Journal of Organizational and End User Computing
Volume 32 • Issue 3 • July-September 2020

A Novel Trust Model for Secure Group Communication in Distributed Computing

Naresh Ramu, SRM Institute of Science and Technology, India
Vijayakumar Pandi, University College of Engineering, Tindivanam, India
Jegatha Deborah Lazarus, University College of Engineering, Tindivanam, India
Sivakumar Radhakrishnan, University College of Engineering, Tindivanam, India

ABSTRACT

Distributed networks are networks in which each node can act as a server or client and hence any node can provide service to any other node. In such a scenario, establishing a trust model between the service providing user and the service utilizing user is a challenging task. At present, only a few approaches are available in the past literature to provide this facility. Moreover, the existing approaches do not provide high trust accuracy. Therefore,a novel efficient trust model has been proposed in this article to support the secure dynamic group communication in distributed networks. The main advantage of the proposed work is that it provides higher trust accuracy. Moreover, the proposed work takes less memory for maintaining the trust values and increases the packet delivery ratio in comparison with other existing works which are in the literature.

KEYWORDS

Distributed Network, Group Communication, Security, Trust Accuracy, Trust Management

INTRODUCTION

In the recent years, rapid development of the distributed computing has numerous realtime applications, which incorporates a number of relative technologies such as cloud computing, utility computing, grid computing, pervasive computing, sensor networks, cluster computing, peer to peer computing, wireless sensor networks (Gray, 2008; Afek et al., 2011). These technologies are used for a variety of applications, such as service providing, information processing, resource sharing and data storing and retrieval. In a distributed network, each user tries to utilize or provide the services from/to the other users and the distributed networks are dynamic in nature as well. Moreover, a open distributed network is easy to enter and also susceptible to a variety of malicious attacks (Zahariadis et al., 2010; Sun et al., 2008). Hence, developing a secure protocol to support group communication in a distributed network is a challenging task since there is no concept of a centralized co-ordinator to co-ordinate the activities between different nodes.

In addition to this, each node should also compute and maintain a trust value about other nodes to perform the trust based group communication. Therefore, a new way of trust and secure group

DOI: 10.4018/JOEUC.2020070101

key management is needed to detect the existing malicious users in the distributed network. Trust management means, the degree of reliability of the neighbour users, who are used to send the information from source to destination securely. Therefore, we introduce an efficient trust management model in this paper to support the dynamic secure group communication in the distributed networks. In order to develop a trusted group communication, researchers have developed various schemes (Yuxing et al., 2008; Xi et al., 2011; Shaik et al., 2014; Libin et al., 2015). However, most of the schemes suffer from high computational cost since each distributed node has to perform two tasks. One is to generate and distribute the group key to the group users who are in the distributed network. The other work is to compute the trust values for all the users based on the past communication history. Moreover, developing an efficient trust model along with higher trust accuracy is a difficult task. Hence, in this paper, we have proposed a new trust model with high trust accuracy to support the trusted secure group communication. To perform secure group communication, we have already developed two protocols (Pandi et al., 2016; Pandi et al., 2016). In this paper, a new trust evaluation model alone is developed with the following objectives:

- To develop an efficient trust model with high trust accuracy;
- To develop a communication efficient trust model;
- To increase the packet delivery ratio;
- To take a minimum memory space for storing the trust values.

The road map of this paper is represented as follows. The existing security and trust management model is discussed in section 2 and the proposed Trust Level Agreement for Distributed Network (TLADN) is presented in section 3. The Trust evaluation of users is mentioned in section 4, performance evaluation and comparative analysis of the proposed trust management methods are presented in section 5. Finally, section 6 provides the concluding remarks.

RELATED WORKS

In this section, we have included various works that are used to provide security and trust in a distributed network.

Security in the Distributed Network

Distributed network supports dynamic group communication because it divides all the works among the users involved in the network and hence presents new issues for security. Till date, there has been more research papers which discuss about security issues in the distributed networks. L. Kagal et al. (2001) discussed several security issues, requirements and challenges that a dynamic group communication faces in the distributed networks. They had suggested some of the security policies and trust evaluation models to resolve these issues in both technological and real time applications such as peer to peer communication, Skype, Facebook,Whatsapp, PAY-TV, Video conferencing, E-mail, Twitter and online games.

One of the basic problems with maintaining distributed networks is provided that not only security services, but also assurance that those services are properly enforced and hold within the distributed networks. Belapurkar et al. (2009) distinguish about the Security issues, Processes and Solutions in distributed networks with more experimental and simulation results that show more vulnerabilities and various attacks detected in the distributed networks using security analysis tools. The authors also challenge to give a level of assurance by providing some security architectures and trust management methods.

Dan (1987) had proposed a new idea of trust based on distributed networks and distributed user trust evaluation levels. They had suggested the fails to make allowances for the distributed network

physical security requirements and trust management factors, by more than one standard legal authority, and the interactions that can occur between users supporting different mandatory and discretionary security services.

The growing technology of distributed networking needs that greater consideration be given to ensuring security services inside these distributed group communication. The different nature of several cooperating users, together with the considered interoperability and inter-connectivity between those distributed dynamic group communications has made the effectual services of security and other trust evaluation methods are more essential. Robin L. Sherman (1992) had suggested some world wide and local security policies which will ensure that the requisite levels of secure communication made to form the secure distributed group communication. But the practical implementation of such complex systems remains questionable.

In a distributed network, vulnerable nodes cause serious risk as they can weaken the right operation of basic functionalities, such as data request or response services. Oscar Garcia-Morchon et al. (2013) proposed that trust evaluation method between users is a necessary part of the distributed network. In detail, sponsor users shall communicate with trusted users only and misbehaving users must be rapidly withdrawn from the distributed group communication. This paper introduces new approaches and property of the mutual security protocol, which enforces trust management model by means of two voting models. In the first voting method, the admission process is done by every user gaining trust by distributing revocation security policy to its neighbor users. These neighbor users, support is essential for the formation of trusted users. If the user collaborate and exposes enough security information, it joins in the distributed group communication and can communicate with the remain of the distributed network. Otherwise, the vulnerable user is rejected. If the permitted user tries to be an internal attacker in the distributed system, the second distributed revocation voting model is used. In this regard, if the user support agrees upon the act of misdeed, they leave the user from distributed group communication using previously disclosed revocation security information.

Trust in the Distributed Network

The distributed reputation based trust management model was proposed by N. Santos et al. (2009). In this system, a trust value is computed and distributed to all the users to take a concrete decision about the trustworthiness of users and the main limitation of the work is more space complexity.

Azzedine Boukerche et al. (2009) proposed that, Nowadays, due to rapid growth, the distributed telecommunication system in telemedicine services has stimulated wide real time applications such as mobile E-health applications, E-Learning about medical prescription. However, in distributed networks, security is an essential feature while providing secure dynamic distributed group communication because many patients have private medical information while it comes to share their personal information over the open distributed network. In this scenario, these authors had developed a novel trust evaluation model which supports secure multicast communication employing expectation in order to assess the performance of each user participating in the group. Therefore, only the trustworthy users are allowed to join in the dynamic group communications, whereas the misbehavior of untrusted users is effectively prohibited. The main advantages are analyzing all the security parameters of multicast protocols and evaluate its behaviour based on simulation experiments with low computation cost. The main limitation is that it does not support indirect trust evaluation method.

Hwang et al. (2010) discussed about the various service-level agreements (SLAs) by their dynamic level of shared services among service providers and utilizing users. Distributed networks deal with several serious security issues which include integrity, confidentiality, and trust among service providers, individual users, and group users. In this paper, the authors suggest using a trust-overlay distributed network over several data centers to implement a standing system for establishing trustworthiness between service providing users and utilizing users.

In the recent years, medical sensor networks have become essential for e-healthcare applications, but the security in this kind of applications remains a very challenging issue and is yet to be resolved. Moreover, the existing cryptographic mechanisms are not enough given the uniqueness of MSNs, and they are vulnerable to a several kind of misbehaving users. J. Yu et al. (2010) and Daojing He et al. (2012) had discussed about the security and performance assessment of networks depending on the mutual and trust based distributed dynamic users and put forward that it is very essential for each user to assess the trustworthiness of other users. In this paper, relevant user behaviors such as data transfer rate and send-off time, into trust assessment to detect malicious users were introduced. The main advantages are that they support all the direct, indirect and historical trust evaluation method. The main limitation of this work is computation overhead.

Many real time distributed network applications are based on Role-Based applications. Ke Chen et al. (2009) suggested that credential chains can be used to implement the trusted peer-to-peer (P2P) applications, where trust assignment should be established between every pair of peers at the particular role level. Role-based trust was distinguished from the coarse-grained trust evaluation model used in most P2P reputation systems. In this paper introduces a new idea based on a heuristic-weighting approach for finding the shortest path to establishing a role-based trusted network. They have considered the history of the routing path information to measure the shortest path complexity and to assess the pair of peers chaining effectively. In addition, this model determines the successive edges of a trust chain to equal with the demands in any given P2P application. These authors had introduced a novel heuristic chaining method for all the directions (backward, forward, and both direction) evaluation of trust chains. The main advantages are efficient trust evaluation scheme in terms of the search time, minimum storage cost and enhance the chaining accuracy in dynamic P2P networks. The main limitation is the computation overhead.

In wide-area distributed networks which provide the facility of distributed services, shared resources such as Bigdata computing centers and huge-performance computing centers suffer from security issues due to lack of centralized coordinator. They are susceptible to a variety of malicious attackers from Internet. Haiying Shen et al. (2013) presents Peer to Peer based infrastructure for truthful and efficient user communication in wide-area distributed networks. This work addresses both the trustworthiness and efficiency in its computing performs in order to achieve the high performance service of distributed network applications. The main advantages are achieving both more trustworthiness and high efficiency in comparison to other existing approaches.

The consistency of delivering packets through multi-hop intermediate users is a significant issue in the distributed network. In distributed networks, all the nodes have established connections to form the dynamic distributed group communication, which possibly will include self-centered and misbehaving several nodes. Antesar et al. (2014) had proposed the recommendation based trust management protocol to remove the misbehaving users while looking for a trust route message delivery is a challenging issue due to the threat of false recommendations like ballot-stuffing, bad mouthing attack, collusion and certain time bound based on a number of communication messages, compatibility of information and nearness between the nodes.

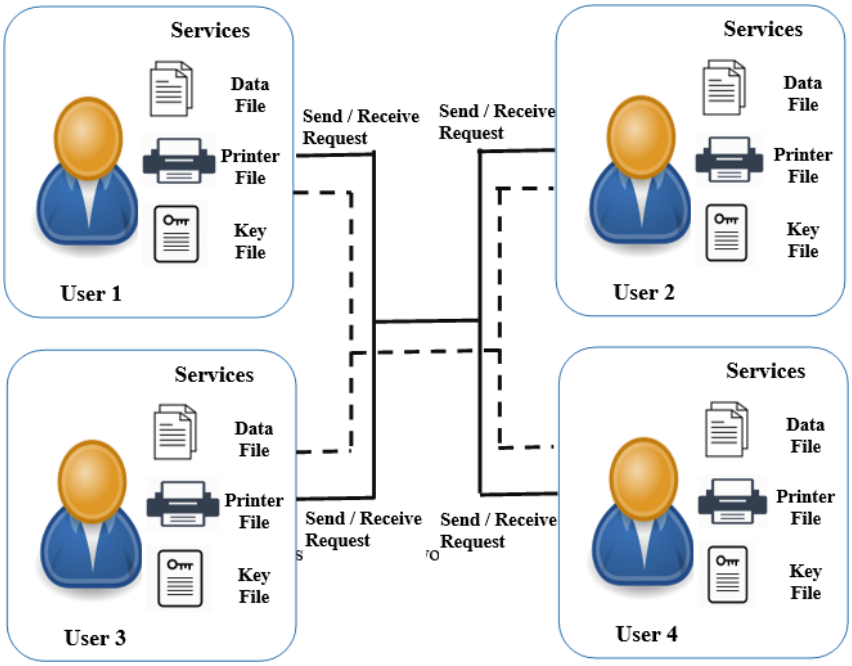
Goutam Mali et al. (2016) proposed a trust-based distributed network model for use in the wireless multimedia sensor networks. This work accomplished the Received Signal Strength (RSS) of the control packets, which are used to establish the secure distributed group communication. In an unsecured distributed network, utilize the trustworthiness helps in providing coverage of a service, and maintaining connectivity, but still in the presence of misbehaving users. The main advantage of the scheme is that it achieves an efficient coverage ratio and optimal packet delivery ratio than existing approaches in the presence of malicious attacks.

TRUST LEVEL AGREEMENT FOR DISTRIBUTED NETWORK (TLADN)

In this section, the proposed trust level agreement has been presented. First, we discuss about a structure of distributed network environment. Secondly, we present the definitions about trust level agreement and the proposed work of Trust Level Agreement for Distributed Network. Finally, we discuss about the way of evaluating the trustworthiness of users.

Figure 1 represents the structure of a distributed network. In this figure, various users are connected with each other in a distributed manner. Each user maintains some files which can be shared with other

Figure 1. The structure of a distributed network

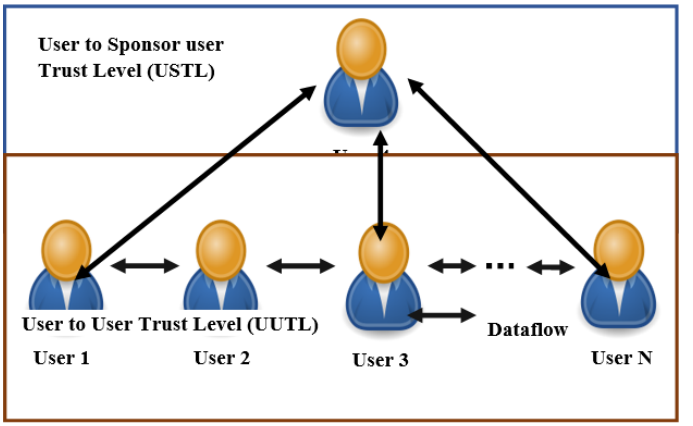


users. In order to share the files with other users, each of the users initially exchange some security parameters as discussed in our previous work (Pandi et al., 2016; Pandi et al., 2016). These security parameters are used for computing a common group key to perform secure data communication.

Moreover, when the security parameters are exchanged, it is necessary to find the trust value of each user for performing a trusted secure communication in the distributed network. In this paper, a novel trust agreement for computing the trust value between two different users is proposed. The main objective of this proposed work is to compute a trust value for each user and to perform a secure communication based on these computed trust values.

To compute the trust value for each user, a two level trust agreement is proposed in this paper. Figure 2 represents the Trust level Agreement based Distributed Network Trust Model. In this figure, we have represented the proposed two level agreement method which consists of two levels, namely User to User Trust Level (UUTL) and User to Sponser user Trust Level (USTL). The first level UUTL is used to find a trust value between user to user. The second level is used to compute the trust value between user to sponsor user. To find the trust value between any two users, we use two approaches, namely Direct trust and Indirect trust. In direct trust, each user computes a trust value based on the number of communications that it performs with other users.

Figure 2. A trust level agreement based distributed network trust model



In Indirect trust computation, each user computes a trust based on the communication that it performs with some intermediate node. For example, if user 1 wants to compute a trust value for user 2, it can use Direct trust computation, since user 1 is directly connected with user 2. If user 1 wants to compute a trust value for user 3, it should compute the trust value based on the information collected from user 2 since there is no direct connection between user 1 and user 3. In this way a trust value is computed using two different approaches. In section 4, we have clearly explained our proposed trust level agreement model.

Trust Evaluation of User

In this proposed approach, we define trust as an expectation about the behaviors of what a user denoted as a u_i, expectation from another user is denoted as a u_j, to perform a given task. Each user uses trust value to assess whether it can trust the other user or not. If a user is not a trusted user, then no other user will perform data communication. The trust values are calculated using two ways namely Direct trust and Indirect trust. When a user u_i has enough communication experience with u_j, u_i uses direct trust to compute the trust value for u_j. Otherwise, when u_i does not have enough communication experience with u_j, u_i uses indirect trust to compute the trust value for u_j. In our approach, we define the communication experience threshold which is defined based on the number successful communication performed between the users connected in the distributed network.

Direct Trust Method

The direct trust value $DT_{u_i-u_j}$ is defined as:

$$DT_{u_i-u_j} = \frac{\sum_{k=1}^{N\left(u_{ik},u_{jk}\right)} S\left(u_{ik},u_{jk}\right)}{N\left(u_{ik},u_{jk}\right)} \tag{1}$$

where:

$$S\left(u_{ik},u_{jk}\right) = \begin{cases} > 0.5 \text{ to } 1, & if\ satisfied \\ < 0.5, & if\ not\ satisfied \\ = 0, & if\ u_i, u_j\ are\ not\ Linked \end{cases}$$

Let $N\left(u_{ik}, u_{jk}\right)$ denotes the total number communications that u_i has performed with u_j and $S\left(u_{ik}, u_{jk}\right)$ denotes the $u_i's$ satisfaction degree of communication in its i^{th} communication with u_j which is in the range of (0,1).

In Equation 1, we determine the average number of failed communications, otherwise unsuccessful interactions may cause its user u_i totally untrusts from user u_j. Based on the value, each user decides to continue (or) stop its communication with other users. For example, if the value of $S\left(u_{ik}, u_{jk}\right)$ is 0, then user u_i does not make any communication to user u_j. After that, user u_j is considered as a malious user to user u_i.

Indirect Trust Method

The Indirect trust value of $IDT_{u_i - u_k}$ is defined as:

$$IDT_{u_i - u_k} = max\left(DT_{u_i, u_j}, DT_{u_j, u_k}\right) \tag{2}$$

where *j* refers to the intermediate users who are available between u_i to u_k and the value of j can be $j = 1,2,3, \ldots, n$.

The mechanism of evaluating indirect trust allows each user to calculate the trust value based on the direct trust value which was computed through a direct connection available between any two users. However, in a large scale dynamic distributed network, the mechanism is not scalable due to message overhead problem. From the perception of distributed network users, the proof of trust computation between individuals is from direct communication information and other users trust information, but not all existing users trust information must be collected. In a dynamic distributed group communication, any user may join / leave from the distributed network at any point of time. Therefore, it is essential to calculate the trust value based on the newer interactions to ensure the dynamic trust value.

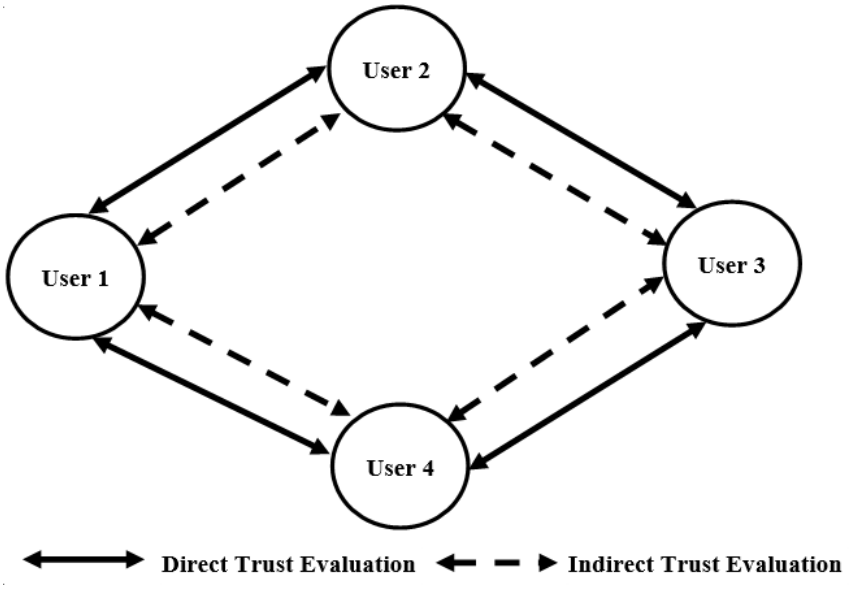
While computing the indirect trust in a dynamic network, a user u_i may get a trust value for a user u_j through two different paths/links. In such a scenario, the user u_i has to select a higher trust value among the two trust values. If more than two trust values are available for a user u_k, then maximum trust value is considered as shown in Equation 2. Based on the above descriptions, both direct and indirect trust evaluation method should satisfy the following conditions:

1. Trust value is computed based on newer interaction;
2. The direct/indirect trust value should not exceed a threshold value T = 1;
3. Communication between the users must satisfy all the quality of service parameters in the distributed network.

For example, in Figure 3, four users are available which are denoted as user1, user2, user3, and user4. Among the four users, we consider user1 as a source node and user3 as a destination node, user2 and user4 are intermediate nodes available between user1 and user3. In our approach, all the individual users maintain trust value computation table which contains the source node, destination node, the number of messages communicated, number of successful acknowledgement received, number of messages failure and trust value.

Consider, for example, in this table source node is used to indicate the node for which trust value computation table is computed. The destination node is the node for which there is a direct link from the source node. The number of messages communicated is used to identify the total number of messages that are sent from source node to destination node. user1 knows about two direct neighbors

Figure 3 Example of direct and indirect trust evaluation model



user2 and user4, and hence user1 can use the direct trust value evaluation method to compute the trust value between the direct neighbors (The user1 to user2, user1 to user4). user1 does not know about user3, and hence user1 cannot use direct trust evaluation method to compute the trust value. Therefore, user1 can use the direct trust value of user2 and user4 to compute the indirect trust value of user3.

Table 1 clearly describes about user1 that is maintaining the trust value of direct neighbors. Here, we have assumed that user1 has sent 10 different messages to user2, but user2 has responded only for

Table 1. User 1 trust value computation table

Source Node	Destination Node	No. of Messages Communicated	No. of Successful Acknowledgement Received	No. of Message Failures	Trust Value
User 1	User 2	10	8	2	0.8
User 1	User 3	-	-	-	-
User 1	User 4	10	4	6	0.4

8 messages to user1 Based on this interaction information, user1 computes the trust value using direct trust evaluation method from Equation 1. The trust value between user1 and user2 is 0.8, since user1 is satisfied for 8 messages among 10 request messages. Therefore, the trust relationship is satisfied because the trust value is greater than 0.5. Also, user1 has sent 10 request messages to user4, but user4 has responded for only 4 messages to user1. Based on this newer interaction information, user1 computes the trust value using direct trust evaluation method. The trust value between user1 and user4 is 0.4, so that the trustworthiness among them is not satisfactory because the trust value is less than 0.5. Hence user 1 will not believe all the messages received from user4. Moreover user1 does not have any direct communication to user3, so the trust value between them is considered as zero.

Similarly, direct trust value is computed for other users as shown in Table 2, Table 3 and Table 4. After computing the trust value using direct trust computation method, each user exchanges

Table 2. User 2 trust value computation table

Source Node	Destination Node	No. of Messages Communicated	No. of Successful Acknowledgement Received	No. of Message Failures	Trust Value
User 2	User 1	10	8	2	0.8
User 2	User 3	10	6	4	0.6
User 2	User 4	-	-	-	-

Table 3. User 3 trust value computation table

Source Node	Destination Node	No. of Messages Communicated	No. of Successful Acknowledgement Received	No. of Message Failures	Trust Value
User 3	User 1	-	-	-	-
User 3	User 2	10	6	4	0.6
User 3	User 4	10	3	7	0.3

Table 4. User 4 trust value computation table

Source Node	Destination Node	No. of Messages Communicated	No. of Successful Acknowledgement Received	No. of Message Failures	Trust Value
User 4	User 1	10	4	6	0.4
User 4	User 2	-	-	-	-
User 4	User 3	10	3	7	0.3

its own trust value computation table to its neighbors. This process takes place periodically. For example, user1 exchanges its table with user2 and user4 and vice versa. After exchanging the trust value computation table with the neighbors, each user can take the unknown information from the received tables using this unknown information each user can compute the indirect trust value of other users who do not directly connected in the distributed network. For example, user1 receives the trust value computation table from user2 (Table 2) and user4 (Table 3) using these two tables and the user1 updates its table as shown below.

In Table 5, the indirect trust value of 0.6 is updated for the user1 to user3. Using Equation 2, we update the trust value of user1 to user3.

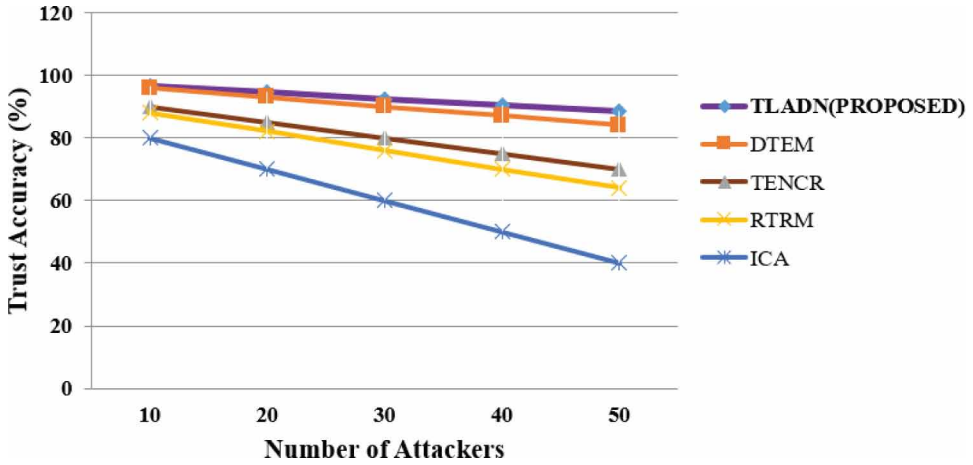
Table 5. Updated trust value computation table of User 1

Source Node	Destination Node	No. of Messages Communicated	No. of Successful Acknowledgement Received	No. of Message Failures	Trust Value
User 1	User 2	10	8	2	0.8
User 1	User 3	10	6	4	0.6
User 1	User 4	10	4	6	0.4

Performance Evaluation

In this section, the proposed work is simulated to analyze the performance of this proposed work (TLADN) with various existing works Recommendation Trust Revision Model (RTRM) (Yuxing et al., 2008), Iterative Classification Accuracy (ICA) (Xi et al., 2011), Trust Evaluation method based on the Node's QoS Characteristics and neighbouring nodes' Recommendations (TENCR) (Shaik et al., 2014) and Dynamic Trust Evaluation Model (DTEM) (Libin et al., 2015). In order to analyze the performance of this proposed work, the proposed trust model is simulated in java by developing a distributed network with Dynamic Source Routing (DSR) protocol. For performing this simulation, 4GB RAM, 500GB Hard disk and Windows OS is used. Based on the simulation, the proposed trust model is analyzed with various parameters, namely trust accuracy, storage complexity, communication complexity and packet delivery ratio. The trust accuracy value is the value of getting accurate trust results through proposed TLADN model on the requirement that all the trust management tasks assigned are completely accomplished. The trust accuracy value is compared with TLADN, RTRM (Yuxing et al., 2008), ICA (Xi et al., 2011), TENCR (Shaik et al., 2014) and DTEM (Libin et al., 2015). We considered that the distributed network size is about 500 users and we have introduced 50 attackers with the maximum transmission range of 400m. Each user possesses a set of services and all the users are uniformly distributed in the group. As shown in Figure 4, with the increase of

Figure 4. Trust accuracy of various schemes



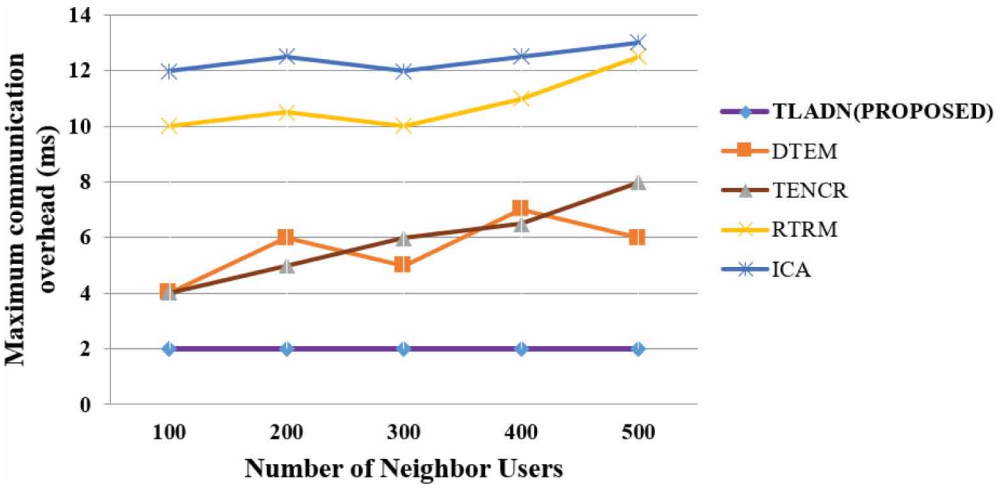
the attackers (the percentage of number of attackers u_m), the TLADN produces high trust accuracy value in comparison with other existing approaches. Despite the number of attackers being 50, our proposed work provides 88.5% trust accuracy. Therefore, the proposed TLADN is more efficient than the existing works DTEM, TENCR, RTRM and ICA. Among the various schemes ICA produces only 40% of trust accuracy.

In a distributed network, each user has its own storage space which is used to store the trust accuracy value of its neighbor users. The storage complexity of the user in our proposed trust management method is 4n where 4n represents four types of values (No of messages communicated, No of successful acknowledgement received, No of message failures and Trust Value) to be stored for 'n' numbers of users. In our proposed TLADN scheme, both direct and indirect trust evaluation methods consume very less storage space than the various existing schemes.

In the existing approaches (Yuxing et al., 2008; Xi et al., 2011; Shaik et al., 2014), when a user wants to make the communication with its neighbor users of direct trust information, it minimally

sends a request message to its neighbors. This request message may take only 01 or 02 bytes in size. But, when a user receives the trust value of neighboring users by using the indirect trust method the size of the request message from each neighbor user may be about 15 to 20 bytes by assuming that each user information takes 2 bytes and it may have 10 neighbor users. Communication overhead is the process of sending the number of messages for computing the trust value before processing the messages. Based on this, communication overhead is computed for our proposed work and existing works. When the number of nodes are high, for example 500, our proposed work takes less than 5 ms for computing the trust value computation table by sharing the information from neighbor nodes. Figure 5 clearly shows that our proposed work is efficient with respect to communication overhead compared to all other existing works.

Figure 5. Communication complexity of various schemes



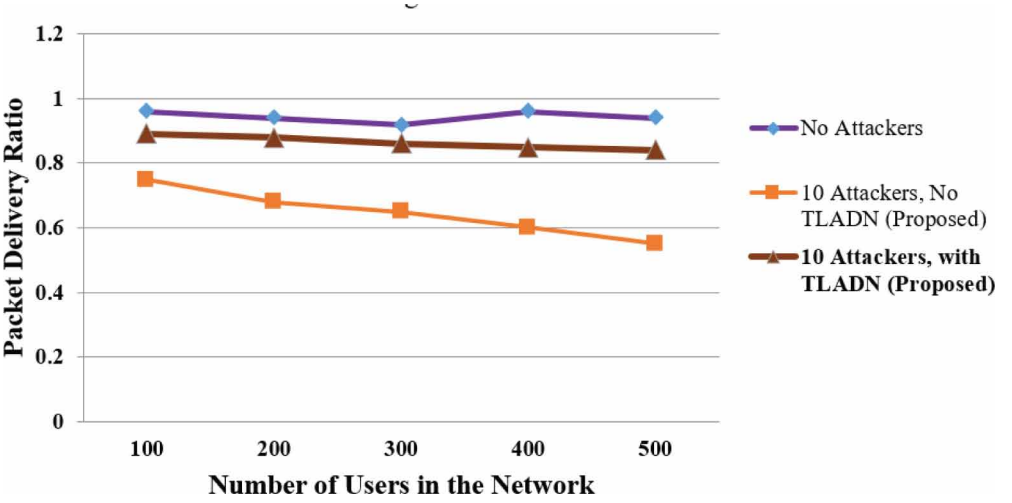
Packet delivery ratio is an important factor of analyzing and evaluating the trust accuracy value of all neighbor users, which means the average ratio of the total number of request messages that are successfully received to the total number of messages sent. In Figure 6, We have compared mainly three parameters. First, the distributed network does not utilize trust management schemes with no attackers. The second is that of the distributed network with 10 attackers who randomly drop about 95% of packets passing through the neighbor users. Third, the distributed network with trust management schemes and 10 attackers.

Figure 6 clearly describes the total number of packets that are successfully transmitted, which represents the distributed network performance. As a result, we obtain two observations. The packet delivery ratio is significantly degraded by 10 attackers. Second, after utilizing trust management schemes, the distributed network throughput performance can be increased because it enables the trusted route establishing which is based on the trust value to avoid less trustworthy users.

CONCLUSION

An efficient TLADN trust evaluation method is presented in this research paper, which is used to detect the existence of malicious users in the distributed network and provides the trustworthiness among the users to perform dynamic secure group communication. The main contribution of this proposed work is that it provides higher trust accuracy compared to existing schemes. Moreover, the TLADN

Figure 6. Packet delivery ratio for various schemes



trust evaluation method takes less storage space for maintaining the trust values while increasing the packet delivery ratio. Moreover, the communication complexity of this proposed work is also less when compared to existing schemes. The future extension of this work is to develop a queuing model along with this trust model so that packet (message) waiting time will also be considered. Therefore, when a message travels from source to destination, both the trust value and the waiting time will be considered for the selection of secure optimal paths.

REFERENCES

Shen, H., Liu, G., Gemmill, J., & Ward, L. (2013). A P2P-based Infrastructure for Adaptive Trustworthy and Efficient Communication in Wide-Area Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems*, *25*(9), 1045–9219.

Afek., Y., Alon, N., & Barad, O. (2011). A biological solution to a fundamental distributed computing problem. *science, 331*(6014), 183-185.

Babu, S. S., Raha, A., & Naskar, M. K. (2014). Trust evaluation based on node's characteristics and neighbouring nodes' recommendations for WSN. *Wireless Sensor Network*, *6*(8), 157.

Belapurkar, A., Chakrabarti, A., Ponnapalli, H., Varadarajan, N., Padmanabhuni, S., & Sundarrajan, S. (2009). Distributed Systems Security: Issues, Processes and Solutions. Wiley.

Boukerche, A., & Ren, Y. (2009). A secure mobile healthcare system using trust-based multicast scheme. *IEEE Journal on Selected Areas in Communications*, *27*(4), 387–399.

Chen, K., Hwang, K., & Chen, G. (2008). Heuristic discovery of role-based trust chains in peer-to-peer networks. *IEEE Transactions on Parallel and Distributed Systems*, *20*(1), 83–96.

Chen, K., Hwang, K., & Chen, G. (2012). A distributed trust evaluation model and its application scenarios for medical sensor networks. IEEE Transactions on Information Technology in Biomedicine, 16(6), 1164-1175. PMID:22623434

Dan, M. (1987). Factors Affecting Distributed System Security. *IEEE Transactions on Software Engineering*, *13*(2), 233–248.

Fang, J. Yu. C., Lu, L., & Li, Z. (2010). Mitigating application layer distributed denial of service attacks via effective trust management. *IET Communications*, *4*(16), 1952–1962. doi:10.1049/iet-com.2009.0809

Garcia-Morchon, O., Kuptsov, D., Gurtov, A., & Wehrle, K. (2013). Cooperative security in distributed networks. *Computer Communications*, *36*(12), 1284–1297.

Goutam, M. (2016). TRAST: Trust-based Distributed Topology Management for Wireless Multimedia Sensor Networks. *IEEE Transactions on Computers*, *65*(6), 1978–1991. doi:10.1109/TC.2015.2456026

Gray, J. (2008). Distributed computing economics. *Queue.*, *6*(3), 63–68. doi:10.1145/1394127.1394131

Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *IEEE Internet Computing*, *14*(5), 14–22. doi:10.1109/MIC.2010.86

Kagal, L., Finin, T., & Joshi, A. (2001). Trust-based security in pervasive computing environments. *IEEE journal of computers, 34*(12), 154-157.

Libin, W. (2015). Service dynamic trust evaluation model based on Bayesian network in distributed computing environment. *International Journal of Security and Its Applications*, *9*(5), 31–42. doi:10.14257/ijsia.2015.9.5.03

Shabut, A. M., Dahal, K. P., Bista, S. K., & Awan, I. U. (2014). Recommendation Based Trust Model with an Effective Defence Scheme for MANETs. *IEEE Transactions on Mobile Computing*, *14*(10), 2101–2115.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards Trusted Cloud Computing. *HotCloud*, *9*(9), 3.

Sherman, R. L. (1992). Distributed systems security. *Computers & Security*, *11*(1), 24–28.

Sun, Y., Han, Z., & Liu, K. J. R. (2008). Defense of Trust Management Vulnerabilities in Distributed Networks. *IEEE Communications Magazine*, *46*(7), 112–119. doi:10.1109/MCOM.2008.4473092

Sun, Y., Huang, S., Huang, H., & Xie, L. (2008, November). A novel recommendation trust revision algorithm for autonomous networks. *Proceedings of the 2008 11th IEEE Singapore International Conference on Communication Systems* (pp. 969-973). IEEE.

Vijayakumar, P., Naresh, R., Islam, S. H., & Deborah, L. J. (2016). An effective key distribution for secure internet pay-TV using access key hierarchies. *Security and Communication Networks*, *9*(18), 5085–5097.

Vijayakumar, P., Naresh, R., Jegatha Deborah, L., & Hafizul Islam, S. K. (2016). An efficient group key agreement protocol for secure P2P communication. *Security and Communication Networks*, *9*(17), 3952–3965.

Wang, X., Maghami, M., & Sukthankar, G. (2011, August). Leveraging network properties for trust evaluation in multi-agent systems. *Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology* (Vol. 2, pp. 288-295). IEEE Computer Society.

Zahariadis, T., Leigou, H. C., Trakadas, P., & Voliotis, S. (2010). Mobile Networks: Trust Management in Wireless Sensor Networks. *European Transactions on Telecommunications*, *21*(9), 386–395.

R. Naresh completed his Ph.D in Computer Science and Engineering in Anna University Chennai in the year 2017. He completed Master of Engineering in the field of Computer Science and Engineering in G.K.M College of Engineering, Chennai affiliated under Anna University Chennai in the year 2011. He completed his Bachelor of Engineering under Adhiparasakthi Engineering College, Melmaruvathur in the year 2007. He is presently working as an Assistant Professor at University College of Engineering, Tindivanam, Tamilnadu, India. His main thrust research areas are Key management in Network Security and Distributed Networks.

P. VijayaKumar completed his Ph.D in Computer Science and Engineering in Anna University Chennai in the year 2013. He completed Master of Engineering in the field of Computer Science and Engineering in Karunya Institute of Technology in the year 2005. He completed his Bachelor of Engineering at Madurai Kamarajar University in the year 2002. He is presently working as Dean at University College of Engineering, Tindivanam. He is guiding for many Ph.D. scholars in the field of network and cloud security. He has published various quality papers in the reputed journals like IEEE Transactions, Elsevier, Springer, IET, Taylor & Francis, Wiley, etc. His main thrust research areas are key management in network security and multicasting in computer networks.

L. Jegatha Deborah completed her Ph.D in Computer Science and Engineering in Anna University Chennai in the year 2013 and completed her Master of Engineering in the field of Computer Science and Engineering in Karunya Institute of Technology in the year 2005. She completed her Bachelor of Engineering under Madurai Kamarajar University, Madurai in the year 2002. She is presently working as an Assistant Professor at Anna University Chennai (University College of Engineering, Tindivanam), Chennai, India.

R. Sivakumar completed his Ph.D in Mathematics in Anna University Chennai in the year 2015. He is presently working as an Assistant Professor at Anna University Chennai (University College of Engineering, Tindivanam), Chennai, India.