Scoring Mechanism for Mobile Networking Issues on Trust Management

A. Abubakr Sirageldin, B. Baharum Bahruddin, C. Low Tang

Computer and Information System Department, University Technology Pertronas

abubakrsirag@gmail.com, {baharbh, lowtanjung}@petronas.com.my

Abstract— nowadays, a number of wireless users, network technologies and applications are in growth. This phenomenon brought up abundant with services to the human everyday tasks and activities, with simplicity, and minimal technical expertise. The great move from virtual to augmented reality changes people's life, and makes daily activity seamless without burden. In such an environment, the possibility of collecting information invisibly without user's intention is very high. The nature of the interaction between users necessitates a trust concept, which required integration of different concepts to evaluate precisely the trustworthiness of each user. This work provides a scoring mechanism that gives the user a degree by implementing a fusion of support vector machine and fuzzy logic to calculate efficiently the trust score, and resolved the uncertainty in the decision.

Keyword: Central node, Fuzzy Logic, Interaction, Membership, Matrix, node, Support Vector Machine, Pervasive, Trust management, Trustworthiness, Recommendation, Relationship

1 INTRODUCTION

In mobile networking, users have the access to the network anytime anywhere, the applications and the services are available in different locations. This phenomenon brought up abundant with services to the human everyday tasks and activities with simplicity, and minimal technical expertise. In contrast, a rapid growth in threads and vulnerabilities is observed and announced. The devices are interconnected and embedded in physical objects to collect process, and transfer information with the least human participation [1]. The characteristic of this environment is the interaction between devices. These devices are engaging in the interaction without prior knowledge of each other and meanwhile need to distinguish each other. This circumstance establishes a congenial environment for users with malicious intent to launch attacks and bad activities. The traditional security models combined authentication, authorization, and access control. These solutions are adequate in wired networks, but they are not sufficient for ubiquitous and pervasive wireless networks because of the dynamic topologies and features of wireless networks [3]. This environment is integrating computing and communication systems, but this vision cannot be fully utilized without addressing privacy and security relevant issues [4]. Therefore, it's important to develop a reliable and sufficient trust management mechanism to mitigate some risks. Such mechanisms supposed to be dynamic and operate without or with at least a little human intervention. The goal of trust management is to assess the activities of nodes, and build a reputation for each node based on the node evaluation of the trustworthiness. The reputation can then be used to determine the trustworthiness for other nodes [12]. Trust is not confused with reputation, which partly affects the trust. Trust should be multidisciplinary; this primarily means including computing and information science on one hand, and psychology as a social context on the other [2]. This paper provides a trust management scheme by implementing the fusion of support vector machine and fuzzy logic; the use of SVM is to calculate the trust score of a node and the use of fuzzy logic for resolving uncertainty and evaluate the trustworthiness of nodes.

2 Previous work

Several methods have been developed to add some values to the field security in multiple mobile computing environments (Pervasive computing). These methods are aimed to evaluate the level of trust between devices, while providing a way to manage the relationships between devices. The mechanism that deals with the evaluation, collection, and propagation of trust is referred to as trust management [4]. This issue has been investigated by many researchers. The earliest concept of trust is presented for the application of Internet security, such as E-commerce and Multi-Agent Systems [3]. Authors in [5] have proposed a distributed trust framework that evolves the trust based on Bayesian formalization, the model is lightweight and protects user anonymity. In [3] a security system is proposed based on a trust management model, which assigns credentials to nodes, updates private keys, manage the trust value of each node, and making appropriate decisions about node's access rights. In [1] they reviewed previous trust and privacy models in pervasive systems and analyze them for importance of trusted computing platforms in tackling their weaknesses. In [4] they have investigated their previous probabilistic trust management scheme, and argued the possibility of a device to choose other appropriate devices to interact, while identifying other as malicious. The scheme allows a device to judge the trustworthiness of another device of current interaction, allows a device to make a better use of recommendations. In [6] they proposed a security policy that assigning credentials to users, verifying the cre-

dential's satisfaction, incorporating the third parties, and reasoning the access rights. In [8] authors introduced a framework consists of three components, social networks, translations, and trust mechanism; the model utilized data sets of social connectivity information to bootstrap trust algorithms. In [12] the researcher described an automated trust management scheme for MANETs using support vector machine to classify nodes as malicious in terms of altering their misbehavior patterns, motion speed and transmission range. In [13] the author surveyed existing trust models in multi-agent systems, mobile ad-hoc networks and VANETs, and their key issues, and then suggested desired properties towards effective trust management. In [14] the author proposed a novel Stable Group-based Trust Management Scheme. Considering mobile geographically position and analyzed the mobility patterns of nodes, then compute trust relationships without relying on fixed networking structure. In [15] they proposed comprehensive approach incorporating fuzzy logic for integrating various trust characteristics. The trust values are stored in a global data store. The previous endeavors in this field developed various methodologies that can be classified into three groups in terms of computer and information sciences area. The first group is based on elementary Bayesian statistics, using Bayesian rules for conditional probabilities. The second group of approaches extends elementary Bayesian statistics, which is the case with Dempster-Shafer Theory of evidence that enables treatment of uncertainties. The third group is based on game theory. This theory models strategic situations where individual's rational choices depend on the rational choices of other players. The main problem with all above methodologies is, first, assume rational players. Second, assume knowledge with quite sophisticated mathematics. Third, they assume transitivity of trust relationships [7].

3 TRUST RELATIONSHIPS AND PROPERTIES

The trust occurs in many branches. The meaning of trust is tailored to its specific use in a particular application domain [11]. In computing trust is essential foundation for information security. Where, the security concerns about 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 [12]. In Social, trust is often used by people in a very broad sense. Its interpretation depends on past experiences, associated risks, recommendations from other parties, reputation of the trusted parties, or even cultural background [11]. 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 [13]. According to above discussions, we argue some sources that assist the establishment of trust.

Experience: The past record provides a good indication of future interactions. Depending on the knowledge recorded from 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's a third party evaluation, and it depends on its source. In real life, recommendation is employed to assist decision-making in daily activities. It helps decision makers by providing evaluations from others.

Reputation: Reputation is another popular mechanism that people employ to deal with unfamiliar parties. Similar to recommendation, it does not require any prior experience with the party for reputation to be used to infer trustworthiness [11]. Some previous research mentioned some features affect trust calculation such as: exist on uncertain and risky environment, context dependent, require previous knowledge and experience, quantitative, based on reputation and opinion, subjective, not necessarily transitive, a symmetric, and dynamic. The present paper considers some properties that have some significance in trust computation:

Required previous knowledge: the most effective factors without information it's very hard to bootstrap trust, and the evaluation process may be unfair.

Uncertain: Trust is a subjective notion based on the concepts of evidence and opinion to measure trustworthiness.

Quantitative: the representation of trust should be in a way that can enable calculation and evaluating operations.

Dynamic: behavior changing cause trust value changing. What is done today may be different than what have been done yesterday, the present activity affects the trust computation, and the trust value updated accordingly.

Trust greatly enhances the security performance over all networks, and reliable for peer-to-peer interactions and conversations. Let us consider the relationship between two nodes A and B, the trust of A to B is $T_{A,B}$ and the trust of B to A is $T_{B,A}$. If A send a packet to B, then A is believe in B behavior which increases the trust value TA,B of B and vice versa; otherwise, if A behaves badly in the interaction with its peer, then A is a suspicious node that will cause penalty and its trust value decreases accordingly.

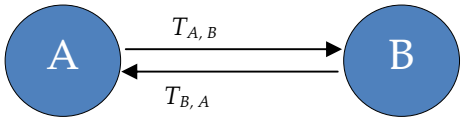

Fig 1: A simple relationships between nodes

4 The Trust Model

Our approach uses a centralized environment. Each environment has a center that operates autonomously and collaborates with other centers. The center also takes responsibility of disconnecting/establishing the connection, and evaluates the trustworthiness of each node. The model uses two sources of trust, history of interactions in the environment as motivated in [1], [6], [7], [9], [14], [15], and recommendations from other environments as motivated in [4], [5], [6], [10], [11]. The history of interaction is used to compute the trust score when a node has more conversation and interaction experience with others and became well-known in the environment, therefore, the trust score will be increased. The recommendation is used when a node completely new to the environment. The central point manages the trust scores generated according to the interaction, evaluate each node individually and prepare the trust score matrix. If a node is completely new to the environment and send a connection request to specific node, the central node act on be-half and search for information related to the quest in the other environments. A node would be trustworthy, secure, or reliable in any interaction according to the overall trust score calculated by the central point.

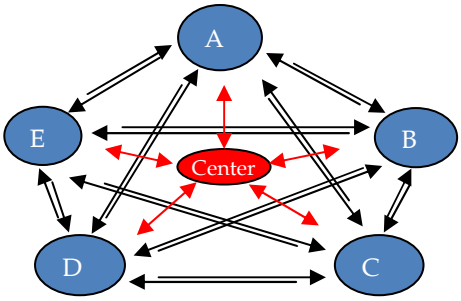

Fig 2: The complexity of the relations in the environment

History of interaction: the experience of previous interaction between nodes is taken under consideration. *A* double linked list relationship data structure that constructs the history of interaction among nodes. The history of interaction H_{AB} between *A* and *B* is computed based on satisfactory / unsatisfactory interactions, and good/bad packet sent. Let *Ps* be the number of good packet, *Pu* the number of bad packet, S the number of satisfactory interactions, and *U* the number of satisfactory interactions, and then *S* and *U* calculated as:

$$S = \frac{P_s}{P_s + P_u} \quad , \quad and \quad U = \frac{P_u}{P_u + P_s} \qquad (1)$$

The history of interaction value *H* is

$$H = \frac{Number\ of\ satisfactory\ interactions}{Total\ number\ of\ interactions}$$

For each node, the average of interactions with another node $\{H_1, H_2, H_{3...}H_m\}$, (*where m is the number of previous interactions*) is computed as:

$$H_{avg} = \frac{\sum_{i=1}^{m} H_i}{m} \qquad (2)$$

The average value then forms the relationship score. In the 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 a *NxN* matrix of real numbers. The rows are the scores that given to others by node *i*, and the columns are the values given to node *i* by others, and the diagonal of the matrix *Hii* is accumulated scores for the node *i*.

$$h_{ii} = \sum_{t=1}^{n} h_{ji} \quad For\ all\ h_{ji} \quad where \quad j \neq i$$

Recommendation: due to the highl mobility of nodes, the environment expects different individual objects, some of them have a history record and some of them are absolutely new comers in the specific environment. In this case, the central node search for information related to the new one (recommendations), from other central points. In fact, the recommendation is the history of interaction of a node in other environments. We use the average value of recommendations. Let $R = \{R_1, R_2, R_3 \ldots R_k\}$ be the set of K's center recommendations, then:

$$R_{average} = \frac{\sum_{i=1}^{k} R_i}{k} \qquad (4)$$

5 Trust computation

Trust is collected from the *N*(N-1)* relationships for each node in the network, where *N* is the number of nodes in the environment, so a matrix of *N x N* is generated. The model uses a kernel function formula (SVM) to predict the trust scores of nodes. However, the kernel trick decision formula is not accurate, but it still shows better result comparing with other statistical methods. For each node the column of the matrix is the scores that have been given by the community members according to the past the interaction. Then the matrix is fed into the SVM classifier to produce the predicted scores. The expensive calculations can be reduced by using a suitable kernel trick function as:

$$K(x,y) = \langle \varphi(x), \varphi(y) \rangle \qquad (5)$$

The above is the general kernel trick function leads to the decision function:

$$f(x) = \operatorname{sgn}\left[\sum_{i=1}^{n} y_i \alpha_i k(x, y)\right] \qquad (6)$$

Fuzzy logic has rapidly become one of the most successful in today's technologies for developing. It addresses such applications perfectly as it resembles human decision-making with an ability to generate precise solutions from certain or uncertain information. This model used

the simple trapezoid member ship function.

$$f(x,a,b,c,d) = \max\left\{\min\left(\frac{x-a}{b-a},1,\frac{d-x}{d-c}\right),0\right\} \quad (7)$$

The fuzzy sets (linguistic variables) are defined as VU, UT, TW, and VW, which represent Very Untrustworthy, Untrustworthy, Trustworthy, and Very Trustworthy respectively, thus there are four membership functions used to evaluate the trustworthiness of a node in this scheme. The crisp values are calculated as:

$$C_i = \begin{cases} 1 \\ 0 \end{cases} \quad \textit{Where } i\textit{=1 to number of functions}$$

We use the wide shoulder trapezoid to resort the crisp values. The Final decision is made according to the if-then rules applied to C_i to select the appropriate fuzzy class according to the network policy.

6 PERFORMANCE EVALUATION

In this section, we test the performance of the hybrid scheme SVM-Fuzzy. We ran the model several times with different vectors of . In the experimental zone there are five different network sizes. The data type is real number range between [0 1]. Any connection request managed by the center, and all well trusted nodes to participate in interaction without obviously involvement of the center. The completely new node implies constructing a new record in the environment, so the new identified node is verified by retrieving its record as recommendations from other centers. In fact, the recommendation is the past interaction history of the new node in these environments. The center then validates the retrieved data for establishing connection with another node. The established connection is confirmed by that destination node. The values are dynamic and updated each time that the record is altered.

Parameter Setup: In our experimental zone, we used three parameters, the relationships values, a vector of as the optimization parameter for SVM, and the number of nodes in the network.

Performance Metrics: We used three performance metrics. The average relationship value represents the statistical mean of relationship's values, the predicted value of the kernel trick. The crisp value represents the trapezoid MF expression, and the threshold value *T*.

7 EXPERIMENT RESULTS

According to the uncertainty of the trust in the environment, trust score is hardly computed. The data is arbitrary prepared for the different environments each of which has a different number of nodes 10, 20, 30, 50, 100, to test the efficiency.

Table I: shows the optimized trust scores

Node ID	Stat	SVM	Node ID	Stat	SVM
1	0.325	0.410	57	0.604	0.771
2	0.342	0.451	58	0.747	0.821
3	0.329	0.419	…	…	…
4	0.273	0.321	66	0.833	0.863
5	0.432	0.521	67	0.309	0.372
…	…	…	68	0.324	0.401
15	0.582	0.653	…	…	…
16	0.129	0.132	78	0.704	0.778
17	0.629	0.711	79	0.312	0.380
18	0.607	0.671	80	0.597	0.675
…	…	…	87	0.426	0.519
28	0.288	0.364	88	0.419	0.503
29	0.769	0.811	…	…	…
30	0.347	0.461	96	0.431	0.528
40	0.138	0.152	97	0.366	0.420
…	…	…	98	0.762	0.801
55	0.819	0.845	99	0.693	0.760
56	0.324	0.401	100	0.826	0.883

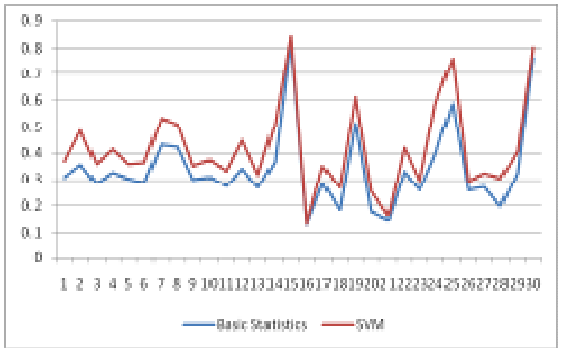

Fig 3: Shows performance of SVM

The performance of trapezoid MF: in this experiment, we argue the effective of fuzzy logic performance under different fuzzy sets obtaining crisp values.

Table II: shows samples fuzzification of trust values and crisp values associated accordingly

Values	C_1	C_2	C_3	C_4
0.544683	0.00000	0.553172	1.00000	0.00000
0.383802	0.161976	1.00000	0.00000	0.00000
0.611474	0.00000	0.00000	1.00000	0.114743
0.314883	0.85117	1.00000	0.00000	0.00000
0.845649	0.00000	0.00000	0.00000	1.00000
0.269443	1.00000	0.694426	0.00000	0.00000
0.761952	0.00000	0.00000	0.380485	1.00000
0.479433	0.00000	1.00000	0.794328	0.00000

0.135476	1.00000	0.00000	0.00000	0.00000
0.801526	0.00000	0.00000	0.00000	1.00000

The performance of trapezoid MF: in this experiment, we argue the effective of fuzzy logic performance under different fuzzy sets obtaining crisp values.

8 Results and Discussion

The experiment went as expected without unusual input data that would have introduced errors. The input data were real values in a range between 0 and 1. The type of the statistical method has been used enforcing the interaction observations to be in the above-mentioned range. Carefully, we have initialized suitable vectors of the optimization parameter for SVM acceptable optimization rate. Those values which approach to 0 or 1 have been given attention. To avoid the expensive of calculations the kernel trick has been used, the kernel function then led to the predicted values. Only one assumed for each data-range in the kernel matrix and the graph in (Fig 3) reveals the differences.

Table I. It shows the optimization rate caused by vector. This modification is almost under the general rules of the trust management policy. The adjustment was done for enhancing the average calculation of interaction history with a single node. We have chosen an acceptable rate due to relationship values. The result shows good performance of SVM comparing 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 calculated for each node accordingly. 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 errors might arise from, the relationship values out of range, this causes that the optimized value might not be precise for the entire range, and unsuitable value that might cause unsatisfied optimization rate.

9 Conclusion

Trust gained high attention, become a challenge, and required to be studied deeply. The possibility of using the hybrid support vector machine and fuzzy logic in trust management for a pervasive environment is approved in this paper. The central node of the environment seamlessly establish the connection for a node according to the overall calculated trust score. The trust score associated to the node is according to the previous interaction record with environment members, the overall trust score is computed dynamically by the central node. This approach can effectively compute the trust value and asses the trustworthiness of a node. In the future trust will be the area of multidiscipline research, its complexity involve various heuristics methods to obtain efficacy and reliability. In addition, simulations will continue as methodology. But, researchers should be aware of standards in this area and recognize its features and factors.

References

[1] Hamed Khiabani, Jamalul-Lail Ab Manan, Zailani Mohamed Sidek, "A Study of Trust & Privacy Models in Pervasive Computting," *University Technology Malaysia* (2009).

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

[3] Azzedine Boukerche, Yonglin Ren.: A trust-based security system for ubiquitous and pervasive computing environments, Computer Communications 31(18): 4343-4351 (2008).

[4] Mieso K. Denko, Tao Sun, Isaac Woungang, "Trust management in ubiquitous computing- A Bayesian approach," *Computer Communications* 34(3): 398-406 (2011).

[5] Daniele Quercia, Stephen Hailes, Licia Capra.: B-trust: Bayesian Trust Framework for Pervasive Computing, University College London, London, WC1E 6BT, UK (2007).

[6] Lalana Kagal, Tim Finin, Anupam Joshi,"Trust-Based Security in Pervasive Computing Environments," *University of Maryland, Baltimore County, Computer 34(12):* 154-157 (2001).

[7] Denis Treck,"Trust Management from Pervasive Computing Environments to Mathematical Economy and Sociology," *Recent Researches in Telecommunications, Informatics, Electronics and Signal Processing*, ISBN:978-1-61804-005-3(2011).

[8] Brent Lagesse, Mohan Kumar, Svetha Venkatesh, Mihai Lazarescu,"Augmenting Trust Establishment in Dynamic Systems with Social Networks," *ACM* (2010)

[9] Florina Almenarez, Andres Marin, Daniel Diaz, Alberto Cortes, Celeste Campo, Carlos Garcia-Rubio," Trust management for multimedia P2P applications in autonomic networking," 1570-8705, *Elsevier* (2011).

[10] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan,"Trust and Trust Management in Cloud Computing – A Survey," February (2011).

[11] Sanjeev Sharma, Renu Mishra, Inderpreet Kaur,"New trust based security approach for ad-hoc networks," 978-1-4244-5540 , *IEEE* (2010).

[12] Wenjia Li, Anupam Joshi, Tim Finin,"SVM-based Automated Trust Management System for Mobile Ad-hoc Networks," FA9550-08-1- 0265 *Air Force Office of Scientists Research* (2011)

[13] Jie Zhang,"A Survey on Trust Management for VANETs," *International Conference on Advanced Information Networking and Applications*, 1550-445X, IEEE (2011).

[14] Xu Wu,"A Stable Group–based Trust Management Scheme for Mobile P2P Networks," *International Journal of Digital Content Technology and its Applications*, Volume 5 Number 2, February (2011).

[15] V. Rhymend Uthariaraj, J. Valarmathi, G. Arjun Kumar, Praveen Subramanian, R. Karthick,"A Novel Trust Management Scheme Using Fuzzy Logic for a Pervasive Environment," *Recent Trends in Networks and Communications* 90: 144-152 (2010).