phase of our model, a process of rebuilding trust among agents in an organization. In section 4, we present the current literature in the field of trust emphasizing on general notions of trust and trust establishment. The paper concludes with the discussions and future work in Section 5.

2. TRUST-BASED ORGANIZATIONAL MODEL

In the trust-based organizational model, the organization and its constituent agents are considered social entities. Given this societal orientation, the entities we establish base their relationships and interactions upon the human resource of trust. In our model, information originating from independent and disparate sources is gathered, compiled, and shared by and among many individuals in the organization. Each agent in the society continuously senses and processes information. She also has a recurring need for information. This acts as an incentive for agents to continuously share information and facts they garner. Human networks such as law-enforcement agencies share these same goals, and thus are examples of networks that are well suited for our trust-based organizational model. The formal definitions of the notions in the trust-based organizational model are presented in the following paragraphs.

The *trust-based organizational model*, *TOM*, is $(O, A, F, ITR, TT, ISP, EI, TPM, ISA)$. O is a set of organizations. For simplicity, we consider our model to consist of a single organization. A is a set of known agents, and F is a fact warehouse, a set of known and static facts. We assume that these elements of the model are known a priori. An *agent*, $a_k \in A$, also denoted as a_k is a known intelligent, autonomous entity. A *fact*, $f_i \in F$, is a datum. Each agent in an organization has a requirement for a fact and produces a fact. An agent's fact requirement, selected from the fact warehouse, is assumed to remain constant. The fact produced and the fact requirement for the agent can be the same. Another agent might require the fact produced by an agent. Agents are not cognizant of other agents' requirements. This is a simplifying assumption we make in this work that will affect the information sharing and its availability. Agent x 's *trust* in agent y is agent x 's

estimation of the probability that agent y will preserve agent x 's welfare with regard to the information transmitted [4]. The *interaction trust relation*, *ITR*, is a trust relation among agents. *ITR*, denoted as $\mathbf{t}(a_i, a_j)$, is the trust agent i has in agent j , where $a_i, a_j \in A$. A trust relation, \mathbf{t} , is an adjacency matrix that contains trust values between its constituent entities. The trust values are quantified in a non-discrete manner as a real value in the range 0.0 to 1.0. If $\mathbf{t}(x, y)$ exists, agent y is said to be the *neighbor* of agent x . The trust relation between agents is assumed a priori. An agent is cognizant of her trust in her neighboring agents which can vary as the system progresses over time. However, the neighboring agents are not apprised of the trust the agent has in each of them. A trust value of 1.0 indicates agent x 's complete trust in agent y . If there exists no initial trust relation between agent x and agent y , agent x either has lack of trust in agent y or agent x is ignorant or cannot make a trust-related judgment about agent y . We make this simplifying assumption initially by interpreting the aforementioned cases as the same and assigning a trust value of 0.0 to them. The *trust threshold*, *TT*, is a user-defined static minimal trust value that guards information sharing, i.e. a threshold. The trust threshold value lies in the range 0.0 to 1.0, both inclusive. Trust threshold is pivotal to the decision that an agent makes, based on trust, in propagating a fact to her neighbors.

Information sharing is the exchange of information that is owned by an agent among agents in the organization in succession with an assumption that the information might satisfy at least one agent's requirement, including its originator. A *cycle* is the amount of time taken by an agent to receive or generate a fact and share it with her neighbors. An agent's *accessible facts* constitute the fact generated by her in the current cycle and the facts that she receives from her neighbors in the previous cycle, if any. An agent is *satisfied* if and only if the fact required by her is the same as the fact she has access to. An agent is *willing* to receive facts if she is not satisfied with the facts she currently has access to. The *information-sharing protocol*, *ISP*, is a collection of rules that govern the information sharing from the transmitting agent (say agent x) to the recipient agent (say agent y) in the TOM. They map to a boolean value representing agent x 's compliance to the rules. If agent x and agent y are neighbors, agent x checks if her trust in agent y is greater than the pre-defined trust threshold value (*ISP1*), and if agent y is willing to accept any facts in the current cycle (*ISP2*). If both the aforementioned conditions hold true agent x propagates the fact to agent y . If agent x and agent y are not neighbors, the initiator agent monitors the traversal path of the fact in every cycle for breaches in security based on the mentioned criteria.

The *agent fact path* of a fact is a sub-graph, where the nodes represent agents that constitute the fact traversal path during information sharing and the edges represent the trust between the agents. An agent fact path is constructed for every fact as it is shared among agents in each cycle. The initiator agent of every fact can query the agent fact path to

obtain the list of agents that are currently in possession of the fact. She checks to determine if her trust in the recipient agents warrants their receiving the fact and classifies them into intended and unintended receivers. An agent a_j is an *intended receiver* in the agent fact path if the ISP1 and ISP2 are true and the agent a_j is not satisfied after receiving the fact. An agent a_j is an *unintended receiver* in the agent fact path if either ISP1 or ISP2 or both are false and the agent a_j is not satisfied after receiving the fact. *Information availability*, IA, is the degree to which information is freely available when shared among a group of agents. *Security Measure*, SM, is the number of unintended receivers. IA_j and SM_j represent the IA and SM values, respectively, at the end of the j th cycle. IA_j is formulated as the sum of number of agents who are satisfied and the number of intended receivers in the j th cycle in Equation 1. Note that the sets, intended receivers and satisfied agents, are disjoint. SM_j is formulated as the number of unintended receivers in the j th cycle in Equation 2. IA and SM are system level information sharing metrics that are measured continuously in the TOM at the end of every cycle to analyze the overall health of the system. The aim of the TOM in terms of IA and SM is to maximize IA and minimize SM, which satisfies our intended objective of maximizing the information sharing while minimizing the breaches in security. *Expiration interval (EI)*, a system level metric, is the number cycles for which a fact can be shared after its creation. A fact is said to be *expired* after its expiration interval.

$$IA_j = \text{Number of intended receivers}_j + \text{Number of satisfied agents}_j \quad (1)$$

$$SM_j = \text{Number of unintended receivers}_j \quad (2)$$

The *trust policy model*, TPM, defines the calculus of trust update policies that regulates the corresponding interaction trust relations if any of the facts' recipients are unintended receivers. The overarching goal considered for the design of these policies is to simultaneously maximize information sharing and minimize unintended receivers. Trust policy models have been devised such that varying degrees of restriction can be applied on the paths leading to unintended receivers. These are applied for every fact that is generated in the system. Thus, using the agent fact paths of the facts generated, every agent can track the different paths or channels (both trusted and covert) that exist in the system. TPM_i ($i=1, 2, \text{ or } 3$) offers such calculi for trust update. The subscript i refers to the varying degrees of restriction that is applied on the trust relations once an unintended receiver is detected. TPM_1 reduces the trust relation between every consecutive pair of agents in a fact path exponentially starting from the unintended receiver back toward the initiator agent by a user-defined trust decrement, based on the relative positions held by the agent in the agent fact path. In TPM_2 , for every edge in the agent fact path, trust is updated with the same user-defined trust decrement factor. The third trust policy model, TPM_3 , is envisioned to update the trust between the initiator agent and every agent in the

path by the decrement factor. TPM_4 , a combination of TPM_1 and TPM_3 , and TPM_5 , a combination of TPM_2 and TPM_3 have also been considered in the trust update calculus with TPM_1 as the least restrictive and TPM_5 as the most restrictive.

In our *trust-based information sharing algorithm*, ISA, trust-based information flooding occurs continuously in each cycle for every agent. An agent produces a unique fact and shares it with all the neighbors who are trusted and willing to receive a fact. Each recipient agent checks if her fact requirement is any one of the facts that are accessible to her in the current cycle. If a fact satisfies her fact requirement, she is not willing to receive any other fact for the current cycle and she will not share that fact in the next cycle. If none of the accessible facts satisfies her requirement, she is willing to receive facts for the current cycle. $\#generatedfacts_{i,j}$ represents the number of facts generated by a_i in the j th cycle, which is only one fact in our model. $\#receivedfacts_{i,j}$ represents the number of facts received by a_i in the j th cycle. All the accessible facts of an agent that don't satisfy her fact requirement are shared with her neighbors, which would be checked by the recipient agents in the next cycle. Such information sharing continues until the fact expires. At the end of every cycle the initiator agents monitor the current recipients of their unexpired facts. By applying ISPs, the initiator agents can easily determine the covert channels that might lead to unintended receivers and correspondingly apply TPM_1 , TPM_2 , TPM_3 or any combination of the three in order to eliminate them.

3. ANALYZING INFORMATION SHARING METRICS

From the trust-based ISA, the ideal values for the system level metrics, IA and SM, as outlined in Figure 1, are expected to saturate at the upper bound on IA and remain at its lower bound value of zero, respectively, as the number of cycles increases. If the number of unintended receivers in the system is zero, as in Figure 1, each agent can either be a satisfied agent or an intended receiver. In this context, the *IA contribution* of an agent is the percentage of total IA that has resulted from the facts generated by her. Then for all the facts that are generated by an agent and are currently shared in the system, every subsequent recipient of those facts in every subsequent cycle increases the agent's IA contribution. Thus, all the agents contribute to the IA of the system; which characterizes an ideal system. One of the key steps towards achieving an ideal state is to estimate the upper bound on the IA. In the latter half of the section, we theorize the formulation for *maximal information availability (MIA)*, which represents the upper bound on the IA given any social network. Firstly, in the following paragraphs we analyze the ISA with regards to the information sharing metrics, IA and SM, is presented.

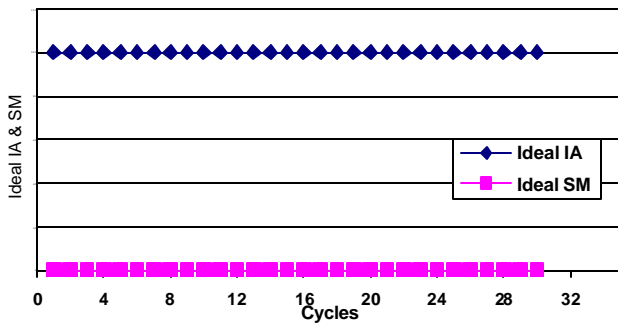


Figure 1 – Ideal IA at MIA and Ideal SM at zero over Cycles

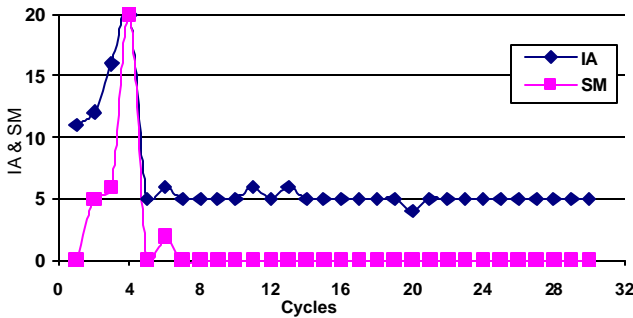


Figure 2 - IA and SM of TOM over Cycles

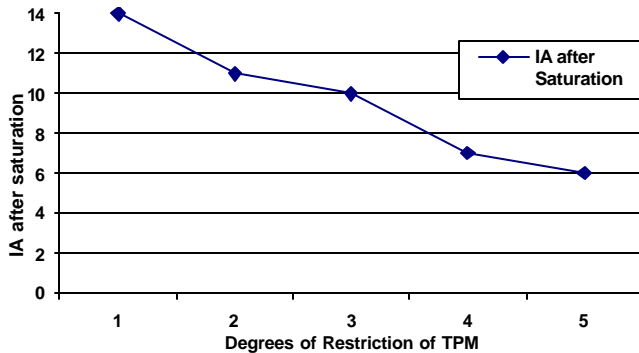


Figure 3 - IA after saturation over Degrees of Restriction of TPM

From the results of the qualitative analysis of ISA in Figure 2, the IA values increase and stabilize at a particular value as the number of cycles increases. This suggests that the degree to which information becomes available to the agents in the network increases and reaches a constant value as time progresses. In addition, SM reaches a value of zero and retains that value as the number of cycles increases. This suggests that the number of security breaches in terms of the unintended receivers is zero. Initially there is an increase in the number of unintended receivers in parallel to the increase in the number of satisfied and intended receivers. The facts in the system are shared initially for a certain interval of time before unintended receivers and corresponding application of the TPM ensue. The restrictions hence applied set the SM to lower values; this eventually reaches a minimal value of zero over a period of time. From the results shown in Figure 2, it is easily

observed that IA and SM reach their expected levels as the cycles increase when TPM is applied.

However, from the Figure 2 it is also observable that the values of IA become a constant, but at a lower value. The application of the trust decrement factor in the TPM is attributed for the lower saturation value of IA. In the TPM, as the unintended receivers arise, the corresponding trust decrement factor is reduced from the inter-agent trust edges. This reduces the number of edges that can communicate, if the trust value before applying the TPM is very close to the pre-defined TT. The number of facts that can be shared among such edges also decrease correspondingly. The system subsequently reaches the expected levels of IA and SM as given in Figure 2. The channels of information sharing that continue to exist after the expected levels are reached are only the trusted channels, i.e., every edge in the channel has a trust value greater than the TT. This property is desirable. However, a decrease in the IA after saturation as the degree of restriction of TPM increases is also evident from Figure 3. This suggests inverse proportionality between IA after saturation and trust policy models, and proposes a trade-off between the degree of restriction in the TPM and the IA. Thus, to meet our initial goal of maximizing IA, we realize the need to rebuild the trust relationships as the system evolves over a period of time with the application of the trust policy models. The state of the system wherein trust relationships are dynamically modified to achieve the dual objective of maximizing IA and minimizing SM is called the *steady state* of the system. The literature also points out such models of societies wherein there exist regulations that punish and reward the agents concomitant to their contribution to the society's goals.

The work in [5], in discussing the fragile nature of the interconnectedness among agencies and individual agents, states that if agents violate the regulations of functioning of the society, a threat of punishment is required to fulfill their duties and meet personal goals and the goals of the system. This assumes that an agent tries to avoid the risk of defeating her goals in trying to violate the system's goals and thus acts in sync with the specified laws. It is observable that in any social system the more an agent contributes to the societal goals the greater are the rewards that she receives in turn from the society. The mutually symbiotic existence of the individuals of a society results in a behavior wherein the goals of both the society and the individual agent are achieved. Hence, a balance is established between individually rational decisions and socially rational decisions at every agent in each of her actions [6]. This property of societies of agents makes multi-agent systems and social sciences an important field of study. Hence, a *rehabilitation* phase is proposed as an inclusion to our trust organizational model, wherein an agent rebuilds her trust in the agents of the system. The goal of every agent in the system is to maximize her contribution towards the IA of the system, which in turn maximizes the net IA of the system. This can be achieved if the agent

establishes new trust relationships or upgrades her existing relationships by assigning trust values in such a way that the IA that results from the facts she generates increases while keeping the overall SM at the minimal value of zero. This property characterizes pareto-optimality of the system, wherein re-establishment of trust results only in a net gain, with regards to the metrics IA and SM. To achieve the maximum IA in the rehabilitation phase and reach the proposed steady state, a measure of the upper bound of IA vis-à-vis *maximal IA (MIA)* is required. Given any social network of n agents, the quantitative formulation of the MIA is obtained from the following analysis.

Lemma 1: The minimum number of consecutive connections between the source agent of a fact and the fact's unintended receiver is always equal to two.

Proof: This Lemma can be proved using the concept of trust-based flooding. In trust-based flooding, a fact is shared from the source agent (say agent x) to her neighboring agent (say agent y) only if the neighboring agent is sufficiently trusted. Now if agent y shares the fact with another agent z that is not trusted by agent x , then agent z is considered to be an unintended receiver by agent x . If agent z is sufficiently trusted by agent x , then agent x and agent z would have been neighbors and agent x would have shared the fact with agent z also in the first place, along with agent y . Thus, the minimum number of edges between the source agent of a fact and the fact's unintended receiver in the current cycle is always equal to two.

Lemma 2: The total IA and total SM of the system in any cycle are the sum of the IA and SM of all the unique facts generated by the agents respectively.

Proof: In each cycle, every agent generates a unique fact. This uniqueness is achieved from the combination of cycle number and agent identity. The fact is shared with the source agent's trusted neighbors in the first cycle, then with their neighbors and such sharing continues until the EI is reached for that fact. In each cycle, the agents currently in possession of the fact produced by the source agent can be classified as intended, unintended or satisfied agents. Note that the three sets are disjoint for a fact. An agent can be in possession of more than one fact produced by different source agents. Thus, an agent can be an intended, an unintended or a satisfied agent in the same cycle but for different facts. Since each agent is concerned with the covert channels that exist for the facts she has generated, a particular recipient agent can be accounted for one of the three categories for each of the source agents. The contribution of a source agent towards the net IA in the current cycle is then equal her IA contribution in the same cycle. Thus, the total IA in the current cycle is the sum of IA at each agent for each fact she generated in the same cycle.

Lemma 3: MIA is achieved when the number of satisfied agents is zero and the number of cycles for which the fact exists in the social network is equal to EI.

Proof: From Section 2, we know that a satisfied agent doesn't share the satisfying fact in the next cycle. This reduces the IA contribution of the source agent in the next cycle because the fact ceases to be shared after the current satisfied agent. In addition, if no agent is satisfied all recipient agents are either intended or unintended receivers, who continue to share the facts they are not satisfied with, which includes also their generated facts. Also, the number of facts received by an agent in the current cycle is the same as the IA of the previous cycle. Thus, in this case, the IA at the end of each cycle accrues on the IA in the previous cycle resulting in the maximum possible IA. Based on this we can easily deduce, from the definition of EI, that the MIA is achieved only on completion of the number of cycles for which the fact is valid, i.e. until EI is not expired.

Lemma 4: MIA is achieved when the social network is a fully connected graph, i.e., a clique.

Proof: From the definition of the ITR we can construct a trust graph for the social network. An agent x that has a directed edge to agent y with a weight of $t(x, y)$ is said to trust agent y with the trust value $t(x, y)$. The trust value can be greater or less than the trust threshold. Herein, we assume that every edge in the fully connected social network is a trusted edge, i.e. its weight is greater than the trust threshold. In such a social network, considering Lemma 1 and Lemma 3 it can be easily seen that no agent is an unintended receiver. Thus, the facts in each cycle are sent to every other agent in the network until the fact validity interval expires, while accruing the IA at each cycle.

Theorem: Given any social network of n agents (where n is an integer ≥ 3), the maximal information availability after the expiration of the fact validity interval is computed by Equation 3 provided no agent is satisfied with her fact requirement.

$$MIA_{EI} = (n) * (n-1) * ((n-1)^{EI} - 1) / (n-2) \quad (3)$$

Proof: Given the number of agents in the social network as n , where $n \geq 3$. From Lemma 4 we know that MIA is achieved when the social network is a fully connected graph. For the case of a fully connected graph, in the ISA, each agent shares all the facts that she received in the current cycle (i.e., received facts generated and carried over from the previous cycle and the facts generated in the current cycle) to every agent in the network in the subsequent cycle. This behavior of the system can be described in Equation 4 from Lemma 2. Let i represent the index of an agent wherein a_i belongs to A , j represent the cycle number where $j < EI$, $out-degree_{i,j}$ represent the out-degree of a_i at the beginning of the j th cycle in the social network, $\#receivedfacts_{i,j-1}$ represent the number of facts received by agent i at the end of $(j-1)$ th cycle, and $\#generatedfacts_{i,j}$ represent the number of facts generated by agent i in the j th cycle.

$$\begin{aligned}
IA_j &= \sum_{i=1}^n (\text{outdegree}_{i,j} * \\
&\quad (\#receivedfacts_{i,j-1} + \#generatedfacts_{i,j})) \quad (4) \\
&= \sum_{i=1}^n ((n-1) * (\#receivedfacts_{i,j-1} + 1))
\end{aligned}$$

(out-degree of an agent in a fully connected graph is $n-1$)

$$\begin{aligned}
&= ((n-1) * \sum_{i=1}^n \#receivedfacts_{i,j-1}) + (n-1) * n \\
&= (n-1) * IA_{j-1} + n * (n-1)
\end{aligned}$$

(an agent receives every fact from every agent in $j-1$ cycle)

$$IA_j = (n-1) * (n + IA_{j-1})$$

Applying recursive substitution for the value of IA_j , the IA at the end of the j th cycle is given by,

$$IA_j = (n) * (n-1) * ((n-1)^j - 1) / (n-2) \quad (5)$$

The MIA can be derived from the Equation 5 if j holds for every cycle until EI is reached. The proof for this is derived using mathematical induction as follows,

Step 1: Let $j = 1$ in the base case step. We need to verify that $IA_1 = (n) * (n-1)$. Substituting $j = 1$ in Equation 5, we get,

$$IA_1 = (n) * (n-1) * ((n-1)^1 - 1) / (n-2) = (n) * (n-1)$$

The base case is true for a social network of n nodes that is fully connected because after the first cycle each agent has shared her fact with every other agent. The total IA is thus equal to the number of edges in the network, i.e., $(n) * (n-1)$.

Step 2: Let us make an inductive assumption wherein the equation holds for the general case of $j = k$

$$IA_k = (n) * (n-1) * ((n-1)^k - 1) / (n-2)$$

Step 3: In this inductive step we must prove the following assertion, "If there is a k such that the equation of IA_k holds true, then IA_{k+1} should also hold true for the same k ."

Let $j = k + 1$.

$$IA_{k+1} = (n-1) * (n + IA_k)$$

(Applying recursive substitution for the value of IA_k)

$$IA_{k+1} = n * (n-1) * ((n-1)^{k+1} - 1) / (n-2)$$

The inductive step holds true for the case $j = k + 1$. Therefore, IA at the end of the j th cycle is given by IA_j . From Lemma 3, MIA is achieved at the end of EI and this is represented in Equation 6.

$$MIA_{EI} = (n) * (n-1) * ((n-1)^{EI} - 1) / (n-2) \quad (6)$$

•

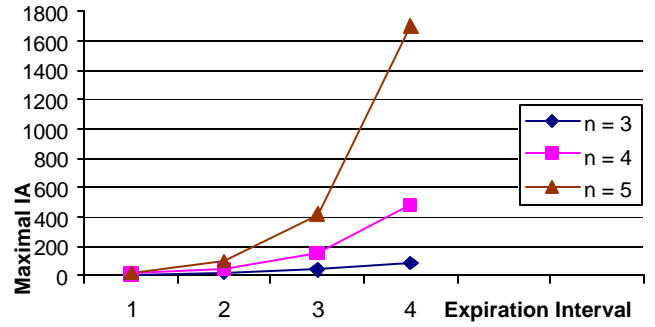


Figure 4 - Maximal IA over EI (simulated experiment)

Given that every edge in the trust graph is a fully trusted edge, i.e. with a value 1.0, and that the network is fully connected (from Lemma 4), we can conclude from the analysis of the trust-based ISA and the information sharing metrics that the MIA depends on the number of agents in the trust graph, n , and the value of EI. This conclusion is reflected in Equation 6, which puts forth the following relationships between EI, MIA and n : MIA is directly proportional to the EI and MIA is directly proportional to n . Figure 4 describes the results of simulating the trust-based ISA for a fully connected graph and with each edge being fully trusted. The simulations have been run on fully connected and fully trusted graphs of degrees 3, 4, 5. The values of MIA have been observed for EI values of 1,2,3,4 and the corresponding MIA values are depicted in Figure 4. We observe from the graph that the values of MIA are directly proportional to EI and n . The graphical results foster the aforementioned conclusions drawn from the analysis as well as Equation 6. Further, the values of MIA obtained from the Equation 6 and the simulation of the ISA match. Thus, in addition to the information sharing metrics results depicted in Figure 2, the experiments conducted corroborate the following theoretical conclusions: the formulation of MIA and the directly proportional relationship between MIA and EI, and MIA and n .

4. RELATED WORK

Trust has a silent presence in all social interactions [7]. It forms a crucial element in making organizational decisions and framing security policies, and building secure e-business applications [8], [9], [10]. Gambetta in [11] proposed the following definition of trust: "Trust (or symmetrically distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action." Alfaraz Abdul Rahman and Stephen Hailes, adopt this definition of trust as a basis in their work in [11], [12], [13]. Trust, in [10], is defined as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context. Multiple definitions of the concept of trust exist in literature that are suited to domains of their respective works rather than a generalized notion [10], [14].

Tyrone Grandison and Morris Sloman analyze the intrinsic nature of trust in e-commerce scenarios in [10], [15] and discuss the importance of trust in those contexts. Sara Jones, et al. in [9], recognize the Internet, open systems, their complexity, and vulnerabilities of digital objects in such rapidly evolving systems as key drivers behind the specification of trust in the interactions among entities. A generic model of identifying and positioning trust relationships is presented in [8]. Vertical trust relationships such as dependability, accountability and authenticity, and horizontal trust relationships such as business, personal and physical trust are established within the hierarchy of an organization and between organizations, respectively. [10] discusses concerns regarding the trust establishment process such as unintentional and conditional transitivity of trust, different functional mappings between trust relationships, and the different levels of trust assigned. Broadly, two types of trust relationships have been identified in literature, the *direct trust* and the *recommended trust*. The net trust value is formulated as a combination of direct and recommended trust values. Direct trust corresponds to the view of the source agent that is computing the trust value towards the target agent. Recommended trust is the trust value computed by collecting the trust values from the viewpoints of other agents in the network. This becomes necessary in cases when the source agent has no prior relationship or history of interactions with the target agent. In such scenarios the source agent checks the properties of the target agent (that are important for furthering her goals) from the perspective of the neighboring agents whom she trusts.

The trust framework SULTAN (Simple Universal Logic-oriented Trust Analysis Notation) in [16], [17] proposes constructs for specifying the direct and recommended trust relationships. A word-of-mouth mechanism is used for building trust in [12]. A decentralized approach towards a reputation based trust establishment is chosen by the authors in [11], [12], [13], wherein trust of a subject is calculated instantaneously by taking a product of recommended trust value and the trust values of the edges (between interacting agents) on the recommendation path, and calculating the minimum of all the path values. Work in [14] parallels the abovementioned concepts in building a trust relationship between a source and a sink node. The sink node's reputation is computed from the majority of the trust ratings of the source's neighboring agents, if the ratings can be directly computed by them. If not, they aggregate it through the majority of each of their neighbor's ratings about the sink node. This continues until at least one agent obtains the ratings of the sink node. The net trust value at the source is then computed by passing the trust rating back to the source. Similar rating methodologies, called *confidence ratings*, have been employed by [18], which are based on the concept of reputation. Trust is a notion that is closely knit with other social concepts such as risk, expectation, probability, and reputation. A large section of the literature studies the various properties of trust using the mentioned secondary social concepts. The popular advogato trust metric in [19] applies Ford-Fulkerson's max flow min cut

algorithm to the trust graph between the source and the target agent and computes the trust value by performing network flow computation. The trust graph here is viewed as certifications and name, key bindings. In [20], the author describes the trust metric that meets the theoretical best case in resisting different types of attacks. Appleseed [21] is yet another trust metric that bases its evaluation on spreading activation models (which are based on human memory). A finite amount of energy injected into the system at a node in the trust graph is allowed to spread in the graph based on the normalized weights of the edges. The agents are then ranked based on the energy accumulated at each node.

The fields of trust and trust management are largely concerned with the definitions of trust, trust establishment methodologies, trust management policies and attack resistance. Each work presented here has made a significant contribution to the field of trust management and trusted computing from the soft security point of view. Our current work concerns the trust-based information sharing and the trust establishment processes (in the rehabilitation phase), and we have been influenced by the literature discussed herein.

5. DISCUSSIONS

Trust-based information sharing algorithm, presented in this paper, answers the problem of maximizing IA while minimizing the breaches in security to a large extent. However, the steady state of the system with the MIA, as formulated in Section 3, is not fully realized. The rehabilitation phase aims to answer this question by building a dynamic model of trust establishment between agents to improve the overall IA of the system. This brings about the properties of pareto-optimality, self-healing and self-configuration among the agents in the society in trying to meet their personal goals and the organizational goals. We identify trust establishment and the process of combining different values of trust obtained from different entities as recommendations for a particular subject as open problems. Trust negotiation is a prominent model of establishing initial trust relationships between organizations or agents by revealing credentials in a pre-defined fashion [22]. To establish the trust relationships in the rehabilitation phase we hope to introduce the concept of trust negotiation, but from a soft security perspective, in our future direction of work. Negotiation, between the source agent and the agents affected by the inclusion of a trusted edge between the source and the target agent, plays an important role in the trust building process. New challenges and questions such as, "which target agent is chosen by a source agent to re-establish a trust relationship?", "what is the structure of negotiation?" and "what is the basis for assignment of the trust value?" arise in the analysis, which we hope to answer in our future work.

ACKNOWLEDGMENT

This work is supported by the AFOSR grant FA9550-04-1-0429.

REFERENCES

- [1] Henry Hexmoor, Sandeep Bhattaram, and Seth L. Wilson, "Trust-Based Security Policies", In the *Proceedings of Secure Knowledge Management Conference*, Buffalo, New York, USA, September 22-24, 2004, pages 33-38.
- [2] Britton, C. and Bye, P. *IT Architectures and Middleware: Strategies for Building Large Integrated Systems*. 2nd ed. Addison-Wesley Professional, 2004.
- [3] Jøsang, Audun. "The Right Type of Trust for Distributed Systems". In *Proceedings of the New Security Paradigm Workshop '96*, Lake Arrowhead, CA, USA, September 16-19, 1996, pages 119-131.
- [4] G. Beavers, H. Hexmoor, "Understanding Agent Trust", In *Proceedings of The International Conference on Artificial Intelligence (IC-AI 2003)*, June 2003, pages 769-775.
- [5] Partha Dasgupta. "Trust as a Commodity". In Diego Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations*, Oxford: Basil Blackwell 2000, chapter 4, pages 49-72.
- [6] Hogg, L. M. J. and Jennings, N. R. "Socially Intelligent Reasoning for Autonomous Agents". *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, Vol. 31, No. 5, September 2001.
- [7] Abdul-Rahman, A. and Hailes, S., "Supporting Trust in Virtual Communities", In *IEEE Proceedings of the Hawaii International Conference on System Sciences*, Maui, Hawaii, January 4-7, 2000.
- [8] Mortaza Bargh, Wil Janssen and Alko Smit, "Trust and Security in E-business Transactions", Telematica Institute, The Netherlands, 2002
- [9] Jones, S., Wilikens, M., Morris, P., and Masera, M. "Trust Requirements in E-Business". In *Communications of the ACM, 2000*, Vol. 43, Issue 12, pages 81-87.
- [10] Grandison, T. and Sloman, M., "A Survey of Trust in Internet Applications". In *IEEE Communications Surveys and Tutorials*, Vol. 3, No. 4, October-December, 2000, pages 2-16.
- [11] Diego Gambetta. "Can We Trust Trust?" In Diego Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations*, Oxford: Basil Blackwell 2000, chapter 13, pages 213-237.
- [12] Alvarez Abdul-Rahman and Stephen Hailes. "A Distributed Trust Model". In *Proceedings of the New Security Paradigm Workshop'97*, Langdale, Cumbria, UK, September 23-26, 1997, pages 48-60.
- [13] Alvarez Abdul-Rahman and Stephen Hailes. "Using Recommendations for Managing Trust in Distributed Systems." In *Proceedings of IEEE Malaysia International Conference on Communication'97 (MICC'97)*, Kuala Lumpur, Malaysia, November 11-13, 1997.
- [14] Golbeck, J. and Hendler, J., "Inferring Reputation on the Semantic Web". In *Proceedings of the Thirteenth International World Wide Web Conference (WWW2004)*, New York, NY, USA, May 2004 ACM Press (2004)
- [15] Tyrone Grandison and Morris Sloman. "SULTAN - A Language for Trust Specification and Analysis". In *Proceedings of the 8th Annual Workshop HP OpenView University Association (HP-OVUA)*, Berlin, Germany, June 24-27 2001.
- [16] Grandison, T. and Sloman, M., 2002. "Specifying and Analysing Trust for Internet Applications". In *Proceedings of the 2nd IFIP Conference on E-Commerce, e-Business, and e-Government (I3e 2002)*, Lisbon, Portugal, October 7- 9.
- [17] Tyrone Grandison and Morris Sloman. "SULTAN - A Language for Trust Specification and Analysis". In *Proceedings of the 8th Annual Workshop HP OpenView University Association (HP-OVUA)*, Berlin, Germany, June 24-24, 2001.
- [18] Siebes, R., van Harmelen, F. "Ranking Agent Statements for Building Evolving Ontologies". In *Proceedings of the AAI-02 Workshop on Meaning Negotiation*, Alberta, Canada, 2002.
- [19] Levien, R. "Attack Resistant Trust Metrics". Draft Ph.D. Thesis . June 27, 2002.
- [20] R. Levien and A. Aiken. "Attack-Resistant Trust Metrics for Public Key Certification". In *Proceedings of the 7th USENIX Security Symposium*, San Antonio, Texas, January 1998, pages 229-242.
- [21] Ziegler, C.N., Lausen, G. "Spreading Activation Models for Trust Propagation". In *Proceedings of the IEEE International Conference on e-Technology, e-Commerce, and e-Service*, Taipei, Taiwan, IEEE Computer Society Press (2004), pages 83-97.
- [22] T. Barlow, A. Hess, and K. E. Seamons. "Trust Negotiation in Electronic Markets". In *Eighth Research Symposium in Emerging Electronic Markets*, Maastricht, Netherlands, September 2001.