www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Measuring and Increasing the Security in Large-Scale Wireless Ad Hoc Networks

[1]Mr. R. NavinKumar, MCA.,MPhil., Associate Professor/MCA
[2]Mr. P. Vimal Raj, Final MCA,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: navinsoccer@gmail.com, vimalraj2515@gmail.com

***Abstract*—The growth of networks such as the Internet and wireless cellular systems, over the last decade has surpassed many expectations. Indeed, going back in time to the origins, it would have been hard to imagine the importance and scale to which these networks have developed. Now, projecting into the future, they strongly believed that this trend will continue, if not accelerate. Hence, the communication devices and protocols of today must be capable of operating with the same efficiency in the very large-scale networks of the future. This highlights the need for asymptotic analysis on a network and its corresponding protocol design, which characterizes the asymptotic behaviors of network performance as its size grows. This is especially the case for wireless ad hoc networks (WANETs).**

***Index Terms*- Multi Agent Systems (MASs), Secure Link Augmentation (SLA), Wireless Ad Hoc Networks (WANETs),**

I. INTRODUCTION

In a multi-agent system, agents interact with each other to achieve a definite goal that they cannot achieve alone and such systems include P2P, grid computing, the semantic web, pervasive computing and MANETs. Multi-agent Systems (MASs) are increasingly becoming popular in carrying valuable and secured data over the network.

Nevertheless, the open and dynamic nature of MAS has made it a challenge for researchers to operate MAS in a secured environment for information transaction. Malicious agents are always seeking ways of exploiting any existing weakness in the network. This is where trust and reputation play a critical role in ensuring effective interactions among the participating agents. Researchers have long been utilizing trust theory from social network to construct trust models for effectively suppressing malicious behaviors of participating agents.

Trust issues have become more and more popular since traditional network security approaches such as the use of firewall, access control and authorized cortication cannot predict agent behavior from a 'trust' viewpoint.

II. RELATED WORKS

In the paper "An Agent-Based Approach For Building Complex Software Systems" [1] the author *NICHOLAS R. JENNINGS* stated that Building high-quality, industrial-strength software is difficult.

Indeed, it has been argued that developing such software in domains like telecommunications, industrial control, and business process management represents one of the most complex construction tasks humans undertake. Against this background, a wide range of software engineering paradigms have been devised.

Each successive development either claims to make the engineering process easier or promises to extend the complexity of applications that can feasibly be built. Although evidence is emerging to support these claims, researchers continue to strive for more effective techniques.

To this end, this article will argue that analyzing, designing, and implementing complex software systems as a collection of interacting, autonomous agents (that is, as a multiagent system [11]) affords software engineers a number of significant advantages over contemporary methods.

This is not to say that agent-oriented software engineering represents a silver bullet [12]—there is no evidence to suggest it will represent an order of magnitude improvement in productivity. However, the increasing number of deployed applications [13, 14] bears testament to the potential advantages that accrue from such an approach.

In seeking to demonstrate the efficacy of agent-oriented techniques, the most compelling argument would be to quantitatively show how their adoption improved the development process in a range of projects. However, such data is simply not available (as it is not for approaches like patterns, application frameworks, and componentware).

"A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities" [3] the authors *LI XIONG AND LING LIU* stated that One way to minimize threats in such an open community is to use community-based reputations, which can be computed, for example, through feedback about peers' transaction histories.

Such reputation information can help estimating the trustworthiness and predicting the future behavior of peers. This paper presents a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. There are two main features of their model.

First, they argued that the trust models based solely on feedback from other peers in the community is inaccurate and ineffective. In addition to feedback a peer receives through its transactions with other peers, they incorporated the total number of transactions a peer performs, and the credibility of the feedback sources into the model for evaluating the trustworthiness of peers.

Second, they introduce two adaptive factors, the transaction context factor and the community context factor, to allow the metric to adapt to different domains and situations and to address common problems encountered in a variety of online communities. With the problems of Trust Parameters Overcoming Inaccuracy and Non-flexibility, they designed and developed PeerTrust model.

In PeerTrust, a peer's trustworthiness is defined by an evaluation of the peer in terms of the level of reputation it receives in providing service to other peers in the past. Such reputation reflects the degree of trust that other peers in the community have on the given peer based on their past experiences in interacting with the peer.

They identified important factors for such evaluation: the feedback in terms of amount of satisfaction a peer obtains through transactions with others, the number of transactions the peer has performed with other peers, the credibility of the feedbacks submitted by peers, the transaction context factor, addressing the impact of transaction characteristics (such as values or types of the transactions) on the trustworthiness of the peers, and the community context factor, addressing the impact of community-specific properties on the trustworthiness of peers.

They illustrated the importance of these parameters through a number of example scenarios and address the problems with feedback-only methods. They formalized these factors, and show that they play an equally important role in evaluating the trustworthiness of a peer.

In the paper "Developing an Integrated Trust and Reputation Model for Open Multi-Agent Systems" [4] the authors *DONG HUYNH, NICHOLAS R. JENNINGS AND NIGEL R. SHADBOLT* stated that Trust and reputation are central to effective interactions in open multi-agent systems in which agents, that are owned by a variety of stakeholders, can enter and leave the system at any time. This openness means existing trust and reputation models cannot readily be used.

They presented FIRE, a trust and reputation model that integrates a number of information sources to produce a comprehensive assessment of an agent's likely performance. Specifically, FIRE incorporates interaction trust, role-based trust, witness reputation, and certified reputation to provide a trust metric in most circumstances. FIRE is empirically benchmarked and is shown to help agent's effectively select appropriate interaction partners.

Their Role-based trust (RT) models the trust resulting from the role-based relationships between two agents (e.g. owned by the same company, a service provider and its registered user, friendship relationship of their owners). Since there is no general method for computationally quantifying trust based on this type of relationship, we use rules to assign RT values. This means end users can add new rules to customise this component to suit their particular applications.

In the paper "A Computational Model of Trust and Reputation" [5] the authors *LIK MUI, MOJDEH MOHTASHEMI* AND *ARI HALBERSTADT* stated that

Despite their many advantages, e-Businesses lag behind brick and mortar businesses in several fundamental respects. The paper concerned one of these: relationships based on trust and reputation. Recent studies on simple reputation systems for e-Businesses such as eBay have pointed to the importance of such rating systems for deterring moral hazard and encouraging trusting interactions.

However, despite numerous studies on trust and reputation systems, few have taken studies across disciplines to provide an integrated account of these concepts and their relationships. The paper first surveys existing literatures on trust, reputation and a related concept: reciprocity. Based on sociological and biological understandings of these concepts, a computational model is proposed. This model can be implemented in a real system to consistently calculate agents' trust and reputation scores.

The EigenTrust Algorithm for Reputation Management in P2P Networks [7] the authors *SEPANDAR D. KAMVAR MARIO T. SCHLOSSER HECTOR GARCIA-MOLINA* stated that Peer-to-peer file-sharing networks are currently receiving much attention as a means of sharing and distributing information.

However, as recent experience shows, the anonymous, open nature of these networks offers an almost ideal environment for the spread of self-replicating inauthentic files. They described an algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads.

They presented a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network.

A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities" [8] the authors *LI XIONG AND LING LIU* stated that Peer-to-Peer eCommerce communities are commonly perceived as an environment offering both opportunities and threats.

One way to minimize threats in such an open community is to use community-based reputations, which can be computed, for example, through feedback about peers' transaction histories. Such reputation information can help estimating the trustworthiness and predicting the future behavior of peers.

Their paper presented a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. There are two main features of their model.

First, they argued that the trust models based solely on feedback from other peers in the community is inaccurate and ineffective. They introduced three basic trust parameters in computing trustworthiness of peers. In addition to feedback a peer receives through its transactions with other peers, they incorporated the total number of transactions a peer performs, and the credibility of the feedback sources into the model for evaluating the trustworthiness of peers.

Second, they introduced two adaptive factors, the transaction context factor and the community context factor, to allow the metric to adapt to different domains and situations and to address common problems encountered in a variety of online communities. They presented a concrete method to validate the proposed trust model and report the set of initial experiments, showing the feasibility and benefit of their approach.

III. METHODOLOGY

A. Problem Description

Bayesian network based trust model believes that trust is multi-dimensional and agents need to evaluate trust from different aspects of an agent's capability. This model uses bayesian network and bayesian probability to calculate trust. This model's main flaw lies in the assumption that all the agents have identical bayesian network architecture which is unrealistic because different agents have different requirements which leads to different network architecture.

In case of aggregating recommendation from other agents, this model assumes that all the agents are truthful in providing their feedbacks. This assumption is also not realistic as malicious agents will often provide false feedback to other agents to disrupt the system.

Load balancing is the severe problem in the existing system. For selective scenario, it first computes the trust of agents who respond to a transaction request and then it selects the agent with the highest trust value. However, in this scenario the agent with the highest trust value will have immense workload while other capable agents with slightly lower reputation will have considerably less workload.

The problem that will arise from this disproportionate allocation of workload is that the quality of service will fall greatly due to the heavy workload present at the highly trusted agents. So a load balancing algorithm is required for the sustainability of good service quality.

Security vulnerabilities in software have been a significant problem for the computer industry for decades. While the use of safer programming languages such as Java and C# has alleviated the problem, there are still many software packages that are created and maintained in C and C++. This is primarily driven by concerns about performance and access to low-level constructs, which is not always possible in languages executed in a managed environment. On the other hand, writing safe and secure programs in C and C++ is difficult, despite an increase in education and the availability of safer APIs designed to help detect errors.

As a result, the challenge of finding mechanisms to detect and remove vulnerabilities persists. With the large amount of code written every year, it should be noted that despite the fact that the vulnerability density is decreasing, the overall number of vulnerabilities is increasing. Many techniques have been developed to eliminate vulnerabilities, but none of them provides a complete solution.

Modern static analysis tools are capable of finding many varieties of programming errors, but a lack of runtime information limits their abilities. Some also have a relatively high false positive rate, making them expensive to use in practice. Dynamic and runtime tools are often not effective because they lack a baseline to use for detection. This thesis considers the problem, and provides the solution for the problem.

B. Existing System

- The existing system cannot minimize both (common transmission range and probability of neighboring nodes having a primary security association) to maintain secure connectivity.
- Security mechanism induced in end-to-end secure paths in such WANETs is more challenging than in conventional networks.
- The communication devices and protocols of today is not capable of operating with the same efficiency in the very large-scale networks of the future.
- Some keying materials for primary security associations (SAs), which we will formally define later, are already preconfigured in communication devices based on the trust relationships among the persons involved.
- Cannot provide secure communications for arbitrary node pairs when needed.

C. Proposed System

The price of security (performance degradation) we have to pay in WANETs. It design a protocol to achieve the optimal secure network performance or minimize the price of security. In this project, these questions with rigorous analysis based on reasonable assumptions on WANETs are answered.

The proposed system formally characterizes the tradeoffs between key predistribution related to and secure network performance. The results show that the minimal price of security with SLA is strictly smaller than that without SLA, which theoretically necessitates SLA operations in WANETs with security requirements.

Also the proposed system designs two schemes to achieve the minimal price of security with or without SLA, respectively. Furthermore, these schemes provide several important insights on protocol design for secure communications in WANETs as follows. 1) It is unnecessary and even harmful to think that in order to achieve the minimal price of security, and have to obtain as many derived secure links as possible.

Advantages

- Considers both network performances with and without Secure Link Augmentation.
- Based on a general random network model, the dynamic behaviors of secure throughput and delay with the common transmission range and the probability of neighboring nodes having a primary security association are quantified when the network size is sufficiently large.
- Securing a physical link is possible between two neighboring nodes even if they are not friends
- The costs and benefits of secure link augmentation operations on the secure network performance are also analyzed.

D. Satisfaction

Satisfaction function measures the degree of satisfaction an agent has about a given service provider. In other words, it keeps record of the satisfaction level of all the transactions an agent makes with another agent. However, instead of storing all of the transaction history we have defined an exponential averaging update function to store the value of

satisfaction. This greatly reduces the storage overhead and at the same time assigns time relative weight to the transactions. Let, $Sat^{t}_{n}(p, q)$ represent the amount of satisfaction agent p has upon agent q based on its service up to n transactions in the time interval.

The satisfaction update function is definedas follows-

$$Sat^{t}_{n}(p,q) = \alpha \times Sat_{cur} + (1-\alpha) \times Sat^{t}_{n-1}(p,q)$$

Here, Sat_{cur} represents the satisfaction value for the most recent transaction and we have used a feedback based system where an agent rates other agent's service quality according to the following function.

$$Sat_{cur} = \begin{cases} 0, & \text{if transaction is fully unsatisfactory} \\ 1, & \text{if transaction is fully satisfactory} \\ \in (0,1), & \text{otherwise} \end{cases}$$

E. Load Balancing Among Agents

An algorithm is proposed for balancing loads among the trusted agents. For selective scenario, it first computes the trust of agents who respond to a transaction request and then we select the agent with the highest trust value. However, in this scenario the agent with the highest trust value will have immense workload while other capable agents with slightly lower reputation will have considerably less workload.

The problem that will arise from this disproportionate allocation of workload is that the quality of service will fall greatly due to the heavy workload present at the highly trusted agents. So a load balancing algorithm is required for the sustainability of good service quality.

In the load balancing algorithm either a heuristic value of workload is calculated and the agent is chosen with the smallest load or a probabilistic choice is made based on the computed trust value of agents. The load balancing algorithm is started by first classifying the responders (agents that respond to a transaction request) into two groups namely-good service providers (G) and unknown service providers (U) based on a threshold value of trust (γ). Then first seek to choose an agent from G by computing an approximate value (heuristic value) of load present at each responders in G. Sorting the responders in increasing order of load, take the responder with the smallest workload.

In case of no responders being present in the class G an agent is selected from U either probabilistically based on its trust value or randomly.

Algorithm

Input: Evaluating agent p and the set of agents responding to a service request S
Output: Service providing agent q

```
for each x ∈ S do
        compute Trust(p, x)
        if Trust(p, x) > γ then
                G ← G ∪ {x}
        else
                U ← U ∪ {x}
        end if
end for
if G = ∅ then
        for each x ∈ G do
                compute load N(p, x)
        end for
        sort G in increasing order of load N
        return agent q with the smallest load N
else
        Total trust ← 0
        for each x ∈ U do
                Total trust ← Total trust + Trust(p, x)
        end for
        if Total trust > 0 then
                for each x ∈ U do
                        compute Prob(p, x)
                end for
                return agent q with probability Prob(p, q)
        else
                return any agent q randomly
        end if
        end if
```

IV. CONCLUSION

The thesis presented a novel trust computation model called Secured Trust for evaluating agents in multi-agent environments. Secured Trust can ensure secured communication among agent s by effectively detecting strategic behaviors of malicious agents. In this paper we have given a comprehensive mathematical definition of the different factors related to computing trust.

It also provide a model f or combining all these factors to evaluate trust and, finally it propose a heuristic load balancing algorithm for distributing work-load among service providers. Simulation results indicate, compared to other existing trust models

Secured Trust is more robust and effective against attacks from opportunistic malicious agents while being capable of balancing load among service providers.

V. FUTURE ENHANCEMENT

The new system become useful if the below enhancements are made in future. All the complications in this project can be easily solved. For further enhancing the project, the following enhancements were added in this project.

- The statistical analysis of code injection attacks data if prepared can be used for further project development.
- N number of software can be found out easily where the injections are found out.
- Once code affected part are send the mail to particular client that intruders came to affect the software.
- The multimedia files attacks can also be detected
- The efficiency of the project is further improved by improving coding efficiency
- In future, the time taken to complete the task is minimized
- Multitasking can also performed

The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

REFERENCES

[1] N. R. Jennings, "An agent-based approach for building complex software systems," Communications of the ACM, vol. 44, no. 4, pp. 35–41, 2001.

[2] M. Srivatsa, L. Xiong, and L. Liu, "TrustGuard: Countering vulnerabilities in reputation management for decentralized overlay networks," in Proceedings of the 14th ACM international conference on World Wide Web (WWW), 2005, pp. 422–431.

[3] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities [extended abstract]," in Proceedings of the 4th ACM conference on Electronic commerce(EC), 2003, pp. 228–229.

[4] T. D. Huynh, N. R. Shadbolt, and N. R. Jennings, "Developing an integrated trust and reputation model for open multi-agent systems," in Proceedings of the 7th International Workshop on Trust in Agent Societies, 2004, pp. 65–74.

[5] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation for e-businesses," in Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02), 2002, pp. 2431 – 2439.

[6] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: enabling scalable virtual organizations," International Journal of High Performance Computing Applications, vol. 15, no. 3, pp. 200–222, 2001.

[7] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in Proceedings of the 12th ACM international World Wide Web conference (WWW), 2003, pp. 640–651.

[8] L. Xiong and L. Li, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843–857, 2004.

[9] J. Sabater and C. Sierra, "Regret: A reputation model for gregarious societies," in Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies, 2001, pp. 61–69.

[10] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "An integrated trust
and reputation model for open multi-agent systems," Autonomous
Agents and Multi-Agent Systems, vol. 13, no. 2, pp. 119–154, 2006.

[11] Jennings, N.R. and Wooldridge, M., Eds. Agent Technology: Foundations, Applications and Markets. Springer Verlag, 1998.

[12] Brooks, F.P. The Mythical Man-Month. Addison Wesley, 1995.

[13] Jennings, N.R. and Wooldridge, M., Eds. Agent Technology: Foundations, Applications and Markets. Springer Verlag, 1998.

[14] Parunak, H.V.D. Industrial and practical applications of distributed AI. In G. Weiss, Ed., Multi-Agent Systems. MIT Press, 1999, 377-421.

[15] Simon, H.A. The Sciences of the Artificial. MIT Press, 1996.

[16] Foster, I. and Kesselman, C. (eds.). The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, 1999.

[17] Beiriger, J., Johnson, W., Bivens, H., Humphreys, S. and Rhea, R., Constructing the
ASCI Grid. In Proc. 9th IEEE Symposium on High Performance Distributed Computing,
2000, IEEE Press.

[18] Brunett, S., Czajkowski, K., Fitzgerald, S., Foster, I., Johnson, A., Kesselman, C., Leigh, J. and Tuecke, S., Application Experiences with the Globus Toolkit. In Proc. 7th IEEE Symp. on High Performance Distributed Computing, 1998, IEEE Press, 81-89.

[19] Johnston, W.E., Gannon, D. and Nitzberg, B., Grids as Production Computing Environments: The Engineering Aspects of NASA's Information Power Grid. In Proc. 8th IEEE Symposium on High Performance Distributed Computing, 1999, IEEE Press.

[20] Stevens, R., Woodward, P., DeFanti, T. and Catlett, C. From the I-WAY to the National Technology Grid. Communications of the ACM, 40(11):50-61. 1997.

[21] Sculley, A. and Woods, W. B2B Exchanges: The Killer Application in the Business-to-Business Internet Revolution. ISI Publications, 2000.

[22] Barry,J., Aparicio,M., Durniak, T.,Herman,P., Karuturi,J., Woods,C., Gilman,C., Ramnath, R. and Lam, H., NIIIP-SMART: An Investigation of Distributed Object Approaches to Support MES Development and Deployment in a Virtual Enterprise. In 2nd Intl Enterprise Distributed Computing Workshop, 1998, IEEE Press.

[23] Foster, I. Internet Computing and the Emerging Grid. Nature Web Matters, 2000.
http://www.nature.com/nature/webmatters/grid/grid.html.

[24] I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In ACM SIG-COMM, 2001.

[25] Gnutella. http://www.gnutella.com.

[26] J. E. Youll. Peer to peer transactions in agent-mediated electronic commerce. Master's thesis, Massachusetts Institute of Technology, 2001.

[27] S. Ba and P. A. Pavlou. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. MIS Quarterly, 26(3), 2002.

[28] S. Ketchpel and H. Garc´ ıa-Molina. Making trust explicit in distributed commerce transactions. In 16th International Conference on Distributed Computing Systems, 1996.

[29] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems. Communications of the ACM, 43(12), 2000.

[30] P. Resnick, N. Iacovou,M. Suchak, P. Bergstrom, and J. Riedl. GroupLens: An open architecture for collaborative filtering of netnews. In CSCW '94, 1994.