Pertanika J. Sci. & Technol. 21 (1): 183 - 192 (2013)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Issues on Trust Management in Wireless Environment

Abubakr Sirageldin*, Baharum Baharudin and Low Tang Jung

Computer and Information Science Department, University Technology Petronas, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia

ABSTRACT

Developing a trust management scheme in mobile computing environment is increasingly important, and the effective trust management model is a challenging task. Business, education, military, and entertainment have motivated the growth of ubiquitous and pervasive computing environments, which are always available due to the widespread of portable and embedded devices. Wireless and mobile computing are good example of ubiquitous and pervasive computing environments. Due to the uncertainty and mobility in such environments, the issue of trust has been regarded as an important security problem. Malicious nodes are a major threat to these networks; the trust system can monitor the behaviour of nodes and accordingly rewards well-behaved nodes and punishes misbehaving ones. At present, there are a lot of endeavours on the trust model of the pervasive computing environment. In this paper, a trust management framework for mobile computing is presented. The hybrid framework is based on a fusion of the support vector machine (SVM) and fuzzy logic system. From the results, it can be stated that the framework is effective, dynamic, lightweight, and applicable.

Keywords: Trust management, support vector machine, fuzzy logic, membership, interaction, pervasive, recommendation, central node, relationship

INTRODUCTION

Due to the rapid growth in network and communication technology, and the widespread of various types of computing devices, and the constant availability of services, security, confidentiality and the reliability are required in such an environment. Devices interact, collect and transfer information with simplicity, and minimal technical expertise without being previously introduced to each other. This necessitates a certain concept of security such as trust. In order to maintain a secure, dependable, and reliable environment, a smart security system without or with the least human participation is

Article history:
Received: 31 March 2012
Accepted: 31 August 2012

E-mail addresses:
abubakrsirag@gmail.com (Abubakr Sirageldin),
baharbh@petronas.com.my (Baharum Baharudin),
lowtanjung@petronas.com.my (Low Tang Jung)
*Corresponding Author

ISSN: 0128-7680 © 2013 Universiti Putra Malaysia Press.

needed. Therefore, both privacy and security challenges are confronting security professionals, because in such environments, a chance is available for bad intent entities to launch attacks to others easily (Mieso *et al.*, 2010). The traditional security models are based on the integration of, authentication, authorization, and access control to provide a secure environment. These traditional solutions can be useful in wired infrastructures. However, they are not efficient in pervasive and wireless infrastructures due to the dynamic topology of the wireless network that changes quickly, and the scalability of the wireless networks needs to be considered as well (Boukerche *et al*., 2008). Many studies have been conducted in this field. The previous works used different methods to achieve the objectives of the trust management system, and these can be briefly summarized as the trust models based on Bayesian approach and probabilistic theory (Almenarez *et al*., 2011), and trust models based on fuzzy logic (Wenshuan *et al*., 2007), trust model based on Dempster-Shafer and the theory of evidence (Zeng *et al*., 2010), and some approaches based on game theory. Despite these previous efforts, the optimum solution has not been reached. In this paper, a combination of two methods is proposed to recover the limitations of the existing ones. In particular, a trust management scheme is proposed by implementing a fusion of support vector machine (SVM) and fuzzy logic. The main motivation of the proposed scheme in using SVM is to predict the optimal relationship values for approximation purpose. Those approximated values will then relate the fuzzy basis functions for uncertainty resolving purpose, and the inference rules are invited for evaluating the trustworthiness of the devices.

The Previous Work

Trust in pervasive computing environments has obtained wide attention and become a challenge, with both wireless and mobile networks growing in a complex way. Many solutions have been proposed to solve the issue. Among other, Wenshuan *et al*. (2007) proposed a trust framework for pervasive computing using statistical distribution. The framework is composed of three models, namely, trust, security, and a risk model to resolve the uncertainty problem. Meanwhile, Boukerche *et al*. (2008) proposed a security system based on the trust management model using linear functions. The model assigns credentials to nodes, updates private keys, calculates trustworthiness for a node, as well as presents authority policy and access rights. Dong *et al*. (2010) presented a lightweight multilevel trust management framework based on the Bayesian formalization to produce trust assessments based on direct and recommended interaction. Mieso *et al*. (2010) investigated their previous probabilistic trust management scheme, and identified the possibility of a device to choose another for interaction by assessing its trustworthiness according to the current interaction and recommendations. Similarly, Shuai *et al*. (2010) proposed a dynamic trust model using the Dempster-Shafer for the set hypothesis on trust evaluation based on the accumulation of evidence. The model expresses the relationship between entities as direct, indirect, and integrated trust. Using their model, anonymous object can participate in the interaction with other trusted parties without any central security control.

Denko *et al*. (2008) proposed a model which utilizes probability distribution. The trust value is a probability of satisfactory interactions between any two neighbours. The distributed model uses filtering methods for recommendations. The weighting method is used for measuring the effect of time on the current behaviour of the devices. Wu (2011) proposed a Stable Group-based trust Management Scheme by considering geographic position, analysing the mobility patterns of nodes, and evaluating the trustworthiness without relying on any specific networking architecture. Meanwhile, Rhymend *et al*. (2010) proposed an approach that utilizes fuzzy logic for different trust characteristic's integration, whereby the trust values are calculated based on the interaction of the devices with the environment, and the model also uses a global data store point. Nonetheless, some drawbacks have been observed in the existing approaches; these include assuming transitivity of the trust, ignorance of the vagueness and uncertainty, and ignorance of the network traffic nature. Despite these previous efforts, an optimum solution has not been reached yet. In this work, a combination of two approaches is made using SVM to cope with network traffic nature and fuzzy logic as well as to cope with uncertainty problem. Accordingly, the model has shown the expected results.

Trust Concept

Trust concept occurs in many fields. The meaning of trust is tailored to its specific use in a particular application domain (Walt Yao, 2004). In computing, trust is an essential foundation for information security, where the security is concerned with the correct operations of software and hardware. The challenge of exploiting trust in computing lies in extending the use of trust based solutions. First to artificial entities such as software agents or subsystems, then to the human user's subconscious choice (Punam *et al*., 2008). In Social, trust is often used by people in a very broad sense. Its interpretation depends on many issues such as past experiences, associated risks, recommendations from other parties, the reputation of the trusted parties, or even cultural background (Walt Yao, 2004). The basis of this form of trust lies in familiarity, bonds of friendship and common faith and values. In networks, the relationships among participating entities are extremely needed for reliability and security of the collaborative environment. In this context, trust is defined as a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities Jin-Hee *et al*. (2011). Based on the above discussions, some sources that assist the establishment of trust are discussed.

Experience: The past record provides a good indication of future interactions. Depending on the knowledge recorded from the previous interactions, the degree of trust may either increase or decrease. Experiences can involve some trusted parties, and they may be as useful in recommendations.

Recommendation: It is a third party evaluation, and it depends on its source. In real life, a recommendation is employed to assist decision-making in daily situations. It helps decision makers by providing evaluations from others.

Reputation: is another popular mechanism that people employ to deal with unfamiliar parties. Similar to the recommendation, it does not require any prior experience with the party for a reputation to be used to infer trustworthiness (Walt Yao , 2004). Some previous research mentioned some features of trust such as exist on uncertain and risky environment, context dependent, requires previous knowledge and experience, quantitative, based on reputation and opinion, subjective, not necessarily transitive, asymmetric, and dynamic.

THE APPROACH AND METHODS

In our approach, a centralized environment is considered. Each centre operates autonomously and collaborates with another centre, and takes the responsibility of disconnecting or establishing a connection, and evaluates the trustworthiness of each node. We have two types of trust, namely, direct trust (the history of interactions in the environment as motivated by Sanjeev *et al*., 2010) and others) and indirect trust (or recommendations, as motivated by Zhong *et al*. (2010), Trcek (2011) and others. In order to understand the model architecture in a simple way, let us consider the relationship between two nodes, namely, A and B. The trust of A to B is $V_{A,\,B}$ and the trust of B to A is $V_{B,\,A,}$ as shown in Fig.1. If *A* sends to *B*, and *B* sends to *A*, then the relationship is established, and values initiated. Each node has (*N-1*) relationships with the others. The total number of the relationships in the network is *N**(*N-1*) relationship.

Direct Trust Computation

The previous interactions are taken under consideration in the context, such as the history of interactions H_{AB} between *A* and *B* is computed numerically in the range [0, 1], based on satisfactory/ unsatisfactory interactions, and good/bad packets sent. Let *Ps* be the number of good packets, *Pu* is number of bad packets, *S* is the number of satisfactory interactions, and *U* is the number of satisfactory interactions, while *S* and *U* are calculated as:

$$S = \frac{P_s}{P_s + P_u} \tag{1}$$

The history of interaction value, H, is:

$$H = \frac{\text{number of Satisfactory Interactions}}{\text{Total Number of Interactions}} \tag{2}$$

For each node, the average of interactions {*H1, H2, H3…Hm*} with another node where *m* is the number of previous interactions that is computed as:

$$H_{average} = \sum\nolimits_{i=1}^{m} H_i \tag{3}$$

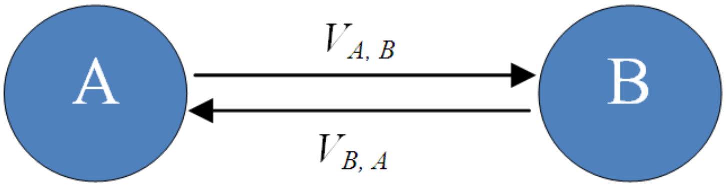

Fig.1: The simple trust relation between nodes

The average value then forms the relationship value. In a network of *N* nodes, each node has (*N-1*) relationships, the total number of relationships in the network is *N**(*N-1*). Now, these relationships are forming an *NxN* matrix of real number. The rows are the values given to other nodes in the environment by node *i*, and the columns are the values given to node *i* by others. Where H_{ij} denotes the history of interaction value for node *i* to node *j*, and the diagonal of the matrix H_{ii} is the accumulated interaction values for the node, *i*.

Indirect Trust Computation

In fact, the recommendation is the history of interaction of a node in other environments. In this study, the average value of recommendations is used. Let $R= \{R_1, R_2, R_3 ... R_k\}$ be the set of K's centre recommendations, then:

$$R_{average} = \frac{\sum_{i=1}^{k} R_i}{k} \tag{4}$$

The average recommendation is the accumulated relationship value from outside the environment.

The Hybrid Computation

The previously mentioned matrix, which constructed by *N**(*N-1*) relationships, is now the kernel trick matrix. The matrix is fed into the support vector machine for prediction purpose based on the relationship values. A suitable kernel trick function such as k(x,y)=(<Φ(x),Φ(y)>) is used.

Where the input data are the relationship values forming the kernel matrix. The SVM technique approximates the total value for each node according to the relationship values in the kernel matrix. The expensive calculations can be reduced by using a suitable kernel trick decision formula.

$$f(x) = \operatorname{sgn}\left[\sum_{i=1}^{n} y_i \alpha_i . k(x, y)\right] \tag{5}$$

The output results in a vector of N elements describe the predicted value for each node, and this vector contains values range in an interval [0 1]. These values imply fuzziness and uncertainty expression for evaluating trustworthiness of a node. Among the various fuzzy logic (MFs), the simple trapezoid MF is used to reduce execution overhead in order to make a lightweight model. The fuzzy sets designed for this model are VU, UT, TW, and VW, which represent Very Untrustworthy, Untrustworthy, Trustworthy, and Very Trustworthy, respectively. Therefore, there are a total of four MFs, as shown in Fig.2.

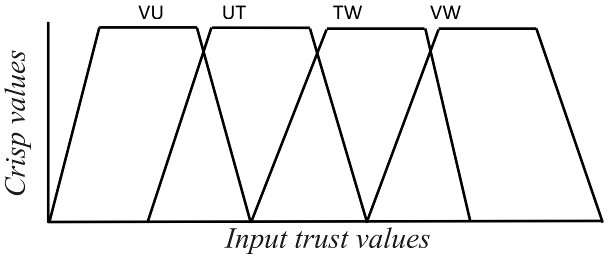

Fig.2: Trapezoid Fuzzy set membership functions

The trapezoid MF is described by four numerical parameters (a, b, c, and d), with d-c shoulder which is expressed by the following formula:

$$f(x,a,b,c,d) = \max\left\{\min\left(\frac{f(x)-a}{b-a},1,\frac{d-f(x)}{d-c}\right),0\right\} \tag{6}$$

The MF expression generates two crisp values in different MFs. The first value denoted as lower bound MF and the second denoted as upper bound MF. If the upper bound MF value is greater than the threshold value, the decision will then be upper bound MF, or else, the decision is the lower bound MF. The inference rules are playing a role in the final decision manifesto.

Performance Evaluation

In this section, the performance of the hybrid scheme SVM-Fuzzy is tested. In particular, the dynamic characteristic of the model is examined, while the values are collected perfectly. The data type is a real number, and the values are in a range [0 1]. Any connection request managed by the centre and all well-trusted nodes participate in the interaction without any obvious involvement of the centre. The completely new node implies constructing a new record on the environment, so the new identified node is verified by retrieving its record as recommendations from the other centres. In fact, the recommendation is the past interaction history of the new node in these environments. The centre will then validate the retrieved data for the purpose of establishing a connection with another node. The established connection is confirmed by that destination node. The values are dynamic and updated each time the record is altered.

Parameter Setup: In the experimental zone, three parameters are used, namely, the relationship values, the recommended values, and the number of nodes in the network.

Performance Metrics: The model used five metrics. The average relationship value *H* represents the statistical mean of relationship values, and the predicted value *f(x)* of kernel trick. The crisp value represents the trapezoid MF expression *f(a,b,c,d)*, average recommendations, *R*, and the threshold value, *T*.

The Results of the Experiments

The effective of SVM: the model is tested offline, and due to this circumstance, the data are arbitrary initiated in a range between 0 and 1. The number of nodes and the values of α are varied in order to study the performance of SVM.

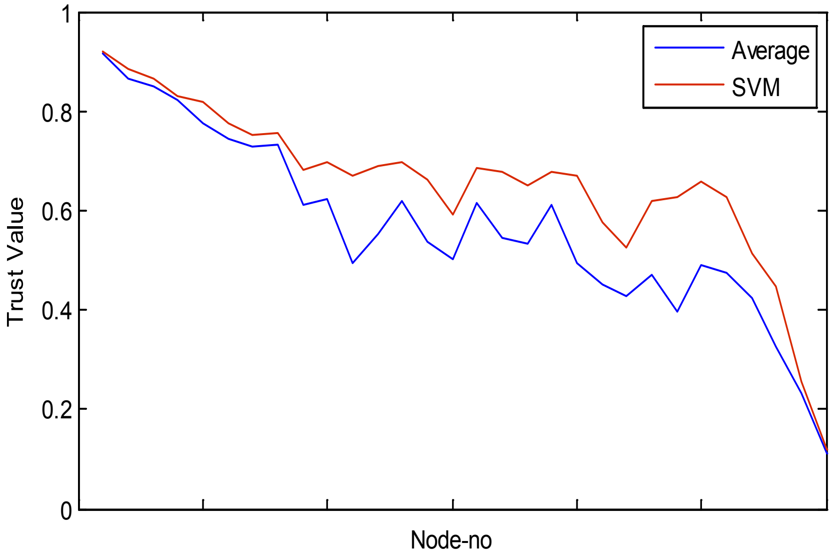

Fig.3: The performance of SVM against basic Statistics (average)

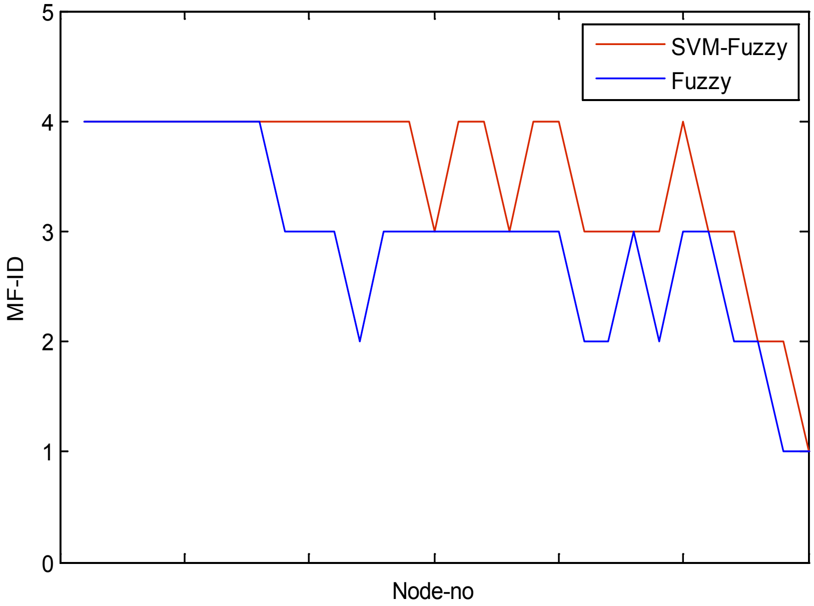

Fig.4: Comparison of SVM-Fuzzy against Fuzzy, the vertical axis 1, 2, 3, 4 represent the four MFs VU, UT, TW, VW, respectively.

The significance of threshold value: In this experiment, the effectiveness of the fuzzy logic performance under different threshold values is argued.

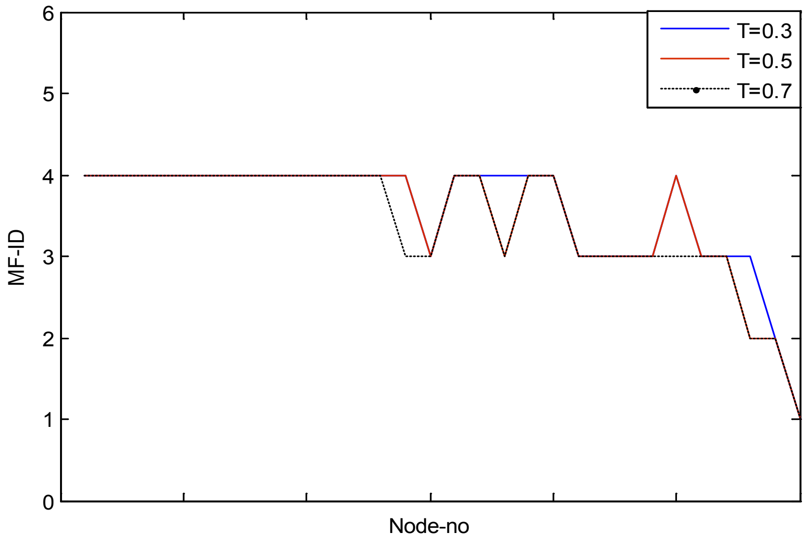

Fig.5: Fuzzy logic Performance

RESULTS AND DISCUSSION

The experiment went as expected without unusual input data that would have introduced errors. The input data were the real values in a range between 0 and 1. The type of the statistical method used has enforced the interaction observations to be in the above-mentioned range. Carefully, the SVM parameters were initialized, and the Gaussian function which led to the predicted values was used to avoid the the execution overhead of the kernel trick. Only one α was assumed for each data-range in the kernel matrix and the graph depicted in Fig.4 reveals the differences. Fig.3 shows the the performance of SVM and the modified values. This modification is almost under the general rules of the trust management policy. The adjustment was done to enhance the average calculation of the interaction history with a single node. In this study, an acceptable rate was chosen due to the relationship values. The result shows a good performance of SVM compared to the statistical average. As a part of this experiment, the predicted values were the input of the fuzzy expression, and the crisp values were accordingly calculated for each node. In this calculation, the values were assumed to be couple according to the trapezoid MF expression. The inference rules were applied to the couple under a predefined threshold value. The comparison between SVM-Fuzzy and Fuzzy (see Fig.5) is exactly different. In Fig.4, the vertical axes 1, 2, 3, 4 represent the four MFs VU, UT, TW, and VW, respectively. The results of the combined SVM-Fuzzy have been studied by comparing them with the performance of the Fuzzy logic alone under a threshold value T=0.5 before the optimization process.

The threshold value is an administrative issue, and it should have been specified previously due to the policy. Fig.5 shows the results of different threshold values (T=0.3, T=0.5, T=0.7). Note that the threshold value is defined according to the trust policy in the entire network. Errors may arise when the relationship values are out of the range, and this indicates that the optimized value may not be precise for the entire range.

Contributions

The main contribution of the current work is the possibility of the use of automated hybrid SVM-fuzzy for trust management. In addition, the framework shows some advantages such as follows: first, it does not conflict with any security infrastructure in the environment; second, it is dynamic as the trust changes according to the activities of the node; third, it is protected against false recommendation that can be given by human; and finally, it lets the autonomous entities interact freely without security management overhead.

CONCLUSION AND RECOMMENDATIONS FOR FUTURE WORK

The issue of trust is really a challenge in ubiquitous and pervasive computing environments, especially for wireless and mobile networks. In this paper, the concept of trust has been presented and the basic of a controlled environment has also been explained. The framework is based on simple statistical methods which are used in interaction computation. Hence, a framework that integrates both the SVM and fuzzy system is proposed. Other than the trust frameworks, the importance of the central point, which is responsible of the trust calculation and evaluation process, have also been taken into consideration. In order to obtain a reliable recommendation, the central point request policy has been adopted. In addition, the framework has the capability of: (1) avoiding conflict with any security infrastructure in the environment, (2) dealing with the dynamic nature of trust, (3) giving protection against the false recommendation, and (4) avoiding security management overhead. A possible future work is the direction towards multidisciplinary approaches due to the complexities in the environments.

REFERENCES

Almenárez, F., Marín, A., Díaz, D., Cortés, A., Campo, C., & García-Rubio, C. (2011). Trust management for multimedia P2P applications in autonomic networking. *Ad Hoc Networks, 9*(4), 687-697.

Bedi, P., & Gaur, V. (2008). Trust based prioritization of quality attributes. *International Arab Journal of Information Technology*, *5*(3), 223-229.

Boukerche, A., & Ren, Y. (2008). A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications, 31*(18), 4343-4351.

Denko, M. K., Sun, T., & Woungang, I. (2011). Trust management in ubiquitous computing: A Bayesian approach. *Computer Communications, 34*(3), 398-406.

Deno, M. K., & Tao, S. (2008, 17-20 Dec. 2008). *Probabilistic Trust Management in Pervasive Computing*. Paper presented at the Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference.

Jin-Hee, C., Swami, A., & Ing-Ray, C. (2011). A Survey on Trust Management for Mobile Ad Hoc Networks. *Communications Surveys & Tutorials, IEEE, 13*(4), 562-583.

Rhymend Uthariaraj, V., Valarmathi, J., Arjun Kumar, G., Subramanian, P., & Karthick, R. (2010). A Novel Trust Management Scheme Using Fuzzy Logic for a Pervasive Environment. In N. Meghanathan, S. Boumerdassi, N. Chaki & D. Nagamalai (Eds.), *Recent Trends in Networks and Communications* (Vol. 90, pp. 144-152): Springer Berlin Heidelberg.

Sharma, S., Mishra, R., & Kaur, I. (2010, 9-11 July 2010). *New trust based security approach for ad-hoc networks.* Paper presented at the Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference.

Trcek, D. (2011). Trust Management in the Pervasive Computing Era. *Security & Privacy, IEEE, 9*(4), 52-55.

Wenshuan, X., Yunwei, X., & Guizhang, L. (2007, 21-25 Sept. 2007). *A Trust Framework for Pervasive Computing Environments.* Paper presented at the Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007.

Wu, X. (2011). A Stable Group–based Trust Management Scheme for Mobile P2P Networks. *International Journal of Digital Content Technology and Its Applications*, *5*(2), February.

Yao, W. (2004). *Trust management for widely distributed systems*. Technical report, UCAM-CL-TR-608. Retrieved from http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-608.pdf

Zeng, S., Xu, F., Xin, Y., Yand, Y-X., & Hu, Z-M. (2010). Trust Model based on Dynamic Policy Similarity for pervasive Computing Environments. *IEEE,* 978-1-4244-6349.

Zhong, D., Zhu, Y., Lei, W., Gu, J., & Wang Y. (2010). Multilevel Trust Management Framework for Pervasive Computing. *Third International Conference on Knowledge Discovery and Data Mining*. *IEEE*, 978-0-7695-3923.