International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 1, pp 55-60, January-2023

https://doi.org/10.47001/IRJIET/2023.701009

Proposed Tree Based Trust Algorithm (TBTA) for Manufacturing Grid (MGrid)

[1]Avijit Bhowmick, [2]Goutam Sutradhar, [3]Arup Kumar Nandi

[1]Budge Budge Institute of Technology, Kolkata, India
[2]Director, NIT- Manipur & Professor, Dept. of Mech. Engg., Jadavpur University (On Lien), India
[3]Senior Principal Scientist, CSIR-CMERI, Durgapur, India

***Abstract* - In order to safeguard the private data in the Grid-based collaborative manufacturing environment, providing security is a crucial challenge. The crucial component of Manufacturing Grid is trust management, which is connected to resource sharing, role assignment, cooperation across resource entities from various domains requires careful consideration how to determine and estimate the suggested level of trust. In this research, we present a Tree Based Trust Algorithm for MGrid that combines elements of Interactive Trust, Honesty Trust, and Content Trust. The primary purpose of this research is to minimize the possibility of misleading nodes and to lessen the expense of routing as well as secured data transfer by making use of trust levels.**

Keywords: Trust Algorithm, Security in routing, Trust model, Grid, Cluster architecture.

I. INTRODUCTION

MGrids are used in a variety of settings, including several small, medium, large scale factories, which are geographically scattered. They are responsible for gathering data and wirelessly transmitting it back to the base station. SN is capable of receiving information in addition to sending it out. Once nodes of MGrid are put into operation, they are susceptible to a broad variety of attacks due to the fact that they are often positioned in open space. As a result, it is essential to make certain that the nodes are protected by putting in place a trust mechanism that is dependent on the dependability of the nodes that are located in close proximity to it. Trust is dynamic and varies based on the circumstances. The trust mechanism examines the node's reputation, behavior, and dependability in order to determine whether or not it is malicious. This allows for the discovery of any potentially harmful nodes. When a node's actions, reputation, and general trustworthiness are evaluated in relation to an agreed benchmark, the node's trust value is calculated and decided. The trust model allows trustworthy nodes to communicate and prevents the access of untrustworthy nodes to the network while minimizing the route overhead of the MGrid. The purpose of trust is to enable a secure route from one node to another during a transition.

II. RELATED WORKS

Trust plays a significant role in MGrids because it enables access to potential, scalability, and security for the nodes. For instance, they may investigate the node to determine whether or not it is malicious. A great number of researches have been carried out in order to discover how the trust mechanism in MGrid might be altered to improve its level of safety. This section only examines a handful of different works.

Contemporary design and production processes are becoming increasingly complex, especially due to the rapid expansion of networks. As a result, businesses have an increased need to use and share resources both inside and outside of their organization to meet their business objectives and for international cooperation. For contemporary manufacturing businesses, manufacturing grid offers a networked, trustworthy distribution system [1].

The MGrid completely differs from the conventional traditional grid system a few key ways. The resource is wider, more flexible, and diversified and different.

Resources for manufacturing include tasks like design, software like CAD, hardware and expertise engineers, project managers, etc. The collaborative mechanism is more participatory and responsive to product data. Therefore, issues and challenges related with security are the biggest hurdles to the massive real-life application of MGrid.

Trust defined as identity and action are the two categories trust in the MGrid may be classified. Passwords, certification, and authentication among other methods can be used to establish identity trust. The solo and several domain identity validation approaches are discussed in publications [2] and [3]. However, the main focus of modern trust management is action trust.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 1, pp 55-60, January-2023

https://doi.org/10.47001/IRJIET/2023.701009

A trust evaluation strategy based on entity subject assumptions and object expertise is suggested in literature [4]. When software services collaborate, this method is used to support security decisions. A trust analysis technique that is sensibility-based is suggested in reference [5] to fulfill the assignment of accountability and right.

The cornerstone of trust management is trust evaluation, which primarily entails making recommendations and carefully evaluating trust values. In the manufacturing sector, there are regions for functions and regions for collaboration. We provide a Tree-based Trust management system to put in place the associated trust value calculating mechanism and arrange dispersed cross-domain collaboration in the sector of manufacturing.

A dynamic trust prediction model was published by researchers where it was taken into consideration not just the trustworthiness of a network's current nodes and routes, but also the trustworthiness of the connections that it has had in the past. One model, based on entropy, directly estimated the trust value, while another model, based on probabilities, determined the trust value propagation via various pathways. Both models were based on the same data. A hierarchical trust management system that could take in new information and alter as appropriate in response to changes in the surrounding environment was suggested.

III. PROPOSED WORK

In the proposed research, a multi-cluster configuration for cluster-based MGrid is taken into consideration. When compared to the parameters of the other all nodes found in the cluster, the cluster head has the greatest levels of each cluster's total available parameter's value. This section discusses the presumptions people have about networks, how clusters are established, and how leaders are selected for clusters. Both the Intrusion Detection System and the Tree Based Trust Algorithm, which is used by the system to calculate trust, are described in full.

A) Assumption

1) It is possible to build up Nodes inside of a Cluster-based MGrid.
2) The formation of a cluster of MGrid nodes occurs, each of which has its own unique MG ID.
3) After being sent to a new area as part, nodes stay there in a permanent capacity.

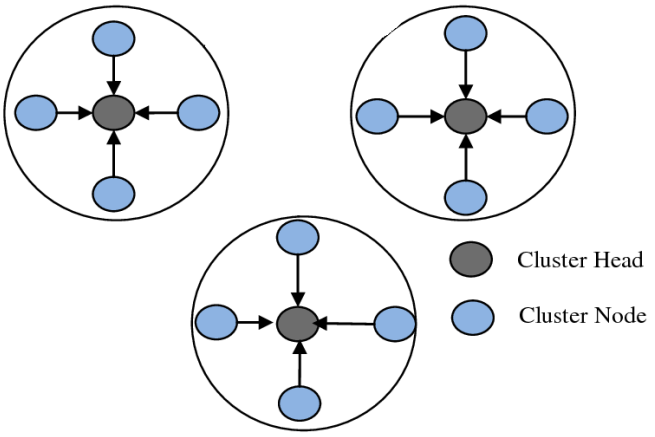

Figure 1: MGrid Nodes - Cluster Formation

B) Cluster Formation

After the all nodes have been established, the following stage is for a number of all MGrid nodes to collaborate with one another and establish a cluster. When analyzing data from several nodes, one method for classifying nodes is based on the distance between those nodes. Nodes are in close proximity have a tendency to congregate together.

C) Cluster Head Selection

Each node is equipped with adequate power to transmit data to another node. Significantly shortening the lifespan of a network is one of cluster head's negative impacts. At the beginning of each communication, it is needed to require to choose cluster head. The improper selection of cluster head results in decreased utilization of resources, which in turn reduces the network's lifetime. In this study, the node that has the greatest feature based on parameters is considered to be the leader of the cluster.

D) Tree Based Trust Algorithm

Our proposed technique calculates trust using a multidimensional trust evaluation technique that is based on a hierarchical trust algorithm. The degree of communication that exists between two cluster heads may be inferred from the level of trust that exists between them. The level of trust that exists between cluster head and MGrid nodes is in its early stages of growth. With the aid of the Tree-Based Trust Algorithm, multidimensional trust in cluster-based MGrids may be securely achieved. In the research that has been given, we make use of three different measures of social trust: honesty trust, content trust, and interactive trust. The malicious node may be easily removed from the network with the assistance of the trust value.

When determining the degree to which other nodes further up the network may be trusted, cluster head takes into

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 7, Issue 1, pp 55-60, January-2023
https://doi.org/10.47001/IRJIET/2023.701009

consideration the ratings that have been assigned to those nodes by other cluster heads that are part of the same cluster. Every single MGrid node in the cluster evaluates the veracity of the other nodes in the cluster and then provides the cluster head with an overall rating for the cluster's trustworthiness.

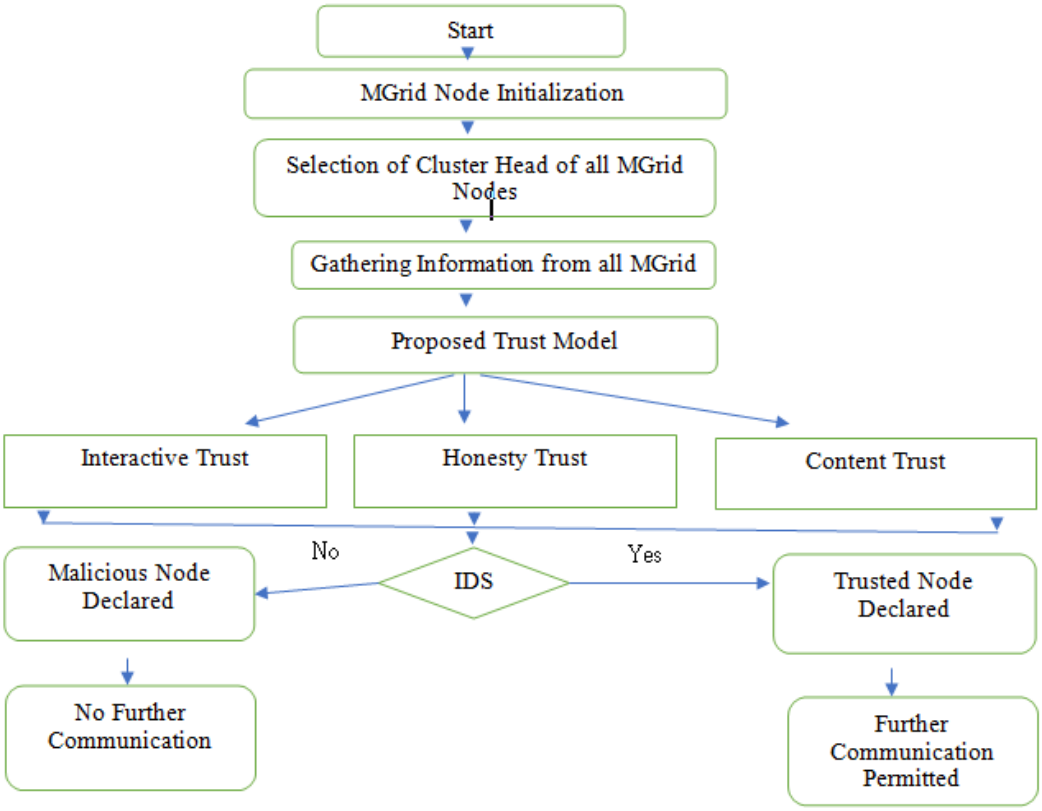

Figure 2: Flow-Process of TBTA -MGrid

Algorithm for calculation of Trust

Input : MGrid Nodes(MG_nodes)

Output : Calculated Value of the MGrid node

Initializing an array for Trust MG nodes and another array for Untrust MG nodes

Trust = [], Untrust = [];

For (i=1 to n)

MG node[i].honesty<-T_i^{honest}

MG node.[i]<-$T_i^{Interactive}$

MG node[i]<-$T_i^{content}$

If(MGnode[i].honesty>-1 && MGnode[i].interactive>=1 && MGnode[i].content>-1)

Trust =i:

Cr=cr+MGnode[i].crate;

Else

Untrust(i) =I;

Endif

MGnode[i]=MGnode(i ,rand(i))

End;

Trust Model

Relationships that are predicated on trust are prone to instability and shift as a result of external factors. It is possible to establish the dependability of individual sensor nodes that have been placed in a MGrid by using social metrics. The value Tij is the total of the confidence that MGridnode j has in the honesty of MGridnode I the confidence that Mgridnode j has in the content of MGridnode I and the confidence that MGridnode j has in the interactivity of MGridnode i. The value of a real number, such as the one that is shown for Tij, might fall anywhere between 0 and 1. When a new MGridnode is added to the existing MGrid environment, its reliability is evaluated for the first time. The trustworthiness of every MGridnode in the MGrid network is evaluated at predetermined intervals by adding up the trustworthiness ratings obtained from each of the node's trust components. The

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 1, pp 55-60, January-2023

https://doi.org/10.47001/IRJIET/2023.701009

following is the methodology that we use to determine the Trust vertices:

$Tij = W1T_{ij}^{honest} + W2T_{ij}^{interactive} + W3T_{ij}^{content}$

Where,

$W1T_{ij}^{honest}$ which represents the honesty trust between MGridnodes i and j

$W2T_{ij}^{interactive}$ represents the interactive trust between MGridnodes i and j

$W3T_{ij}^{content}$ represents the content trust between the MGridnodes i and j.

Since, entire whole of the weights for honesty, interactivity, and context trust is always 1, it can be said that MGrid nodes i and j have a content trust represented equal to (w1+ w2+ w3 = 1).

Interactive Trust

The amount of communication that takes place inside the network serves as the foundation for Interactive Trust. Interaction occurs between two MGridnodes when the first node transfers data to the second node and then gets data from the third node. The node that has the most interactions is considered to be the most dependable. This is the consensus among most experts. For the purpose of determining whether or not a node is malicious, an interactive trust system utilizes a threshold value. The node exchange is evaluated in relation to a restriction that has been established. If it is more than the limit that has been established, MGrid node will be marked as a possible threat to network security and will be barred from taking part in network conversations. Regarding the time t, the interactive trust is denoted by the notation W2T interactive, where I and j are two MGrid nodes that have communicated with one another a certain number of times. Belief in Integrity the sincerity of the trust may be strengthened through interactions of both a good and negative kind. It is considered that a contact has been successful when one node or cluster head is able to effectively send data to either another node or cluster head. In the event that data cannot be sent from one node or cluster head to another, an interaction has been deemed unsuccessful. The reliability of an encounter is directly related to the likelihood that it will be successful.

Integrity in W1T denotes the active participation required in trust. Within the context of an interactive process, the level of trust held between two nodes, I and j, is the defining characteristic of integrity at time t. The value of W1T honesty is set to 1 if node i is able to successfully transmit the data to node j; otherwise, it is set to 0. The maximum and lowest values of a node are both established by the node's capacity to interact with other nodes successfully. This is the trust algorithm that places an emphasis on being honest.

Content Trust

The capacity of a node to supply information is essential to the functioning of this trust paradigm. The Content Trust is monitoring everything that is going on with the node, from the amount of data that is being sent to the other node. When determining whether or not a node is malevolent in terms of content trust, one looks at the capabilities of the node in question. As soon as the node starts transmitting data, it will start using computation processing. In an effort to save resources utilization, nodes will behave like in a self-serving way, which will lead to the gradual reduction of the number of nodes which are malicious may affect the system. When determining how much trust to place in a piece of content that is represented by W3T content, the parameter of a node in respect to the passage of time t is taken into consideration.

E) Intrusion Detection System - IDS

As a result of the way that nodes in MGrid are deployed at random, in the open environment, with limited processing which are more susceptible to being attacked. As a consequence of this, locating rogue nodes is very necessary in order to protect the network from being attacked. Any node that has been determined to be malicious is kicked from the network and is barred from connecting with any other nodes moving forward. The solution that was recommended makes use of a dynamic threshold value where malignant nodes can be identified and detected. The trust value of each node is getting calculated dynamically and then gets compared to a standard that has been established. When a node's behavior starts to put others in danger, that node loses some of its credibility. When compared to a predetermined minimum, the trustworthiness of a node determines whether or not it is malicious.

IV. EXPERIMENTAL RESULT AND ANALYSIS

Our recommended model has been implemented in simulation software and the cluster-based MGrid has been built with a total of one hundred nodes that have been spread out randomly throughout a one hundred by one-hundred-kilometer region. As a first step, we examine each node's data rate in order to establish whether or not it can be trusted. When assessing the reliability of a node, both its highest and lowest throughputs are taken into account simultaneously. It is possible to determine which devices are the most trustworthy based on the trust components and the trust value. During each round, the trust value of each node is investigated at various times to determine whether or not it is trying to do harm. The number of nodes that might possibly do damage has reduced

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 1, pp 55-60, January-2023

https://doi.org/10.47001/IRJIET/2023.701009

as a result of the fact that the node now distributes information based on its trustworthiness.

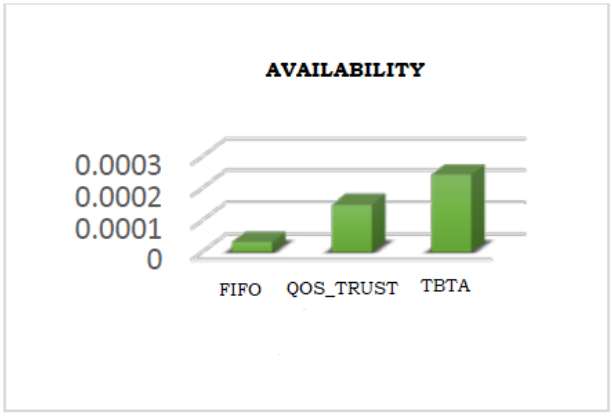

Figure 3: Comparison Availability

The reaction time performance of the average and the number of added tasks, depending on each trust model's response time performance features, is compared in Fig. 3.

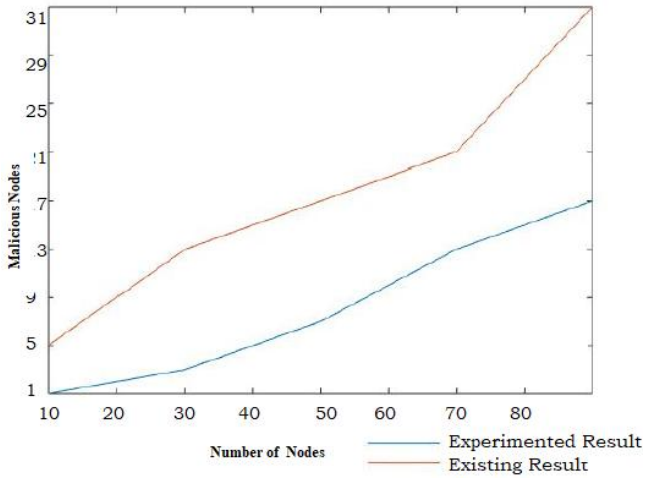

Figure 4: Nodes Vs Malicious Nodes

Each and every MGridnode is having a unique starting trust value in our proposed technique and each round that value is examined and recomputed to determine whether the node is malicious or not. The number of malicious nodes has decreased since the node now sends data or messages based on their trust values. In the Fig.4 compares the decrease in malicious nodes with the current trust model.

V. CONCLUSION

When compared to standard grid applications, Manufacturing Grid has more potential security vulnerabilities because to its spread, heterogeneity, resource sharing, and cooperativity characteristics. The purpose of the research is to enhance MGrid's security. Malicious nodes may be identified by their low trust date rate in comparison to their high dynamic threshold value. In our approach we introduced a completely novel algorithm which evaluates the dependability of each node based on three degrees of trust: honesty, content, and interactivity. Our proposed Tree-based algorithm approach facilitated the management of trust in the manufacturing grid and enhanced resource sharing effectiveness and built a stronger framework for collaboration.

REFERENCES

[1] Fan YS, Zhao DZ, Zhang LQ, Huang SX, Liu B. Manufacturing grid: Needs, concept, and architecture. Source: Gird and Cooperative Computing, pt 1 3032: 653-65, 2004.

[2] W Mao. An identity-based non-interactive authentication framework for computational grids. Hewlett-Packard Laboratories, technical report HPL-2004-096, 2004.

[3] PENG Hua-Xi. Chinese Journal of Computers, 2006, 29(8), 1271-1281.

[4] XU Feng, LU Jian, ZHENG Wei, CAO Chun. Journal of Software. 2003, 14(06), 1043-1051.

[5] CHEN Jian-Gang WANG Ru-Chuan WANG Hai-Yan. Computer Science, 2007, 34(7), 80-83.

[6] Globus Security Team, Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective.http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf, Version 4, September 12th, 2005.

[7] L. Pearlman, V. Welch, I. Foster, and C. Kesselman, A Community Authorization Service for Group Collaboration," Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

[8] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman., "Role-based Access Control Models," Proceedings of the 5th ACM1 Workslop on Role-Based Access Control, 2000, pp. 38-47.

[9] S. Godik et al, "eXtensible Access Control Markup Language (XACML) Vers. 1.1", OASIS Standard, July, 2003

[10] P. Hallam-Baker et al, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)", Oasis Standard, November 5th. 2002.

[11] Marty Humphrey. Mary R. Thompson, "Security Implications of Typical Grid Computing Usage Scenarios", Cluster Computing 5, 257-264, 2002.

[12] Lorch, M., Adams, D. B., Kafura, D., Koneni, M.S. R, Rathi, A., Shah, S., "The PRIMA System for Privilege Management, Authorization and Enforcement in Grid Environments", Proceedings of the Fourth International Workshop on Grid Computing.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 1, pp 55-60, January-2023

https://doi.org/10.47001/IRJIET/2023.701009

Citation of this Article:

Avijit Bhowmick, Goutam Sutradhar, Arup Kumar Nandi, "Proposed Tree Based Trust Algorithm (TBTA) for Manufacturing Grid (MGrid)" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 1, pp 55-60, January 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.701009

****

