Enhancement of Reputation Aggregation based Dynamic Trust Protocols for Edge Computing based E-Health Care System

Mary Subaja Christo (marysubaja@gmail.com)
SRM Institute of Science and Technology

Bommi R M
Chennai Institute of Technology

Anandaraj S P
Presidency University

Udhaya Sankar S M
Velammal Institute of Technology

Anbarasu V
SRM Institute of Science and Technology

Ramkumar G
Saveetha Institute of Medical and Technical Sciences: Saveetha University

Research Article

Keywords: Reputation Aggregation, Edge Computing, e-healthcare, Secured Communication, Reliable Decision

DOI: https://doi.org/10.21203/rs.3.rs-560368/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Abstract

In recent years, E-services such as e-healthcare, e-learning, e-ticketing, depend on computer networks where the attackers have started introducing new types of attacks. Therefore, it is necessary to enhance security for communication which is needed for the transfer of confidential information relating to patients through the network. In our research we have developed a reputation aggregation based dynamic trust model for edge computing based E-health care systems. In this model, the edge node evaluates the trust value of a user and allows the user to access the E-health care system only when the trust value is satisfied. In order to do this, initially the user information is collected with the help of user agents and then this information is processed and the relevant data alone is sent to the edge nodes for evaluating the trust. Finally, the trusted users can be identified through edge nodes and they are only given the permission to access the e-health care system. Attacks generated in the simulations are detected using the prevailing algorithms and also the suggested techniques. The simulation results of this work prove the ability of the proposed techniques which are used to detect the attacks accurately and to prevent them effectively.

I. Introduction

In recent years, Internet technologies have been ubiquitous in day today life for communication, with continuous changes in the lifestyles of the modern Internet users and improvements arising there from. These advancements in lifestyles are the results of invention and usage of wireless networks (WN), mobile computing and web services. Most of the emerging application areas use these networking technologies for Internet usage for providing highly useful facilities and services to people. Among all these services, medical services are the most important in the context of pollution seen in water and problems with air quality which lead to health problems in conditions with diseases of various types spreading and attacking human beings continuously. In such a scenario, it is necessary to introduce new healthcare applications which would have the ability to diagnose diseases through the user interaction with the patients as users to the systems for collecting details relating to the past history of patients and current symptoms for the diseases which are responsible for the health problems.

A healthcare model should behave intelligently by applying rules relating to past data aimed at expecting the upcoming results with previous and current statistics and should handle uncertainty effectively (Sethukkarasi, 2014). A prediction model developed for building a healthcare application meant for monitoring through online discussions can be e-healthcare application. Moreover, such applications are more useful for the patients for getting authentic knowledge relating to their disease in advance. It is also possible to know the details of the treatment provided to them for particular disease on the basis of the analysis of the existing symptoms and also the expert opinions obtained from senior doctors for providing quick and effective remedy. Such e-healthcare applications will be useful also for the physicians as well as helping the performance of the analysis regarding the treatment plan and also to provide more effective treatments leading to fast recovery.
In recent years, different types of computer networks are used for developing e-healthcare applications with effective communication using wired and wireless networks, ad-hoc networks and the Internet. Advancements in the development of new e-healthcare services are seen based on the new paradigm called Peer-to-Peer networks in which the patients are allowed to record their symptoms/medical details to enable obtaining adequate and reliable coordination with other type of networks is rather different in the absence of a centralized administrator for authorizing the users (Nemat, 2011).

The coordination in P2P networks is ensured by the peers themselves. The rapid advancement of this P2P network for developing new healthcare applications is a highly useful paradigm considering the possible cost reduction. Moreover, physicians will be able to post their medical tips relating to the symptoms and analysis pertaining to a particular disease to enable taking appropriate remedial action. Doctors with experience share their knowledge with others and provide advice free of cost. However, security is an important issue in this scenario considering the need to protect the information relating patients, diseases and the doctors who treat patients. Based on the above intention, the reputation model developed which helps the peers to access the system directly with high trust levels. Finally this implementation becomes the key component of the e-health care system portal. In our research we have suggested, a Secure Routing Techniques using Reputation and Packet-Hiding for Wireless Networks has been proposed.

In this model, two techniques, namely, reputation aggregation and cryptographic message hiding have been introduced for enhancing the security of communication in edge computing based E-health care system. Attacks generated in the simulations are detected using the previous techniques and also the suggested techniques. The research has shown in this work prove the ability of the proposed techniques to detect the attacks accurately and to prevent them effectively. Here, peers are also considered as neighbour nodes and the neighbour trust values are used for making reliable decisions on attack detection and prevention.

1.1 Security Based Wireless Network

Network communication using WN is subjected to several kinds of hackers (Baptiste Pretre, 2005) actively participated in Internet era. Even though many types of new types of attacks are introduced by attackers most frequently, some of the known attacks such as worm propagation, relational attack, file poisoning, Sybil attack, DOS attack and Man in Middle attack (Yu et al 2008) and eclipse attack are also more serious. Therefore, it is necessary to apply more efficient techniques to detect these attacks and to prevent them. However, the existing WN networks provide some potential security services (Shane Balfe et al 2005) including integrity, control of access, authentication, confidentiality and non-repudiation by applying known security algorithms based on cryptography, key management techniques and soft computing techniques.

Disregarding the presence of numerous techniques and procedures for maintaining the security in networks, Client Server model and Internet have implemented by the Conventional algorithms. In present form trust and safeguarding are more challenges in Wireless Networks. Therefore, new protocols which
consider the features of WN networks must be designed and implemented to protect the resources and data from attackers. One of the major issues with the design of the solution using a centralized networking system is that the node failure in the network is fault tolerant but the centralized coordinator failure will lead to the failure of the entire system. In WN, each node is enhanced the security with help of certification authority (CA). Therefore, the transaction carried by attacker node so, the certificate produced by the malicious node to perform the transaction in the particular site of the computer network. In such a scenario, a transaction may need more number of certificates involving multiple certification authorities to perform authentication.

In most of the WN, All nodes are segregated into different clusters if the number of nodes is higher and the group size is bigger. This partitioning is performed on the basis of certain parameters namely distance, trust value and past history. Each node should belong with a member of one group or more than one group through logical membership. This helps to identify the users perfectly and avoid the involvement of attackers from the malicious peers. The certification authority method is used for providing the certificate to the group of nodes and the individual nodes which nodes are attached to the CA. Moreover, all the nodes which are involved in the group or outside of the group members can able to accesses the certificate from the corresponding authority nodes by group head node or individual node.

Here, Digital Signature method has provided the group authority to all the nodes which are stored in a database which is located at the node which acts as the group authority. All the credentials provided by the peers are authenticated by the group authority and issued to the group members. The group authority doesn't record the information pertaining to other group members and hence it is not possible to verify the certificates without the support of the corresponding certificate authority as discussed by Arulkumar et al (2012).

1.2. Trust Management System

Trust management is a most significant factor at the same time it's become a difficult perception in security systems. In the real world, faith supports the individuals to create suitable judgements by using the trust values so that even in unpredictable circumstances, it is possible to make decisions with confidence by reducing the uncertainty (Qin et al 2009). Many distributed systems are suffering from attacks by malicious nodes which are irregular in addition to undefined objects which attempt to cooperate with all other in order to attack the genuine users. Trust is important to move with people in common life. In a social environment, trust management helps to make collaborative decisions by trusted members. Similar to this, a number of nodes are present in a network and identifying the trusted nodes among all the peers is a toughest job. Moreover, due to the presence of a large number of possible threats in the varying networking applications always depends on the Distributed System (DS) and the trust value of those system is complex one due to the varying nature of participating nodes (Xiong and Liu 2004).

Research on trust management schemes is undertaken by many researchers who work on security systems and social network analysis for edge Computing. In such systems, the essential components
include trust modelling framework, trust management policies design and implementation and the application of the trust model to security systems (Hayam Mousa et al 2015). Most of the authentication techniques goal is to progress collaboration through the participants either in the form of nodes or applications in a distributed system. They work by predicting the future behaviours of peers based on their past and present behaviours. Therefore, a trust management scheme must perform the following tasks in this way the system can provide effective facilities to the application domain. First, each node in the network must observe and store the behaviour of its peer nodes also called neighbouring nodes. Second, each node must collect the behavioural characteristics of peer nodes and such data must be stored in their databases including the details regarding notices, intelligences received from reaming peers regarding their neighbouring nodes information. Next, all the peer’s must calculate their historical confidence values regarding their behaviour and maintain information based on the collected reports and they must be stored for all neighbouring nodes. Finally, the current trust score must be computed with help of the historical faith, current rules and their rules usage the faith values, and then by assigning suitable weights for information received from other nodes. Therefore, it is possible for each node to decide the finest peer or cluster of peers to join the wireless network system.

2. Literature Review

Hui Li has proposed a Configurable Online Reputation Aggregation System. This protocol helped to discuss the global issues with help of rating information, which is collected from the different peers. This rating information is used to validate the node efficiently than reputation values. The rating data collected from several systems are aggregated to develop a local reputation. The entire aggregated local reputation is then converted into global reputation. This aggregation is performed on the basis of options as well as weights that are chosen by the querying agent based on the system requirements (Li and Hui, 2008).

Gupta et al have proposed the Differential Gossip technique to the Reputation Aggregation method in P2P network. In the power law network, the trust values from various nodes are aggregated without identifying the power nodes and by using the aggregation mechanism. Since node identification is not required, it is possible to have quick implementation of the approach as node identification is a hard task to avoid. The reputation aggregation is performed in a differential method by taking into account the feedback from nodes that have increased weight. This makes the approach more robust towards collision and avoids the free riding issue (Gupta R et al, 2015).

Zhao et al have suggested effective routing in Wireless Networks by Self-Organized Tree-Based Energy-Balance routing protocol. In the above model, they have implemented a tree model which is used to keep up the hierarchy of the data. They have chosen a particular node as a Root node from the tree which has low mobility and high energy, each node has been connected with their neighbour’s node so the root node can easily broadcast the data’s to every other nodes. All the nodes have been mutually connected to every other node in the network with help of root nodes. The simulation results have shown this model has high energy and enhances the network lifetime through the network (Han et al 2014).
Selvi et al have proposed an efficient data collection method with new group based energy efficient routing methods established with help of covering the LEACH algorithm. Here, they have added the extension of fuzzy rules which is used to give the new techniques for data collection and take the decision in routing. This algorithm helps to form effective cluster based routing with help of fuzzy temporal logic rules, here they have introduced new cluster head one is primary cluster and another one is secondary cluster these clusters are used for gathering the records then forward these data to their neighbour's nodes. They have proved the group based forwarding techniques provides efficient performance with simulation tools (Selvi et al, 2017).

Trong-Thua Huynh et al have proposed a new and distributed clustering model to accomplish group based forwarding for reducing the energy consumption and delay in Wireless Sensor Networks (WSN). In this protocol, the author has found the cluster head from the regular nodes and this cluster head used to perform the multi-hop routing here the cost of each path is estimated by the parameters such as distance from the neighbor node, energy consumption, distance from the cluster heads, reliability in throughput and packet delivery. This protocol is mainly used to find the cost from one node to another node. The authors have carried out the experiments using the existing work on cluster based routing and also their proposed model with their proposed cost function. Using the experiments conducted by the authors, this model has provided more efficient in terms of energy efficiency and reduction in delay. The perfection of this work has shown the usage of cost is very low in their proposed work (Trong at al, 2016).

Ren et al have suggested a new energy balanced protocol for routing in WSNs. The goal of this model is to find the distance from the particular node to the base node with a low level of energy by automatically, so the key gain of this algorithm is used to find the distance at a very low level of energy consumption. Moreover, the authors have addressed the routing loop problem present in the basic algorithm by providing enhancements used for detection and elimination of the loops. They carried out experiments using the basic algorithm and the extended algorithm through simulation. Their experiments proved that their model which eliminates the loop increased the network lifetime and balanced the energy. Finally, their model enhanced the coverage ratio and throughput as well (Ren et al, 2012).

Xiumin Wang et al have developed a new geographic routing protocol called K-any_cast routing protocol for effective routing in WSNs. In their model, they have performed a guaranteed delivery of packets at least in K-different destinations. The main advantage of their model was its performance of both local optimization and global optimization. With help of optimization, we can select the next hop. The process was repeated at all nodes to make a global optimization algorithm. The node's information share to all other nodes by flooding method and the author has proved the efficiency with simulation results (Wang et al, 2012).

Zeynab Molay Zahedi et al have proposed a new routing algorithm which uses swarm intelligence and fuzzy rules for performing effective routing in WSNs. Their model is considered as the residual energy, the distance of the node to the sink, and the distance of the node from the respective cluster centroids. In this model, cluster centroids have been used for making decisions on clustering while fuzzy logic was used
for handling the uncertainty present in the WSN environment. The authors have made efficient use of fuzzy input and output variables efficiently and handled the uncertainties effectively. This algorithm provides efficient routing from one node to another node and it has very less complexity to implement the protocol and provide high network security to the network. However, the presence of attackers will also lead to a high packet drop ratio. Hence, it is necessary to measure the trust of nodes and to perform routing only through the trusted nodes (Zeynab et al, 2016).

Farahani et al have proposed IoT based e-Health care system with fog-driven methodology. The use of IoT and Fog computing can be useful for e-health and medical services and quality. This system used for monitoring the patient remotely through IoT devices the device sensed the data and store in Fog computing methods which is provided the high computing storage medium for sensed data (Farahani et al, 2018). Yang et al have proposed Self adaptive access control system for health care application with IoT devices, here Privacy and security for health systems can be enhanced with advanced encryption algorithms. Fusion between IoT, big data and security for health systems is essential (Yang et al, 2019).

Kaur et al have enhanced secured privacy health care system with block chain based cloud storage application, here Block chain can be used to enhance security and privacy for health care systems and services to higher levels application (Kaur et al, 2018). Shi et al have enhanced the study about Smart Medical Application with RFID security system. This study helps to understand the advantages of Ethical concerns together with threats and ways for protections should be reinforced for security in smart medical areas (Shi et al, 2019).

In some networking systems, the trust management schemes used for security maintenance allow trust redemption in order to allow a participating node to regain the trust of its neighbours if it is lost in the previous communications. For example, in a WSN (Idris Abubakar Umar et al, 2017) which is composed of a set of sensor devices which are constrained by available resources is an area of research where trust based routing is essential due to the presence of unreliable radio as the medium for wireless communication. In such a scenario, there exists a great possibility that unintentional temporary communication errors might occur leading to delay and increased packet dropping. The behaviour of a node is measured based on the success probability in sending the packets to other nodes which are routed through this node.

When a node performs routing with high delay and increased packet dropping ratio due to network congestion or non-availability of bandwidth will also be treated as a bad node. Therefore, it is necessary to distinguish between malicious nodes which drop the packets intentionally and the genuine nodes which drop the packets unintentionally. A good trust management system which identifies the genuine nodes and malicious nodes perfectly is the necessity of the routing protocols which are used in WSN for performing secure routing. Therefore, increase in false positive rate by the detection algorithm will reduce the trust of genuine node and take alternate and longer routes leading to increase in energy consumption, delay and bandwidth utilization. Such a system must have separate security policies based on rules,
access control, authentication techniques (Chuang et al 2014) and key management schemes helps to enhance the security level and the performance of the system.

The Next type of schemes includes fault detection and management schemes. Such systems allow a redemption scheme in which the security system may avoid a faulty detection of misbehaving nodes as genuine or an erroneous identification of a genuine node as malicious node. Such a redemption scheme in the security algorithm using trust modelling will provide further opportunities to the genuine nodes which are affected due to failure by non-availability of energy. This will help to recover the trusted nodes and make them to participate in the routing activities by highlighting the node failure as a cause for delay and hence such nodes will be allowed to continue in the group of trusted nodes and their behaviours will be tested by excluding the delay occurred during the failure of the node. Therefore, fault tolerant routing schemes are proposed by many researchers who are working on providing optimal and secure routing protocols for WSNs.

In spite of the presence of many existing redemption schemes for WSNs, the existing schemes are more suitable for only WSN in which all routing activities are carried out to send the nodes information to the root station through the sensor peers. In such applications, cluster based routing protocols played a major role in performance improvement. However, the cluster based routing protocols are more suitable for WSNs in which the nodes and the base station are static or the nodes and the base station or mobile. Mobility based networks will lead to change of groups by members. In such a scenario, group of the head node will be designated dynamically by selecting a node with high values of energy, low mobility and high trust as the cluster head. Such a trust based model which considers node distance, energy level, and mobility speed and trust values is more suitable for providing a secure routing protocol to the WSNs.

On the other hand in a P2P network, to create the effective results we don't bather about the distance from the source node to the base system and the energy level between these systems. Moreover, the cost of removing a node from the group is different in WSN when it is compared with P2P networks. Hence, it is essential to progress a original and well-organized trust management scheme which is more suitable for providing secure routing in P2P network is highly important and it must be a secured routing protocol.

Trust evaluation techniques can be developed in different methods. Among all the methods, most of the existing techniques follow the different types of the trust they are direct trust and indirect trust. In this direct trust the behaviour of the nodes information and the period of time have computed. This is more reliable since it is computed directly and is not based on the opinion from other nodes. On the other hand, indirect trust is computed by consolidating the opinions obtained from the neighbour nodes. This measure will be more useful when the neighbour nodes are genuine and impartial. If one of the neighbour nodes is a malicious node, then the opinion given by that node will be different from the opinions given by all other nodes. This can be neglected either by taking the average value or by considering only the majority opinions. If more than one malicious node is present in the network, a group will be formed by malicious nodes and they will be collectively destroying the reputation of genuine nodes. In such a scenario, more intelligent algorithms must be developed and careful analysis must be carried out.
If one node tries to influence other node in collaborative decision making, such nodes should be monitored and eliminated so that it is possible to increase the true positive rate. This research work attempts to increase the true positive rates by proposing a rumour riding protocol which will coordinate with the trust model in this direction this proposed model has given authenticated communication between the networks.

2. Proposed Work

In this research paper, we have suggested a reputation aggregation based dynamic trust model for edge computing which helps to secure the wireless network for e-services. In wireless networks, all the nodes are connected to one node to another node with radio waves and the access points. Initially, we formed the clusters of nodes with Fuzzy logic through the mobility, energy level, and the base system distance like we could form the clusters from the wireless network. Then, we used the Reputation algorithm to find the nodes’ trust value with the help of the Reputation table. We had collected all the node information from one node to another node through their neighbor’s and the values were stored in the reputation table based on the trust value we had chosen from the cluster head. The trust values were calculated in relation to the number of messages that node had sent to other nodes and also based on the time span that the node had been active in the network based on the parameters found in the trust value of all the nodes. Further, one node was chosen as cluster head whose trust value had become high. Finally, the authentication of valid user by dynamic trust model for edge computing was made with the aid of cluster head. The cluster received the notification from the reputation table so the head of the cluster had gathered the nodes data through reputation table and verified the trust level of that requested node whether it had trusted. Moreover this algorithm was used for providing enhanced security to information sharing and communication activities related to e-healthcare applications in the Wireless Sensor networks. So, our proposed system had followed these three steps:

1. Forming the clusters with Fuzzy logic
2. Finding the Cluster head with Reputation Aggregation algorithm
3. Authenticating the user by cluster head with dynamic trust model for edge Computing.

From Fig 1, we can easily recognize the stream of our proposed method. We had chosen a highly secured routing protocol so that the cluster node then selected the cluster head and finally the cluster head gave the access control to the requested node that had been using the e-health care application. Here all the e-services applications had been depending on the wireless network in this network. One of the nodes was sending the request to use the health care application so that requested node trust level had to be verified by dynamic agents. To verify the requested node first the details of that node such as user name, password, and trust level of the node had been collected and all these information were stored in the reputation table. Later, the user agents sent the notification to the head of the cluster node. Then, this node had also checked the user name, password and trust value of that requested node.
Finally, comparison was made between this information and reputation table information in order to determine whether both the information had the same cluster head and give the access permission to the requested node. In this way, we carried out a secured routing protocol for e-services such as e-health care applications.

3.1. Form the clusters with Fuzzy logic:

There had been an assumption of the network consisting of individual nodes which were grouped into a single cluster with all the nodes having the same energy level. These nodes were positioned randomly and grouped into clusters on the basis of the distances and energy levels that had been varied as a result of increase in communication. The distance was calculated from the current node to the root node with help of time and distance factors. Moreover, one among the nodes in their cluster which had high energy and least distance with other nodes had been elected by each of those clusters and the selected node was considered as the cluster head which was used for communicating with other clusters as well as with the own group. The head node collects the node’s information and forwarded to other nodes in the tree. This algorithm also used fuzzy rules for performing clustering and re-clustering of the nodes.

The new group formation and cluster head established routing model developed in this work had used a probabilistic threshold value that was found having application in taking decisions on clustering instead of using a normal predefined threshold value to make decisions with respect to the categorization of the nodes. Here, the cluster head election was carried out periodically, starting from the first communication in which initial clusters had been formed and was repeated on the basis of the available energy and distance for performing further communication. Fuzzy information was used in this work for effective choice of the cluster heads in the network by handling uncertainty more effectively. Moreover, the non-cluster head nodes called member nodes were found to have performed the task of joining the existing cluster head nodes.

The threshold value for making decisions was computed by using equation 1

\[ N_{th} = \frac{CC}{(1-CC \times (r \mod \frac{1}{CC}))} \] (1)

Where \( r \) was number of iterations, \( CC \) was probability selection of cluster head

Fuzzy Logic based Cluster Formation Algorithm

Step 1: The threshold Value for each group was determined.

Step 2: Initial Threshold value was considered as a Cluster head.

Step 3: Each and every random node for finding the threshold was considered randomly.

Step 4: It was ensured whether the threshold of random nodes had been lesser than the threshold, in the context where had been was lesser, then cluster head was assigned temporarily after checking the radius using if—then rules.
Step 5: The radius value was calculated with degree of the node and remote of the node.

Step 6: The specific peer (S) as a head of the group (cluster) and sent the message to their neighbour connected nodes.

Step 7: Other node K on the network received the message from node S.

Step 8: If $T_{Score}(K) > T_{Score}(S)$ then

Step 9: Considered the node K as cluster head.

Step 10: K node is one of the member of cluster list CM.

Step 11: Applied fuzzy rules which are framed on the basis of the distance for finalizing the cluster head from CM.

Step 12: All the nodes were shown cluster wise.

In this system, the temporary head node had been formed through the fuzzy rules. The responsibility of fuzzy rules are find the temporary cluster head and create the connection between one temporary cluster with other cluster head with help of the radius values and the distance of these cluster head values. Moreover, the proposed system used three linguistic variables for finding the ratio of the nodes which also consisted of close, medium and far with extension to include more variables for forming the fuzzy rules. This model also considered the trust scores called the current credit scores of the node for enabling taking the final decision. We computed the ranges from one node to another node with help of valuable input and linguistic variables. Another contribution of this work was that a third variable called degree of the node which had been introduced in the decision making process to confirm the improvement of the accuracy of the decisions. The fuzzy variables are used to find the distance from degree of the node to the base station is as follows:

1. Distance$_{BS}$ – (Very_close, medium_close, close, medium, far, very_far)
2. Degree of the Node – (very low, very high, medium, low, high)

The fuzzy output variable was used to form the cluster with respect to the temporary cluster head. We had used nine different linguistic parameters to find the temporary cluster they were low, very-low, far, very-far, medium, close, medium-close, high and very high been used for finding the nodes degree and used to find the distances between one node to other nodes.

**3.2 Select the Cluster head with Reputation Aggregation algorithm:**

The reputation value of the node was adjusted in a reputation table when had received fresh information related to the trust value of its neighbour nodes. The trust value of the inviting node was checked with its reputation table, when a node had requested its neighbouring node for resources. The resource was allocated on the basis of the trust value of the requesting node. Based on the requests, the received nodes
checked the trust value of the requested peer. The trust value of that requested node had been easily tracked whenever the requested node was the neighbour of received node. In addition to that, the trust value of the requested node had to be checked in the reputation table with help of the overall information whenever that requested node was not a neighbour node. Finally, we could find the trusted requesting node with help of estimated trust values.

In this research work, a reputation aggregation algorithm was performed with edge computing based algorithms. In this proposed technique, each node of the network had shared the information with a set of its neighbour nodes. The received information was shared with its remaining neighbour nodes. Thus, each node had received different trust values for a specific trusted user through edge computing network. Then, the aggregated value of a node was tested for convergence. The node was declared trustworthy and no more aggregation was required when the convergence condition had been satisfied. In Fig 2 shows how the cluster head was formed from the clusters..

The reputation aggregation mechanism has been described in algorithm 1.

**Notations:**

- \( i \): Node
- \( j \): Node
- \( q \): Degree of the node
- \( f_{bi}^j \): Feedback of \( j^{th} \) node estimated by the node \( i \)
- \( gw_{ij} \): Gossip weight of \( j^{th} \) node estimated by the node \( i \)
- \( \text{Convergence}_{value} \): Converging value

**Algorithm 1:**

1. Step 1: During gossiping, each node had randomly chosen a node from its neighbourhood and shared some basic information with it.
2. Step 2: The received information was stored by the receiving node.
3. Step 3: The \( i^{th} \) node is estimate the neighbour degree by the data's received from all the neighbouring nodes
4. Step 4: Each node had randomly chosen \( q \) nodes from its neighbourhood, and then pushed some information into those neighbours.
Step 5: Based on the feedback of other nodes, the $i^{th}$ peer saved the values on the table and forwarded its response with the enduring nodes.

Step 6: The overall reputation value of every node was evaluated by the receiving responses of other surrounding nodes.

Step 7: Whenever $i$ node received feedback from $j$, then

\[ j, \text{fb}_{ij} \text{then } g_{wij} = 1 \]

Step 9: The cost of $\text{fb}_{ij}$ and $g_{wij}$ had been documented by every node in the status of Aggregation chart and was measured as a conversation pair.

Step 10: During every gossiping step, the ratio of the gossip pair depicted by equation (3.2.1) had been estimated to determine the convergence value and was recorded.

\[
\text{convergence value} = \frac{\sum_{i=1}^{\infty} \text{fb}_{ij}}{\sum_{i=1}^{\infty} g_{wij}} \tag{3.2.1}
\]

Step 11: The value of $q$ was rounded off to the nearest integer value and had sent

\[
\left(\frac{1}{q+1}\text{fb}_{ij}, \frac{1}{q+1}g_{wij}\right) \tag{3.2.2}
\]

as the gossip pairs to all the $q$ nodes.

Step 12: Determine the gossip pair values.

The convergence cost as predictable from equation 3.2.1 and had been tested with respect to predefined fault endless. Whenever the convergence condition had been satisfied, then the gossiping process was stopped or else it was continued. When the node $i$ had stopped gossiping, it announced among its neighbours that it had achieved convergence. Thus, the valid nodes were detected and recorded as trustworthy based on the reputation aggregated through gossiping.

3.3. Dynamic trust:

Trust scores were computed for each node participating in the edge computing network. All the participating nodes in each cluster send the ‘Hello’ message to all the neighbour nodes. These nodes had increased their destination score on the basis of the acknowledgements received by the nodes. All the participating nodes calculate not only their trust scores but also their neighbour node’s trust values dynamically. Here, a node had been capable of measuring the trustworthiness of other nodes during any
particular interval of time for taking decisions on communication to that node dynamically. Likewise, the suggested model was used to check the trust administration of the developing secured e-services such as e-health care, e-learning, etc. in which the system used to check the user whether the user is an authenticated user or not.

Fig 3 shows the steps to find the authenticated node in health care system. This System describe the characteristics of the trusted node finally the cluster header has given the access to the user node if that node has high accurate level otherwise the access has been blocked by the cluster head node. The following algorithm 2 describes the steps to validate the user nodes. The user agent collects the information from the requested node then this information is stored in edge nodes for computing the trust values. With the help of this dynamic trust, the user can be authenticated. After validation, the authenticated user can use e-health care system and finally check these data with reputation trusted table for verification process these steps are repeatedly performed to check the trust value of the requested node.

**Algorithm 2:**

Step 1: The user (Patient/Doctor) gave the request to access the e-health care system in wireless network

Step 2: The user agent had collected the user name and password then stored it to the private cloud database and forwarded to the cluster head to validate that requested node.

Step 3: The head node (cluster) had accepted the documents from the database and verifies the trust value of the requested node with help of reputation aggregation algorithm.

Step 4: If the node had a high trust value it was identified as the authenticated node and permission was given to access the e-health care system.

Step 5: If the node had low confidence rate it was identified by the attacker and couldn't access the e-health care system, it was inferred that cluster head had blocked those nodes from access the e-health care system.

This proposed Reputation Aggregation Algorithm based Edge Computing Dynamic Trust Method (RAA-DT) had been implemented by providing extension to the existing AODV protocol for performing the routing process in the network.

Figure 4 has shown the architecture of the proposed system. This RAA model was used to identify the attacker nodes in the current network. Finally, fuzzy rules had been used in this work for taking effective decisions over the presence and identification of malicious nodes. In this work, a new e-healthcare application was used to validate the algorithms proposed for performing secured communication.

Finally, we developed secured emerging applications including medical and healthcare systems with help of a secured protocol Here, fuzzy rules and rule based decision making with respect to routing decisions
had been incorporated in this work for effective routing. Moreover, rules had been used in this work for network monitoring and the system was tested using a healthcare application. From the experiments conducted in this work using flat routing and cluster based routing, routing through all nodes and routing through trusted nodes, it was proved that the new suggested algorithm delivered increased network presentation in terms of increase in reliability, packet delivery ratio and throughput with reduction in delay.

4. Results And Discussion

NS2 Simulator is used to implement the proposed routing algorithm. We have implemented the basic routing protocols of AODV and AOTDV and the existing protocols compared the proposed protocol. We have taken the parameter such as packet drop ratio, malicious detection accuracy, Delay analysis and Throughput analysis. Our network topology is depends on the time and mobility of the nodes speed. Here, the speed of the mobility will high when the time is set as small. The mobility of the speed will decrease when the time is set as high. The performance of the proposed protocol is compared with the base protocol in the presence of attacker nodes and finally the simulation results have shown that the proposed protocol finds the malicious nodes in high accurate rate and it is possible to block those types of malicious nodes with help of dynamic reputation trust algorithm for edge computing network. Therefore, with the help of proposed model we can implement efficient wireless network for e-services such as e-health care system. Table 1 displays the trust score values of proposed protocol (RAA-DT) and the existing protocols, Ad-hoc Distance Vector and AOTDV protocol.

Table 1: Trust Scores for clusters

| Total Nodes | Cluster Nodes | Score of Trust Score |
|-------------|---------------|----------------------|
|             |               | AODV | AO-TDV | RAA-DT |
| 150         | 10            | 71.2 | 78.4   | 87.5   |
| 250         | 15            | 67.3 | 79.3   | 88.3   |
| 350         | 20            | 56.5 | 80.7   | 82.6   |
| 450         | 25            | 52.5 | 79.8   | 89.5   |
| 550         | 30            | 63.2 | 74.5   | 79.6   |
| 650         | 35            | 62.8 | 84.6   | 90.6   |
| 750         | 40            | 64.5 | 73.7   | 89.7   |
| 850         | 45            | 61.3 | 80.3   | 90.5   |
| 950         | 50            | 68.8 | 81.2   | 89.8   |
| 1050        | 55            | 63.7 | 86.8   | 91.5   |
Table 1 shows the proposed method of RAA-DT trust scores are gradually increased and it has high scored trust values when compared with existing models such as AODV and AO-TDV protocols. This increase in performance is based on the fuzzy rules used by the proposed system for clustering reputation aggregation model for trust computation and rules for making effective decisions. From Table 2 we can understand the time delay between proposed protocols and the base protocols such as RAADT-AODV and AODV, AOTDV techniques. Here the proposed model shows the less delay time in milli seconds (ms) responses and the base protocols such as AODV and AOTDV protocol takes more delay time to reach the destination nodes.

Table 2: Delay Analysis

| Algorithms                  | Number. Of Packets Sent |
|-----------------------------|-------------------------|
| Delay-AODV(ms)              | 5000        8000        11000        14000        17000        20000 |
| Delay-AOTDV(ms)             | 0.795       2.89        3.98         4.21         4.72         4.54   |
| Delay - RAADT-AODV (ms)     | 0.54        1.55        2.34         2.87         3.11         3.79   |

Fig 4 displays the drop ratio of the packets. The proposed algorithm has high security access so it has less drop ratio when compared with the base protocols with minimum and maximum malicious contents of the nodes with different times.

From Fig 5 we can understand the proposed algorithm has less number of packet drop ratio when compared with other existing protocols. Here in X axis represents the number of Packets sent with the scale of m/s and Y axis represents the packet drop ratio. Here, the simulation results shows if the proposed algorithm RAADT-AODV sent 20000 packets the packet drop ratio has detected only 3.9 percentage only but the existing algorithm has detected 7 and 4.9 percentage respectively and the it has gradually increase when the packet size will be increased.

Figure 6 displays the detection accuracy analysis with malicious nodes; the proposed protocol RAADT Shows the detection accuracy is very high when compared with the existing protocol as AODV and AOTDV protocol.

Figure 6 indicates the Detection Accuracy Analysis of the existing and proposed algorithms with different number of Malicious Nodes. The X axis represents the number of malicious nodes and the Y axis represents the scale of Detection Accuracy in percentage. The proposed protocol RAAD has high detection accuracy rate with different kinds of the malicious nodes but the existing protocols such as AODV and AOTDV shows very low detection accuracy rate when the existing algorithms compared with the proposed protocol of RAADT-AODV with different number of malicious nodes. This owes to the routine of smart rules, fuzzy rules, reputation with dynamic trust based proposed methods. We can easily detect the malicious nodes with help of fuzzy temporal logic rules.
Figure 7 indicates the delay time for the existing and proposed algorithms with different number of the mobility nodes; In X axis represents the number of mobility nodes the speed of the node is represented by (m/s) and the Y axis represents the scale of delay time represented in the scale of. The proposed protocol RAAD has less delay time in all possible mobility nodes but the existing protocols such as AODV and AOTDV shows high delay time when it compared with the proposed protocol of RAADT-AODV with different mobility speeds. This owes to the routine of smart rules, fuzzy rules, reputation with dynamic trust based proposed methods. We can easily detect the malicious nodes with help of fuzzy temporal logic rules.

Figure 8 leads the throughput analysis performance for the existing and proposed algorithms with different speed of the mobility nodes; In X axis represents the number of mobility nodes and the Y axis represents the scale of throughput values. The proposed protocol RAAD has high throughput value in all possible mobility nodes but the existing protocols such as AODV and AOTDV shows very low throughput values when it compared with the proposed protocol of RAADT-AODV with different speed of the mobility nodes. This owes to the routine of smart rules, fuzzy rules, reputation with dynamic trust based proposed methods. We can easily detect the malicious nodes with help of fuzzy temporal logic rules. In this work, we have successfully implanted high secure based e-health care services for users without any involvement of attackers.

5. Conclusion And Future Works

In this research work, a reputation aggregation based dynamic trust model with edge computing has been recommended to secure the wireless network for e-services based applications. In addition, Reputation Aggregation based Dynamic Trust model has the ability to perform effective authorization for the users with trust value of that requested node and helps to form the clusters among all the nodes in Wireless Network. This algorithm is used for providing enhanced security to information sharing and communication activities related to e-healthcare applications in the Wireless networks. The proposed system has been designed and formulated in three steps, firstly the clusters had been formed among all the nodes utilizing Fuzzy logic, secondly the cluster head with reputation aggregation algorithm was formed and finally the user had been authenticated by cluster head with edge computing model. The simulation result effectively proves the ability of the proposed techniques to detect the attacks accurately and to prevent them efficiently than the existing counterparts. The experiments conducted validate the proposed reputation aggregation based dynamic trust model with edge computing to be more efficient than the conventional model of ADOV protocol. On the whole, the proposed model provides secured communication that caters to the need of futuristic emerging applications such as e-health care, e-learning, e-ticketing services.

Declarations

We hereby declare that we are the sole author’s of this article. To the best of my knowledge this article contains no material previously published by any other person except where due acknowledgement has
been made.

**References**

Li, Hui. "A configurable online reputation aggregation system." PhD diss., University of Ottawa 2008. 1910-2010, http://hdl.handle.net/10393/27998,http://dx.doi.org/10.20381/ruor - 12344

Gupta R, Singh YN. Reputation aggregation in peer-to-peer network using differential gossip algorithm. IEEE Transactions on Knowledge and Data Engineering. 2015 Apr 29;27(10):2812-23. DOI: 10.1109/TKDE.2015.2427793

Han, Z., Wu, J., Zhang, J., Liu, L. and Tian, K., 2014. A general self-organized tree-based energy-balance routing protocol for wireless sensor network. IEEE Transactions on Nuclear Science, 61(2), pp.732-740. DOI: 10.1109/TNS.2014.2309351

Selvi, M., Nandhini, C., Thangaramya, K., Kulothungan, K. and Kannan, A., 2017, January. HBO based clustering and energy optimized routing algorithm for WSN. In 2016 Eighth International Conference on Advanced Computing (ICoAC) (pp. 89-92). IEEE. DOI: 10.1109/ICoAC.2017.7951751

Huynh, T.T., Dinh-Duc, A.V. and Tran, C.H., 2016. Delay-constrained energy-efficient cluster-based multi-hop routing in wireless sensor networks. Journal of Communications and Networks, 18(4), pp.580-588. DOI: 10.1109/JCN.2016.000081.

Liu, A., Ren, J., Li, X., Chen, Z. and Shen, X.S., 2012. Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks. Computer Networks, 56(7), pp.1951-1967. https://doi.org/10.1016/j.comnet.2012.01.023

Wang, X., Wang, J., Lu, K. and Xu, Y., 2012. GKAR: A novel geographic K-anycast routing for wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 24(5), pp.916-925. DOI: 10.1109/TPDS.2012.143

Zahedi, Z.M., Akbari, R., Shokouhifar, M., Safaei, F. and Jalali, A., 2016. Swarm intelligence based fuzzy routing protocol for clustered wireless sensor networks. Expert Systems with Applications, 55, pp.313-328. https://doi.org/10.1016/j.eswa.2016.02.016

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, 659-676. https://doi.org/10.1016/j.future.2017.04.036.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Information Sciences, 479, 567-592. https://doi.org/10.1016/j.ins.2018.02.005
Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of medical systems, 42(8), 156. https://link.springer.com/article/10.1007/s10916-018-1007-5.

G. Ramkumar & Logashanmugam, E.. (2018). Hybrid framework for detection of human face based on haar-like feature. International Journal of Engineering and Technology(UAE). 7. 1786-1790. 10.14419/ijet.v7i3.16227

Shi, X., Cao, J., Lu, T., & Chang, V. (2019, May). A Survey on RFID Security and Privacy in Smart Medical: Threats and Protections. In IoTBDS (pp. 278-285). https://www.scitepress.org/Papers/2019/77134/77134.pdf

Ganapathy, S., Sethukkarasi, R., Yogesh, P., Vijayakumar, P. and Kannan, A., 2014. An intelligent temporal pattern classification system using fuzzy temporal rules and particle swarm optimization. Sadhana, 39(2), pp.283-302. https://link.springer.com/article/10.1007%2Fs12046-014-0236-7.

Banerjee, A., Neogy, S. and Chowdhury, C., 2012, November. Reputation based trust management system for MANET. In 2012 Third International Conference on Emerging Applications of Information Technology (pp. 376-381). IEEE. DOI: 10.1109/EAIT.2012.6407975

Chuang, M.C. and Chen, M.C., 2014. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications, 41(4), pp.1411-1418. https://doi.org/10.1016/j.eswa.2013.08.040

Govindaraj, Dr & E, Logashanmugam. (2018). Study on impulsive assessment of chronic pain correlated expressions in facial images. Biomedical Research. 29. 10.4066/biomedicalresearch.29-18-886

Geetha G, Jayakumar C, "Implementation Of Trust And Reputation Management For Free-Roaming Mobile Agent Security", IEEE Systems Journal, Vol. 9, No. 2, pp. 556-566, June 2015. DOI: 10.1109/JSYST.2013.2292192

Hai Lin, Lusheng Wang, and Ruoshan Kong, "Energy Efficient Clustering Protocol for Large-Scale Sensor Networks", IEEE Sensors Journal, Vol. 15, No. 12, pp. 7150-7160, December 2015. DOI: 10.1109/JSEN.2015.2471843

Zhu, H., Du, S., Gao, Z., Dong, M. and Cao, Z., 2013. A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks. IEEE Transactions on Parallel and Distributed Systems, 25(1), pp.22-32. DOI: 10.1109/TPDS.2013.36

Govindaraj, Dr & Logashanmugam, E.. (2019). Multimodal verge for scale and pose variant real time face tracking and recognition. Indonesian Journal of Electrical Engineering and Computer Science. 13. 665. 10.11591/ijeecs.v13.i2.pp665-670
Mousa, Hayam, Sonia Ben Mokhtar, Omar Hasan, Osama Younes, Mohiy Hadhoud, and Lionel Brunie. "Trust management and reputation systems in mobile participatory sensing applications: A survey." Computer Networks 90 (2015): 49-73. https://doi.org/10.1016/j.comnet.2015.07.011

Deebak, Bakkiam David, Fadi Al-Turjman, Moayad Aloqaily, and Omar Alfandi. "An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT." IEEE Access 7 (2019): 135632-135649., https://ieeexplore.ieee.org/abstract/document/8839043

Vijayakumar P, Pandiaraja P, Karuppiah M, Deborah LJ. An efficient secure communication for healthcare system using wearable devices. Computers & Electrical Engineering. 2017 Oct 1;63:232-45. https://doi.org/10.1016/j.compeleceng.2017.04.014

**Figures**

![Reputation Aggregation with Dynamic Trust Model](image)

**Figure 1**

Systematic View of Reputation with Dynamic Mode
Figure 2
Cluster head Formation

Step 1: Send Request to access E-Health Care System

User Interface Agent

Step 2: Collect the User Information

Step 3: Store the information to the cloud

Edge Computing

Step 6.1: Access given by cluster head if user trust value is high

Step 6.2: Access Block by cluster head if user trust value is low

Authentication Agent / Cluster Head

Step 4: Request to verify the user

Step 5: Check the Trust value of the User

Reputation Table

| Node Name | Neighbour Node | Trust value |

Figure 3
Functionality of Identify the Trust User by Dynamic Trust
Figure 4

Architecture of Reputation Based Dynamic Trust System

![Diagram of the Architecture of the Reputation Based Dynamic Trust System](image-url)
Figure 5
Packet Drop Ratio for RAADT-AODV with malicious node

Figure 6
Detection Accuracy Analysis

Figure 7
Throughput Analysis

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- AuthorsPictureandBiography.doc