International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012

DOI: 10.7321/jscse.v2.n7.4

Research on the Algorithm of the Trustful Communication over the Metrized Small World Distributed Data Storage System

Dmitry Gusev
Nizhny Novgorod State Technical University, Nizhny Novgorod, the Russian Federation
dgusev@nntu.nnov.ru

Abstract. **In ideal distributed network each node is in trust with all others. But in a real world there is no guarantee that all the nodes will operate with their prescribed rules. There might be ones which malfunction because of the incorrect internal object state and the ones which are infected by an external subject. These use cases reveal the need in trust policies utilized in the network. Because of the distributed nature of the system more effective security algorithm will be the one which implies the trust evaluation without centralized authorities. In this paper we investigate a possibility of developing the secure network where its actors can fully trust each other over the system Metrized Small World (MSW) from the Meralabs LLC.**

Keywords: *distributed data storage, Metrized Small World, semi-metric, trust propagation, trust model, trustful search algorithm*

1. Introduction

A Metrized Small World [1] is a scalable decentralized data storage model where the data units are dynamically consolidated into an overlay network in the form of a so called small world graph. This network is used to navigate through data units during search and new unit addition processes. Small world structures maintain a small average amount of links for every node, at the same time ensuring that every node is accessible from any other node in a small number of link steps. This means that no matter which data unit will be chosen as a start point of the search process, the result can be obtained in a small amount of steps compared to the size of the structure. To determine the right direction for search process and to create the structure where similar data units are properly clustered (cluster is a collection of objects which are “similar” among them and are “dissimilar” to the objects belonging to other clusters [2]), a metric (proximity measure) between data units and queries is added to the small world graph resulting in a Metrized Small World data structure. By design it supports the extensibility because of utilizing the XML [3] in describing the data nodes and XLink [4] in specifying the links between them. This gives an opportunity to use the MSW as a base for a trust network by adding trust policies parameters to the nodes description. Under trustful network we mean the one which nodes are able to evaluate trustworthiness of other nodes, detect the malicious nodes and isolate them from the communications.

The one of the MSW applications is to store and share data. The data sharing requires defining the access rights. As the mentioned system is distributed the centralized administration is not efficient [5] or in some cases may not be easily deployed [6], so the decentralized access control based on a level of trust between the items of the system might become a solution. The current research is aimed to investigate developing a trustful communication over the MSW system and to proof that the system will maintain its key features: extensibility and logarithmic search time. The importance of the research results is in that they should help to adopt the MSW system to the industrial needs.

The focus of this paper is to develop the algorithm of the trustful communication over the MSW system, to point the possible issues and limitations and to predict changing of the MSW system characteristics with introducing the trust properties to the search algorithm.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

The paper is organized as follows: in the "Pure Metrized Small World" section we overview the data structure and the main processes of the raw MSW system. In the "Trust Policies" section we define the trust term and describe the entropy-based trust model. Then in the "Implementing Trustful Communication" section we present the modified search algorithm which will incorporate the calculations of trust.

2. Pure Metrized Small World

The nodes of the MSW system are not static as in traditional databases because each one contains the extensible message processing module, so the special term is used for them – Active Data Unit (ADU). Each ADU consists of the following components [7]:

1. XML content.
2. List of XLink links to other ADUs.
3. Message processing module.

Each of these components has a unique Uniform Resource Identifier (URI) which is a sub-URI of the base URI of the ADU, so that if the URI of any of components is known, the URIs of other components can be trivially calculated. Links in the list (2) point to the base URIs of other ADUs.

ADUs communicate with each other and with non-ADU actors (such as MSW clients) by means of XML messages. Each message contains the following information:

1. Message identifier which determines the semantics of processing of the message.
2. List of string parameters which further specify the details of processing.
3. List of attached XML documents involved in the processing of the message.

The communication is based on a pull model, which means that after a request message is processed, the response message is returned to the sender of the original message. If HTTP (Hypertext Transfer Protocol) is used as a transport protocol, the original message would be sent in an HTTP POST request and the response message would be received in the HTTP response. The latter means that non-ADU agents are not required to have URIs in order to send messages to and obtain responses from ADUs, but cannot receive messages other than responses to their own messages. Such approach perfectly suites the needs of the Web because of its session based communications.

Active data units use the resources of servers which host them and their base URIs are sub-URIs of the server base URI. Therefore at the network level the storage can be viewed as a set of servers processing ADUs and exchanging messages pertaining to those ADUs. But ultimately the ADUs, not the servers, are the endpoints of communication; hence the distribution of ADUs between servers is irrelevant to the semantics of the communication, influencing only the time which is necessary for the messages to reach the destination. The communication of ADUs processed by the same server is logically indistinguishable from the communication of ADUs processed by different servers but can be significantly faster because the network is not involved.

The Metrized Small World distributed data structure built over the ADUs utilize them as vertices of the graph, and by the links locally stored in each ADU which these represent the edges of the graph. For every link (A, B) stored in ADU A, there is a reverse link (B, A) stored in the ADU B, so the MSW graph can be considered undirected. No ADU can contain a link to itself.

To ensure that the data structure formed by ADUs has the following properties: decentralization of both data and data access, accessibility of data in relatively short time compared to the volume of data in the storage, scalability and ability to work with weakly structured data, the next requirements must be met:

1. Any ADU in the structure must be able to serve as an entry point of access to other elements. This is necessary for decentralization since having fixed entry points would create a bottleneck for data access. In the real life scenarios the client might preconfigure the any number of known ADUs to connect to the MSW distributed data storage though their URIs

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

2. A relatively short path must exist between every two ADUs to ensure search in a small number of operations compared to the number of ADUs.
3. Any ADU must store a relatively small number of links so that the access to individual links will not present storage and search complexity problems in itself.

There are also requirements pertaining to the method of construction of the structure rather than to the structure itself: addition of a new ADU must not require iteration over the whole set or a large subset of ADUs and reconfiguration of the links between previously added ADUs. The search operation prepends the addition and its key function is to compare ADUs. In the MSW there is a unified proximity measure between ADUs and between the search pattern and an ADU, called the semi-metric. The semi-metric is calculated between two arbitrary XML documents, i.e. either between the content of two ADUs or between the content of an ADU and the search pattern. The search pattern is considered to have the same structure as ADUs which are expected to match it with relevant XML elements or attributes set to specified values and irrelevant XML elements omitted from the pattern.

There three possible processes in the MSW structure [7]:

1. Searching for existing ADUs.
2. Adding new ADUs.
3. Modifying existing ADUs.

The third process is performed by marking the ADU being modified as obsolete and creating a new version of that ADU with different URI and modified data. The ADUs marked as obsolete will not appear in search results but still can serve as intermediate points in a search process.

The second and the third processes depend on the first one; that is why the search operation is important to be secured in real world scenarios.

3. Trust Policies

Under securing the search we mean performing the operation where all involved parties trust each other. This is critical for establishing communication in the distributed environment because there are no central controlling nodes in the structure and multiple processes of adding new nodes and searching for existing data can be performed independently and simultaneously.

Before applying the trust to the communication in the Metrized Small World system we will define the trust in the following way: “trust is a level of likelihood with which an agent will perform a particular action before such action can be monitored and in a context in which it affects our own actions” [8]. There is a significant difference between what trust is based on in real life, and what it should be based on for the purpose of information security. Humans can be irrational, and so can trust. Irrational trust is not based on knowledge, but for example on faith. The right type of trust for distributed systems should be based on knowledge as much as possible [9]. We will define knowledge as information which can be used for a specific purpose. In this case we are interested in information which can be used for determining trustworthiness in a chosen category [10]. Any information which contributes to this task then becomes knowledge.

A user of a system can never obtain perfect knowledge of the system he uses nor of the threats, and he is therefore unable to exactly evaluate the system security. By gathering as much knowledge as one can about the system, a user will get an idea or a belief about the security, or in other words, a certain trust in the system. The trust thus reflects the user knowledge about the system security. Trust and security can be said to represent two sides of the same thing. Security reflects the idealistic side like, for example, formal modeling, design and development, or in short how we would like the systems to be in theory. Trust on the other hand reflects the realistic side of system knowledge taking into account that no formal model is perfect and those errors will always persist no matter how strict the design procedures are [9].

Then we will formulate the terms used in the calculations of trust.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

- Trust is a relationship established between two entities for a specific *action*. The first entity will be called the *subject*; the second entity will be the *agent*. We introduce the notation *{subject: agent, action}* to describe a trust relationship.
- Trust is a function of uncertainty. In particular, if the subject believes that the agent will perform the action for sure, the subject fully "trusts" the agent to perform the action and there is no uncertainty; if the subject believes that the agent will not perform the action for sure, the subject "trusts" the agent not to perform the action, and there is no uncertainty either; if the subject does not have any idea of whether the agent will perform the action or not, the subject does not have trust in the agent. In this case, the subject has the highest uncertainty.
- The level of trust can be measured by a continuous real number, referred to as the *trust value*. Trust value should represent uncertainty.
- The subjects may have different trust values with the same agent for the same action. Trust is not necessarily symmetric. The fact that entity *A* trusts entity *B* does not necessarily means that *B* also trusts *A*.

The concept of trust is the certainty of the subject about whether or not the agent will perform an action. Let *T {subject: agent; action}* denote the trust value of the trust relationship *{subject: agent; action}*, and *P {subject: agent; action}* denote the probability that the agent will perform the action in the subject's point of view. Information theory states that entropy is a nature measure for uncertainty [8]. Thus, we define the entropy-based trust value as:

$$T\{subject:\ agent;\ action\} = \begin{cases} 1 - H(p), & for\ \ 0.5 \le p \le 1 \\ H(p) - 1, & for\ \ 0 \le p \le 0.5 \end{cases} \quad (1)$$

where $H(p) = -p \cdot \log_2(p) - (1-p) \cdot \log_2(1-p)$ and $p = P\{subject\ :\ agent;\ action\}$. The trust value is a continuous real number in [-1, 1]. This definition satisfies the following properties. When $p = 1$, the subject trusts the agent the most and the trust value is *1*. When $p = 0$, the subject distrusts the agent the most and the trust value is *–1*. When $p = 0.5$, the subject has no trust in the agent and the trust value is *0*. In general, trust value is negative for $0 \le p \le 0.5$ and positive for $0.5 \le p \le 1$. Trust value is an increasing function with p.

While the trust is propagated the uncertainty increases. This can be explained in the following way. When the subject establishes a trust relationship with the agent through the recommendation from a third party, the trust value between the subject and the agent should not be more than the trust value between the subject and the recommender as well as the trust value between the recommender and the agent:

$$|T_{AC}| \le \min(|R_{AB}|, |T_{BC}|),$$

where $T_{AC} = T\{A : C, action\}$, $R_{AB} = T\{A : B, recommendation\}$ and $T_{BC} = T\{B : C, action\}$.

When the trust is propagated through different paths the trust is not reduced: if the subject receives the same recommendations for the agents from multiple sources, the trust value should be no less than that in the case where the subject receives less number of recommendations.

The trust based on multiple recommendations from single source should not be higher than that from independent sources. When the trust relationship is established jointly through concatenation and multipath trust propagation, it is possible to have multiple recommendations from a single source [11]. Since the recommendations from a single source are highly correlated, the trust built on them should not be higher than the trust built upon recommendations from independent sources.

In this paper we will operate with the methods for calculating trust via concatenation and multipath

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

propagation based on entropy. Such methods are referred to as *trust models*.

In the entropy-based model the trust propagations are calculated directly from trust values defined in (1). For concatenation trust propagation shown in Fig. 1 (nodes *A, B, C*), node *B* observes the behavior of node *C* and makes recommendation to node *A* as $T_{BC} = T\{B : C, action\}$. Node *A* trusts node *B* with $R_{AB} = T\{A : B, recommendation\}$. The question is how much node *A* should trust node *C* to perform the action. To show that the trust value is not increased while concatenation propagation one way to calculate $T_{ABC} = T\{A : C, action\}$ is

$$T_{ABC} = R_{AB} \cdot T_{BC} \qquad (2)$$

Note that if node *B* has no knowledge about node *C* (i.e. $T_{BC} = 0$) or if node *A* has no knowledge about node *B* (i.e. $R_{AB} = 0$), the trust between *A* and *C* is zero, i.e., $T_{ABC} = 0$.

For multipath trust propagation shown in Fig. 1 (nodes *A, B, D, C*), let $R_{AB} = T\{A : B, recommendation\}$, $T_{BC} = T\{B : C, action\}$, $R_{AD} = T\{A : D, recommendation\}$, $T_{DC} = T\{D : C, action\}$. Thus, *A* can establish trust to *C* through two paths: *A – B – C* and *A – D – C*. To combine the trust established through different paths, we use maximal ratio combining as [8]:

$$T\{A : C, action\} = w_1(R_{AB} \cdot T_{BC}) + w_2(R_{AD} \cdot T_{DC}) \qquad (3)$$

where $w_1 = \frac{R_{AB}}{R_{AB} + R_{AD}}$ and $w_2 = \frac{R_{AD}}{R_{AB} + R_{AD}}$. In this model if any path has the trust value 0, this path will not affect the final result. It is noted that the weight factors in our model are based on recommendation trust R_{AB} and R_{AD}.

The expressions (2) and (3) satisfy the listed trust propagation rules. Since $T \in [-1,1]$, the multiplication in (2) will make the absolute value of $T\{A : C, action\}$ smaller or equal to $|T\{A : B, recommendation\}|$ and $|T\{B : C, action\}|$. Thus we proved that the concatenation propagation of trust does not increase trust. When applying (2) and (3) to the special cases illustrated in Fig. 1: $R_{AB} = R_{AD} = R_{AB'} = R$ and $T_{BC} = T_{DC} = T_{B'C'} = T$ we obtain $T_{AC} = R \cdot T$ and $T_{AC'} = \frac{R^2 \cdot T + R^2 \cdot T}{R + R} = T_{AC}$. So, we see that the multipath propagation of trust does not reduce trust. When applying the model to the cases in Fig. 1: $R_{AG1} = R_{AG2} = R_{AB'} = R_2$, $R_{G1E} = R_{G2F} = R_{B'E'} = R_{B'F'} = R_3$ and $T_{EC} = T_{FC} = T_{E'C'} = T_{F'C'} = T_2$ we see that trust based on multiple recommendations – entities *E, F* and *E', F'* – from a single source – entity *A* – should not be higher than that from independent sources because $T_{AC} = T_{AC'} = \frac{R_2 \cdot R_3^2 \cdot T_2 + R_2 \cdot R_3^2 \cdot T_2}{R_3 + R_3}$.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

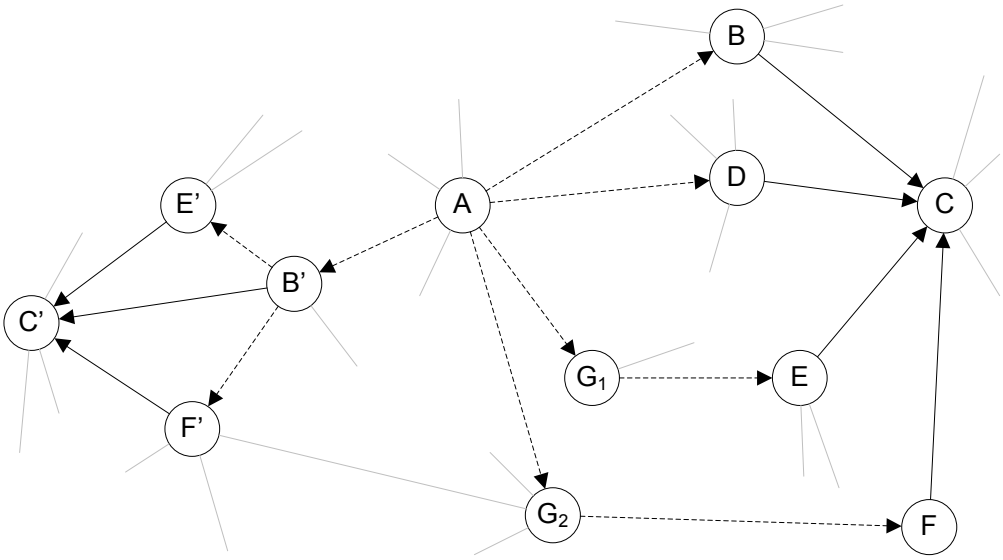

Figure 1. Trust propagation in the Metrized Small World network.

4. Implementing Trustful Communication

The original search algorithm in the MSW system is the following [12]:

The *i* is the current number of nodes in the system. The *n* is the number of algorithm steps per search query. We are going to search the node with the search pattern v_s.

1. Arbitrarily select an ADU v_k where $1 \le k \le i-1$.
2. Let VisitedList be the set of visited ADUs.
3. Let CandidateList be the set of candidate ADUs for returning result, assume initially it contains only v_k.
4. Let the v_R be the resulted ADU, initially is empty.
5. For *j* = *1* to *n* do
   a. Sort CandidateList by value of semi-metric to v_s in ascending order.
   b. Select the first ADU *p* from CandidateList not contained in VisitedList. If no such ADU exists then return v_R.
   c. Let the v_R be the *p*.
   d. Add *p* to VisitedList.
   e. Add the set of *p* neighbor ADUs to CandidateList.

In this algorithm every ADU has the ability to find any ADU. In other words, the search party can read the neighbor list and the contents of any ADU. To make the communication between the nodes trustful we propose to limit the availability of the neighbor list and all or some contents of an ADU based on the number of common ADUs between the search party and the examined ADU and the trust values to the search party stored in the common ADUs.

The search algorithm should be modified it in the following way:

The *i* is the current number of nodes in the system. The *n* is the number of algorithm steps per search

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

query. We are going to search the node with the search pattern v_s.

1. Arbitrarily select an ADU v_k where $1 \le k \le i-1$.
2. Let VisitedList be the set of visited ADUs.
3. Let CandidateList be the set of candidate ADUs for returning result, assume initially it contains only v_k.
4. Let the $v[]_R$ be the list of resulted ADUs, initially is empty.
5. For $j = 1$ to n do
   a. Sort CandidateList by value of semi-metric to v_s in ascending order; the ADUs with more opened contents appear first.
   b. Select the first ADU p from CandidateList not contained in VisitedList with at least one opened contents field or neighbors list.
   c. If no such ADU exists then
      i. Decrease the trust level for the ADUs from CandidateList not contained in VisitedList with no contents and neighbors information.
      ii. Again arbitrarily select an ADU v_k, initialize the CandidateList with this value and continue to the next iteration.
   d. If at least one contents field in the p is opened then
      i. Increase the trust level for the p
      ii. Add or update $v[Length-1]_R$ with the p.
   e. Add p to VisitedList.
   f. If p shares its neighbors with the search party then add the set of p neighbor ADUs to CandidateList.
   g. If p does not share its neighbors with the search party then
      i. Decrease the trust level for the p
      ii. Again arbitrarily select an ADU v_k, initialize the CandidateList with this value

In this model we expect the probability of successful strict search to be decreased in comparison with the 100% of the pure MSW. The search procedure will have several attempts n which finally will return the n or less resulted ADUs close to search pattern. There might be less resulted ADUs because some of the ADUs might share only the neighbor lists and only route the search queries though themselves. Such behavior is very common to real world because the requirements are not always strict and the products in the market do not always perfectly suit the requirements.

The precision of results of the search will be increasing while the ADUs will share more contents fields and open the neighbors list. There is a direct correlation between the search results precision and the trust level in the network. Such a system encourages nodes to act in a trustworthy manner to provide more accurate services [13]. The main goal is to save the *log(O)* average search time appropriate to the pure MSW, but to make the network as much secure as possible.

5. Conclusion and Future Work

In this paper we address the Metrized Small World distributed data storage system in aspect of implementing the trust network over it, the principles and the main processes were investigated. The trust term and the entropy-based trust model were described, which will be utilized in the future calculations. In the simulation part of the paper we modified the search algorithm of the MSW by adding the trust related operations into it: managing access to different information based on the reputation of the search party. The assumption was made about the direct correlation between the search results precision and the trust level in the network.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.7, 2012
Published online: July 25, 2012
DOI: 10.7321/jscse.v2.n7.4

Limitation of the work is in the small amount of real-world data which might be utilized in the experiments. We used to fill the MSW storage system with items containing a random data. This is a fundamental research issue because the probability density function of the input data might strongly affect the resulted search time. In the future work we will need to obtain the test database with enough real-world information.

Another open research issue is in that we examined only one concept of trust – based on the entropy. Such approach does not handle the difference between the unexpected incorrect action and a harmful action. In the future work we will investigate more concepts of trust, for example, based on the previous transaction results history which will form a reputation of a party [8] or rendezvous based trust scheme which assumes sending two types of tickets, trust-request and computed-trust, which will meet in some common rendezvous node with certain probability [14].

The direction of the future work will be focused on managing the two opposite characteristics of the network: the search results precision and the trust level between the parties; and we are going to proof that the average search time will remain logarithmic.

References

[1] Metrized Small World Active Data Storage Overview, http://www.meralabs.com/projects/active/, 06/03/2012
[2] S.Nithya, R.Manavalan "An Ant Colony Clustering Algorithm Using Fuzzy Logic", International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 2, No. 5, 2012, Doi: 10.7321/jscse.v2.n5.2
[3] XML 1.1 Specification, http://www.w3.org/TR/2006/REC-xml11-20060816/, 06/03/2012
[4] XLink 1.1 Specification, http://www.w3.org/TR/xlink11/, 06/03/2012
[5] Seyed Saeed Sadat Noori, Seyed Ali Sadat Noori, Seyed Morteza Lari Baghal "Optimization of Routes in Mobile Ad hoc Networks using Artificial Neural Networks", International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 2, No. 4, 2012, Doi: 10.7321/jscse.v2.n4.4
[6] Abderreahmen Mtibaa, Khaled Harras “Social-Based Trust Mechanisms in Mobile Opportunistic Networks” in Proc. IEEE SIMNA, 2011
[7] V. Krylov, A. Logvinov, A. Ponomarenko, D.Ponomarev "Active Database Architecture for XML Documents" in Proc. CAINE. ISCA, 2008. P. 244-249.
[8] Yan Sun, Wei Yu, Zhu Han, K. J. Ray Liu "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", IEEE JSAC special issue on security in wireless ad hoc networks, Vol. 24, No.2, February, 2006.
[9] A. Jøsang "The right type of trust for distributed systems" in Proc. NSPW 1996. The Norwegian University of Science and Technology, 1996.
[10] A. Abdul-Rahman, S. Hailes “A distributed trust model” in Proc. of 1997 New Security Paradigms Workshop, ACM Press, 1998, pp. 48–60.
[11] A. Jøsang "An Algebra for Assessing Trust in Certification Chains" in Proc. NDSS. ISOC, 1999.
[12] V. Krylov, A. Logvinov, A. Ponomarenko, D.Ponomarev "Metrized Small World Properties Data Structure" in Proc. SEDE. ISCA, 2008. P. 203-208.
[13] R. Guha, R. Kumar, P. Raghavan, A. Tomkins “Propagation of trust and distrust” in Proc. of the 13th International World Wide Web Conference, 2004.
[14] Ningning Cheng, Kannan Govindan, Prasant Mohapatra “Rendezvous Based Trust Propagation to Enhance Distributed Network Security” in Proc. IEEE INFOCOM, 2011

Free download and more information for this paper