EasyChair Preprint

№ 4080

# A Trust Computing Model for Future Generation Networks

Prodipto Das and Somen Debnath



August 25, 2020

# A Trust Computing Model for Future Generation Networks

Prodipto Das[1]
*Department of Computer Science*
*Assam University, Silchar*
Assam, INDIA
prodiptodas@gmail.com

Somen Debnath[2, *]
*Department of Information Technology*
*Mizoram University, Aizawl*
Mizoram, INDIA
somen.nit@gmail.com

***Abstract*—Future generation networks are heterogenous in nature due to variety of nodes, terminals, small-sized networks, private networks, virtual networks, IoTs etc. When number of nodes and terminal machines take part in a network, authentication become a major issue. Authentication of node is associated with trust. Trust of a node is a primary behaviour of the node in the network operations. Networks with fewer restrictions in case of user registration may have more trust related issues. A node may exhibit random behaviour at the time of data transmission and forwarding of packets. The major concern is about the assessment of trust value of a node before actual data communication. Trust computing model is the model which gives trust values of nodes in a network. Different trust computing models are designed and developed for different scenarios. In this paper, a model of trust computing is proposed with maximum possible factors. A simulation program in NS3 is written and executed to check the trust values and its effect in the network operations. The results are analysed with and without risk factors to check the accuracy of network performances. It is observed in the experimental work that trust with risk factors is more authenticated solution for the proposed trust model.**

***Index Terms*—trust, trust computing model, future generation networks**

## I. Introduction

Trust [1] is defined as estimated subjective probability that an entity exhibits reliable behaviour for particular operation(s) under a situation with potential risks. Trust is an important and complex issue in social aspect. Trust may be stated as psychological cognitive process which may consists of expectations, assumptions, belief, behaviour, environment and other factors. Generally trust in humane is used to perform certain actions between two individuals.

Trust in computer network is an expectation of one node to other. Trust is a relationship between two neighbouring nodes based on some criteria and conditions. Trust is context dependent, hence can be defined in many ways. Trust increases confidence of the node before communication. Trust may be defined as quantified belief by a node to other node in terms of honesty, security, competency etc. In networks like MANET, VANET etc. where centralised infrastructure is not available, nodes communicate with each other with cooperative nature and exchange information among themselves depending upon the belief, so trust has a vital role in such networks. When a node is in mobility, number of forwarding nodes come in contact and interation starts when there is a packet to send via the forwarding node. This interaction may not be too long, even then if packets are received and not forwarded that is dropped intensionally. Due to this reason trust value is very important to start any communication. Malicious behaviour of a node is tough to identify. A node may exhibit false trust and behave like a trustee node. That is why trust computation and trust management is a challenging task in future generation networks. An un-trusted node in a network can lead to damages the network resources like battery power loss and control packets dropping. This results the overall poor performance of the network.

A future generation network means 5G network or higher. These kind of networks has the following features:

- Heterogenous Nature
- Infrastructure-less Connectivity
- Fully Secured and Privacy Protected
- Evolutionary Computing and Artificially Intelligent
- Scalability and Integration
- Distributed Computing
- Ultra High Speed with Multimedia
- Cloud Connected
- IoT Enabled
- Social Networking mapped

In network security domain, computational trust is the generation of trusted authorities or user trust through cryptography. In recent time the network technology focuses on distributed computing rather than centralised computing. In centralised systems, security mechanism is comparatively simple as the identity is checked and verified in the central database site. Hence no new user is allowed without proper authentication. Rigid authentication mechanisms, such as Public Key Infrastructures (PKI) are required in distributed computing as the user has multiple avenues to enter into the network.

There may be collaborating domains along with main administrative domain. Each domain must be well equipped with all types of security measures to control the entry of any malicious node inside the network. In spite of stronger security arrangements, untrusted nodes often attacks the communication system. That is the reason behind several security models,

policies and mechanisms needed to protect users information and resources in future networks.

## II. Related Works

In the paper [2], a Bayesian trust framework for pervasive computing is developed. Since pervasive computing is the future generation technology, the model is useful for proposed work. B-trust is the framework designed in the paper which has explained belief in well manner. A similar work is reported in [3] where a trust evaluation model for cloud computing environment is developed. A cloud computing environment is purely distributed in nature and hence there is high risk of malicious node. Trust evaluation model in this case became very helpful for the network environment.

The paper[4] presented various trust models in cloud computing. Though the paper is a review paper, there is a statistical method to choose the best trust model for a new cloud system. An analytical evaluation of P2P reputation systems [5] is developed for distributed systems. From distributed point of view the P2P is not so promising, even then the model shows a good reputation evaluation among nodes. The paper [6] has done survey on trust management techniques for the Internet of Things (IoT).

Researchers [7] developed a computational trust model for IoT. In their model, five levels of trusts are mentioned namely High Trust (HT), Trust (T), Under Trust (U), Distrust (D), High Distrust (HD). The sum of all the levels is considered as 1. That means the range of values are considered from [-1,2]. In the model, every nodes are giving their individual opinion. At a point of time, the model takes n numbers of opinions from n nodes. Using orthogonal sum, the opinion is converted to confidence. The proposed trust mechanism employs Dempster Shafer Theorem to overcome uncertainty and lack of sufficient data about a vehicle for quick trust update. It is concluded that the distrust of a vehicle driver decreases once misbehave is captured in the operation. Confidence is gained at each successful data communication.Similar work is reported in [8].

In the model [9], a group leader based trust model is developed for VANET to avoid the broadcast storm. A modified AODV protocol called GL-TVAODV is designed where a vehicle cannot directly broadcast a message to the network. To broadcast a message a vehicle needs to send request to the Group Leader (GL). In such ways we can reduce the broadcast storm. RSUs are playing the role of GL in their region or area and vehicles are the members of particular group. All the members in a group are one-hop Group Members (GM) i.e. all the GM are within one-hop communication range of the GL. In the NS2 based simulation reasonable accuracy is achieved.

Though there are number of models existing for different networks, there is a high demand for a trust computing model which covers maximum of the influential factors over trust computation so that the trust value computed is a stable, worthy and usable in heterogenous environment. Moreover the risk analysis is not included in many of the existing models. In the proposed model, these two points are highly emphasized.

## III. Trust Computing Model

In this section a trust assessment process is explained. Trust can be broadly categorised into two types:

### A. Individual Trust or Direct Trust

It is the direct trust of a node on another node Fig. 1. The node which has trust on other node is trustor node and the node which is trusted is trustee node. Trust (i,j) means trust of node i over node j. Here node i is the trustor and node j is trustee. The trust is perception based and subjective. It can be sub categorised into two types-emotional trust and logical trust. Emotional trust is directly node dependent. A node can assess emotion trust through request-to-response time, nodes registration information. In this paper, emotion trust includes expectation, willingness, attitude and propensity. Logical trust is the trust of the node which is computed on certain conditions of the network like throughput, end-to-end delay relative to that node. Logical trust includes belief, experience, rationality, uncertainty and reliability.

**Expectation E(i,j)**: Expectation of node i on node j is the physical presence of the node j when node i enquires about it. In the network, the user log or node log is verified for such operation.

**Willingness W(i,j)**: It is the willingness of node j to connect to node i. When node i broadcasts the initial message in the network and if node j responds to that request message for data communication instantly, then willingness W(i,j) exists with respect to response time.

**Attitude A(i,j)**: It is the attitude of node j over node i during data communication. If node i communicates to node j and node j is responding but the response time is random or gradually increasing, the value of attitude A(i,j) will be negative. Attitude A(i,j) will be positive if the response times for each set of communications between two nodes are almost same.

**Propensity P(i,j)**: It is the inclination of node j over node i during data communication. If total number of data packets in the form of ACKs from node j is more than the total number of data packets from node i to node j, then propensity P(i,j) is non-zero otherwise zero.

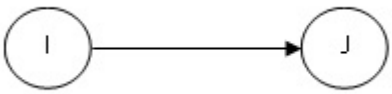


Fig. 1. Direct Trust

Emotional trust is one-sided i.e. only trustor takes the lead role to assess the trust values whereas the logical trust is not one-sided. Proper logic is applied from both the end to assess the trust values. In logical trust, five subcategories are considered in the proposed model. These are as follows-

**Belief B(i,j)**: Its an acceptance between two nodes. Its a mutual factor of two nodes. Node i accepts the presence of

node j and vice versa. Now the main issue is how belief is evaluated in a network. When both nodes agree for data communication, B(i,j) may be considered as 1 otherwise 0.

**Experience Ex(i,j)**: It is the usage of a node in a network. Since it is a mutual factor, both nodes are considered in this case. The number of data packets transmitted by the node is the key factor in evaluating Ex(i,j). There may be various cases of experiences like node i may have more experiences than node j or vice versa. Two nodes may have same experiences. So the net experiences of two nodes as a whole will be normalised to [0,1] interval to get the final value of Ex(i,j).

**Rationality R(i,j)**: A rational node is one which is sensible and is able to make decisions based on intelligent thinking rather than on emotion. The net rationality R(i,j) of two nodes signifies the sensibility of two nodes.

**Uncertainty U(i,j)**: Here uncertainty is unpredictable act of a node. It is difficult to measure accurately. Often uncertainty is either 0 or 1. Type-2 fuzzy logic may be used to quantify U(i,j) in proper manner.

**Reliability Re(i,j)**: The degree to which the result of a measurement can be depended on to be accurate is reliability. Reliability is again depending on consistency. If both nodes have low error rates in data communication, reliability is higher. After evaluating all the direct trust entities, a direct trust is calculated using (1), (2) and (3). Median of both emotional trust and logical trust are calculated first and then their respective weightage are considered.

According to Dale Carnegie [10] and several other studies conclude that up to 90 percent of the human decisions are based on emotion. Human emotions are simply biological states associated with the nervous system brought on by neurophysiological changes variously associated with thoughts, feelings, behavioural responses, and a degree of pleasure or displeasure. There is currently no scientific consensus on the definition of human emotion. For a human being, emotion always win over logic. But for a device like computer, mobile phone, or any kind of nodes in the network follow the opposites. For them logic is more than emotions. Because logic is based on evidence, data, statistics, examples etc. Hence in this proposed model 90

$$DT1(i,j) = M[E(i,j), W(i,j), A(i,j), P(i,j)] \quad (1)$$

$$DT2(i,j) = M[B(i,j), Ex(i,j), R(i,j), U(i,j), Re(i,j)] \quad (2)$$

$$DT(i,j) = 0.1 * DT1(i,j) + 0.9 * DT2(i,j) \quad (3)$$

### *B. Relational Trust or Indirect Trust*

It is the indirect trust of a node on another node Fig. 2. Unlike direct trust, a third node as referral node is considered for relative trust computation. Indirect trust (i,,j) has a new vital factor known as relative co-efficient (a). Relative co-efficient is directly related to various other factors relative to trustee node. In the proposed model four factors namely homophily, mindedness, centrality and importance are considered for indirect trust computation.

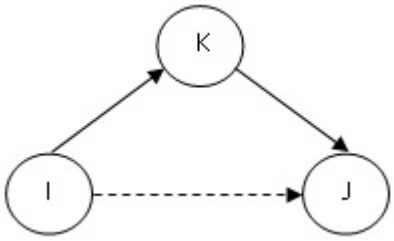


Fig. 2. Indirect Trust

**Homophily H(i,j)**: Homophily refers to the tendency of a node to have (non-negative) ties with other node those which are similar to themselves in the network environment. It depends on the response of a third node k over node j i.e response-time(k,j). If response-time(k,j) and response-time(i,k) are similar, then H(i,j) is non-zero otherwise 0.

**Mindedness Md(i,j)**: Mindedness is the quality of being willing to consider ideas and opinions that are new or different from own. It signifies how a node is ready for openness. The input regarding the openness is considered from a third node which depends on their previous relationship.

**Centrality C(i,j)**: Centrality measures the number of times a node lies on the shortest path between other nodes. It shows which nodes are bridges between nodes in a network. It is calculated by identifying all the shortest paths and then counting how many times each node falls on one.

**Importance I(i,j)**: Importance is the factor by which a node is relatively given importance for any communication. Through importance, the behaviour of the trustee node is assessed although it is relative. After evaluating all the indirect trust entities, an average indirect trust is calculated using (4).

$$IT(i,a,j) = a + M[H(i,j), Md(i,j), C(i,j), I(i,j)] \quad (4)$$

Where indirect trust coefficient is 0.1 since all H(i,j),Md(i,j),C(i,j) and I(i,j) may be zero due to network biasness. That means if H(i,j)=Md(i,j)=C(i,j)=I(i,j)=0, IT(i,a,j) is non-zero. The final trust between node i and node j is calculated (3)) as

$$T(i,j) = DT(i,j) + IT(i,a,j) \quad (5)$$

In the proposed model the final trust T(i,j) is nothing but the confidence of a node over another node.

In the risk analysis part, a risk value is assesed with three factors namely ambiguity, vulnerability and failure impact. Ambiguity in networks includes location ambiguity, flip ambiguity and trilateration. Due to the ambiguity, a node is wrongly localized and data packets sent to wrong positioned node may be a futile task. In a versatile network, proper localization is a big task.

Vulnerability is the security vulnerability which is very common in adhoc networks. Proper intrusion detection mechanism can find out the extent of vulnerability of a node. It is very vital factor as it signifies the attacker's motive.

Failure impact is an index of a node that due to the mishandling and malfunction of a node if any failure occured in the network environment or not. Though failure is an unpredictable event but it is a risk factor.

Risk factors are very rare but can not be ignored. In the proposed model there is risk analysis part. If risk is found, the risk value is subtracted from the trust value.

## IV. Data Analysis

The data analysis is performed with all the factors in the common interval [0,1]. The data considering the initial trust between two nodes is zero and the final trust is calculated through simulation which is is furnished in the table (table 1).

TABLE I
FINAL TRUST

| T(i,j) | D(i,j) | IT(i,a,j) | Final Trust T'(i,j) |
|---|---|---|---|
| 0 | 0.19 | 0.5 | 0.69 |
| 0.69 | 0.19 | 0.55 | 0.74 |
| 0.74 | 0.19 | 0.52 | 0.71 |

It is observed that the trust value is increasing in all iterations Fig. 3. Since few factors like centrality has always a tendency to increase due to the increasing number of nodes in the network. Dynamic topology will change the centrality time to time. Importance is another factor which has a tendency to increase since a node after a few successful data communication gets higher intimacy. Trust value may decrease also.

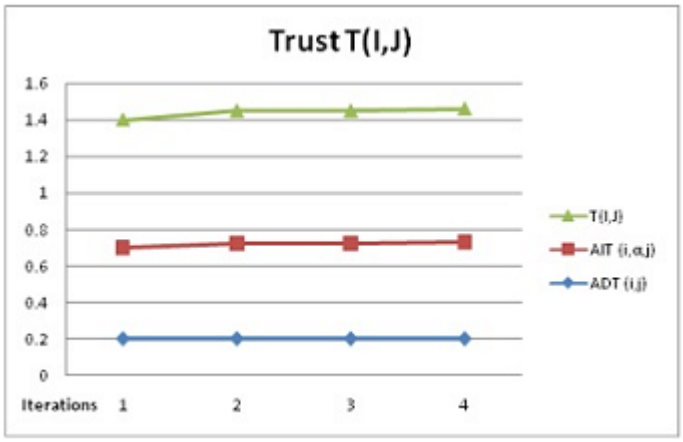


Fig. 3. Indirect Trust

## V. Conclusion and Future Work

In this paper a trust computing model is proposed for future generation network considering almost all the factors affecting the trust. A simple data analysis is done with initial trust value as zero. The proposed model yields increasing trend of trust values in each iteration which is again not expected in every situations. There may be negative trust also which is known as distrust. The distrust is not performed in this paper which is a major limitation of the paper. In the future the distrust will be included in the proposed model.


## Acknowledgment

The authors are grateful to the authorities of both Assam University, Silchar and Mizoram University, Aizawl for providing the facilities and support to accomplish the present research work.


## References


[1] Cho Jin-Hee, Chan Kevin,Adali Sibel, A Survey on Trust Modeling, ACM Journal Computing Surveys, Vol. 48, No. 2, pp. 799-823, 2015.

[2] Quercia D.; Hailes S.; Capra L., B-trust: Bayesian Trust Framework for Pervasive Computing, International Conference on Trust Management, pp 298-312, 2006.

[3] Kim H., Lee H., Kim W., Kim Y., A Trust Evaluation Model for Cloud Computing, In: lzak D., Kim T., Yau S.S., Gervasi O., Kang BH. (eds) Grid and Distributed Computing, Communications in Computer and Information Science, Vol. 63, Springer, 2009.

[4] Ritu, Randhawa Sukhchandan, Jain Sushma, Trust Models in Cloud Computing: A Review, I.J. Wireless and Microwave Technologies, Vol. 4, pp. 14-27, 2017.

[5] Lagesse Brent, Analytical Evaluation of P2P Reputation Systems, InderScience International Journal of Communication Networks and Distributed Systems, Vol. 9, No.1/2, pp. 82-96, 2012.

[6] Ud Din, M. Guizani, B. Kim, S. Hassan and M. Khurram Khan, Trust Management Techniques for the Internet of Things: A Survey, in IEEE Access, Vol. 7, pp. 29763-29787, 2019.

[7] Bhargava, S. Verma, B. K. Chaurasia and G. S. Tomar, Computational trust model for Internet of Vehicles, Int. Conference on Information and Communication Technology, Gwalior, pp. 1-5, 2017.

[8] K. M. Sadique, R. Rahmani and P. Johannesson, Trust in Internet of Things: An architecture for the future IoT network, International Conference on Innovation in Engineering and Technology, Dhaka, Bangladesh, pp. 1-5, 2018.

[9] Roy Debasish, Das Prodipto, Trust and Group Leader based Model to Avoid Broadcast Storm Problem in Vehicular Ad-hoc Networks, Advances in Computational Sciences and Technology, ISSN 0973-6107, Vol. 10, No. 4, pp. 575-597, 2017.

[10] Dale Carnegie, The Art of Public Speaking, Samaira Book Publishers, UP, ISBN: 9789387550278, 2019.