Biomedical Research 2017; Special Issue: S394-S400 *ISSN 0970-938X*
www.biomedres.info

An intelligent fuzzy beta reputation model for securing information in P2P health care applications.

Mary Subaja Christo[1*], Meenakshi S[2], Subhashini R[3]

[1]Research Scholar, Sathyabama University, India

[2]Department of Information Technology, Jeppiaar SRR Engineering College, India

[3]Jeppiaar Maamallan Engineering College, Chennai, India

Abstract

Medical is an important emerging field today in this polluted environment. Health care applications are most useful for the society in the fast world. Health care applications are launched and providing services through all kind of networks such as wireless networks, ad-hoc networks and peer-to-peer networks. Health care applications contain all kinds of secret information about the diseases, patient details and the physician recommendation for the particular patient. In this scenario, security is very important for all kinds of networks to secure the secret information which are shared through the health care applications. For providing security to the emerging applications such as medical, we propose a new secure routing protocol called Intelligent Fuzzy Beta Reputation Model based Ad-hoc On-demand Distance Vector (IFBR-AODV) routing protocol for effective communications in networks. Here, we have used intelligent agents and fuzzy rules for making effective decisions on users during monitoring process in networks. Every health care application users (nodes) and their activities are monitored by the administrator (cluster heads).

Keywords: Wireless networks, Intelligent fuzzy beta reputation model based ad-hoc on-demand distance vector, Beta reputation model, Health care applications.

Accepted on January 18, 2016

Introduction

Today, networking technologies or internet technologies are leading to provide the smart services to the people. Lifestyles of the people are gradually changing in the past two decades due to the enhancement of wireless networking technologies such as mobile computing, cloud computing and mobile cloud computing. Many emerging fields are utilizing these technologies and provide more facilitated services to the public. Among them, medical field is the most emerging today in this polluted world due to the introduction of new diseases every day. It is necessary to introduce the new prediction model (e-healthcare applications) for identifying the diseases as early as possible before affecting the people severely. E-healthcare applications are very much useful for knowing their disease status, the details about the remedial actions for the particular disease by giving the symptoms, physician guidance and for knowing the status of their disease. In addition, these e-healthcare applications are necessary to assist the physicians also for making effective decisions over the diseases based on the given symptoms.

The latest years are endorsing the advancement of a new e-healthcare service paradigm called Peer-to-Peer (P2P) [1] in which patients are entering their symptoms/medical detail and getting sufficient information from the system/application. Is there no centralized administrator for authorizing the users in between these two activities. The rapid advancement of this new healthcare application paradigm is because of the reduction in costs. On the other hand, physicians can post their medical tips for avoiding the particular disease and remedial actions have to be taken. They can provide the information as free of cost or they may charge for their advice. However in this scenario, it is crucial to protect the information of patients and medical doctors. For this reason, the so-called reputation models aimed at assessing the direct trust levels of peers during trade transactions are becoming a key architectural component of any e-health service portal.

Network security is also becoming very complex task today due to the rapid growth of internet users and increasing the volume of information shared in through the network. Most of the emerging services such as e-governance, e-commerce, e-learning and e-healthcare are working in computer networks only. It is necessary to ensure the security of the secret information which is transferring through the network. Protocols are playing major role for transferring the information/data from source node to destination node in any networks. Specially, in ad-hoc networks such routing protocols

in different when compared with routing protocols in wired networks such as Local Area Networks (LAN), Wide Area Networks (WAN) and Metropolitan Area Networks (MAN). Routing protocols in ad-hoc networks are classified into three namely proactive routing protocols, reactive routing protocols and hybrid between the proactive and reactive routing. The table driven protocol is an alternate name of a proactive routing protocol such as Destination Sequence Distance Vector (DSDV) which is each node only to aware about the next node to the sink and also aware how many nodes away the sink. This information are stored in node and formed as table, hence the term "table driven routing", while the reactive protocols such as Ad-hoc On-demand Distance Vector (AODV) Routing protocols. If a node wants to communicate with another one node which it has no route, the routing protocol will try to establish such a route. The AODV protocol works based on the Route Request Message (RREQ) and Route Reply (RREP). Is there any error occurs during the communication is Route Error (RERR) and it will be sent to the source node.

In this paper, a new Fuzzy Beta Reputation and dynamic Trust Model is proposed and implemented for effective communication in P2P healthcare services in networks. Moreover, it calculates the dynamic trust value by using the direct and indirect trust and beta reputation trust for providing secure communication. In addition, a new intelligent fuzzy cluster formation algorithm is also introduced for improving the performance of the healthcare service. Rest of the paper is organized as follows: Section 2 discusses various secured routing protocols proposed by many authors in the past. Section 3 explains the proposed work. Section 4 provides the results and discussion. Section 5 gives conclusion and future works.

Literature Survey

There are many works have been done by various researchers in this direction in the past. Among them, Pujol et al. developed a model for extracting reputation in multi agent systems using communication with other users [2]. Josang and Ismail proposed a beta reputation system for developing a trust based system [3]. Ganeriwal et al. developed a new reputation-based framework for high integrity sensor networks. Their model is useful for maintaining integrity in communication [4]. Qin et al. proposed a new architecture for trust management in communication using effective methods for channel allocation and routing in wireless networks [5]. Zhu et al. introduced an authenticated trust and reputation model for cloud and sensor networks integration [6]. Das and Mohammad proposed a new secured trust framework which is dynamic in nature and is useful for trust computation and secured communication [7]. Dang et al. developed a new clustering and cluster-based routing protocol for delay-tolerant mobile networks [8]. Xie and Xiaohua developed a transmission-efficient clustering method for Wireless Sensor Networks using compressive sensing [9].

Sethukkarasi et al. proposed a new medical diagnosis system for identifying the dead diseases by using the fuzzy temporal cognitive map [10]. Their system is useful for identifying the diseases dynamically. Ganapathy et al. proposed a new fuzzy temporal min-max algorithm for identifying the dead diseases like diabetic and heart diseases [10]. They also used particle swarm optimization algorithm for optimizing the features.

Lin et al. developed a cross layer reputation model which is based on reliable recommendation and privacy preserving for providing secure communication in wireless networks [11]. Moosa and Mahdi proposed a botnet detection system which considers both misbehaving activities and the past data about group coordinating activities in the network [12]. Their system is capable of identifying the bot-infected hosts which perform few misbehaving activities in the attack stage. Next, to participate in some coordinated group activities of the botnet detection lifecycle. Moreover, they introduced a new negative reputation system for tracking suspected nodes in the network and also compute a negative reputation score for confirming the participation in group activities. Finally, they build a new prototype of BotGrab for demonstrating how it works in the real network like a P2P. EdyPortmann et al. show the way for analysing the reputation system further. In addition, they also introduced a new framework which is based on fuzzy logic to gain deeper perceptions into an online reputation system [13].

Kurdi developed a new reputation system called HonestPeer which is enhanced version of the EigenTrust algorithm for calculating the global reputation scores of other peers [14]. The proposed algorithm is used to select the most important nodes, honest peers, dynamically based on the quality of the files. Mousa et al. addressed the sensing systems which are working based on trust [15]. In addition, they proposed a new classification framework of these systems. Moreover, a depth analysis can be done for each type of these systems. They also concluded that the trust based system performance is not up to the mark when compared with reputation systems. Moreover, they presented a general analysis and comparative analysis is also made between the latest trust mechanisms. Finally, they justified the importance of the reputation system for secure communication in networks.

Pecori investigated the possible countermeasures and also proposed a new technique for performing the routing operation and the storage and retrieval of resources in a Kademlia network more secure through the use of a combined trust based algorithm exploiting reputation techniques [16]. Finally, their solution provides a balanced mixing of standard Kademlia algorithms and trust-based algorithms showing promising results in thwarting a Sybil attack in a Kademlia network, in comparison with similar methods as well. Ferrer et al. demonstrated the advantages of reputation systems which provide artificial incentives that can compensate negative payoffs, thereby constructing co-utility still manageable [17]. Especially, the Eigen Trust mechanism is adapted and extended for obtaining a general distributed reputation management protocol that can be applied to a variety of scenarios and reputation needs. Moreover, their system provides a key tool for designing the self-enforcing protocols which are useful for ensuring the secured communication.

EigenTrust (Kamvar 2003) is a famous and accepted structure for reputation management in networks. This paradigm calculates the trust score by adding the successful transactions with each source (peer) and regularizes it over all its nodes (peers) [18]. In addition, it computes the reputation score of every peer by aggregating the trust scores assigned to this node by other nodes (peers) and weightage also assigned based on the reputation of each peers. The trust values are shared in the peer-to-peer network by using a Distributed Hash Table (DHT) [19]. Xiong et al. introduced a new trust paradigm for peer-to-peer network to overcome the disadvantages of the standard EigenTrust paradigm in governing the man in the middle attack [20]. Moreover, their paradigm uses overlay for trust broadcast and public key infrastructure for securing trust scores. In addition, they introduce the concept of opinion creditability to cumulative the global reputation. Muneeswari et al. proposed an intelligent data gathering and energy efficient routing algorithm for Mobile Wireless Sensor Networks [21]. Logambigai and Kannan proposed a Fuzzy logic based unequal clustering for wireless sensor networks [22].

In spite of the presence of available literature, the security and routing issues are to be improved still further due to the presence of delay and security issues in the present in wireless networks. Therefore, a new reputation based routing protocol is proposed in this paper for performing effective routing in networks and thereby improving the performance in terms of reduce the packet loss.

Proposed Work

In this paper, we propose a new cluster formation algorithm using fuzzy logic for grouping the nodes effectively in networks. In addition, a new intelligent fuzzy beta reputation model is also proposed in this work for authorizing the users. These two algorithms are useful for providing security to the information of e-healthcare applications in peer-to-peer network services.

Intelligent fuzzy cluster formation

The peer-to-peer network system model consists of different individual nodes which are organized to track a topology in a network. In this work, we assume the network comprises of individual nodes and also have same energy level, all nodes are positioned arbitrarily, the distance between nodes is calculated based on their request and the base station is located inside the network. The nodes in the network form a group (cluster) with different number of nodes. All these clusters are also had separate cluster head for communicating with other clusters. The cluster head gathers the information (data) from its cluster members, compresses and forwards the compressed data to the base station. The proposed algorithm is used to form an effective clustering. Here, a probabilistic threshold value is used instead of normal predefined threshold value for categorizing/grouping the nodes. Cluster head election is also conduct for selecting cluster head in each group (cluster). Fuzzy variables are used for selecting cluster head in the network. Next, the non-cluster head nodes are joining with the cluster head nodes. The threshold value is fixed by using the Equation 1.

$$N_{th}=CC/(1-CC^{*}(r \bmod 1/CC))$$

where r is number of iterations, CC is desired percentage of cluster head (e.g. CC=0.05).

Intelligent agents are used for performing the cluster formation in this work. The proposed Intelligent Fuzzy logic based Cluster formation algorithm used fuzzy rules for making effective decisions over the threshold setting and finalize the distance.

Intelligent fuzzy logic based cluster formation algorithm

Step 1: Decide the threshold value for each group using intelligent agents.

Step 2: Initial Threshold value is considers as a Cluster head.

Step 3: Consider each and every random nodes for finding the threshold randomly.

Step 4: Check whether the threshold of random nodes is less than the threshold, if less than then cluster head is assigned temporarily after checking the radius using fuzzy rules.

Step 5: Find the radius based on the node degree and distance

Step 6: The particular node (S) can send the cluster head message to their neighbour nodes

Step 7: Other node K on receiving the cluster head message from node S

Step 8: If T_Score (K)>T_Score (S) then

Step 9: Other node K is considered as cluster head for the range.

Step 10: Add K in to the cluster member list CM.

Step 11: Apply intelligent fuzzy rules which are framed based on the distance to finalize the cluster head from CM.

Step 12: Display the cluster members in cluster wise.

In this work, the fuzzy rules are used for computing the radius of every temporary cluster head node. To find the radius of nodes, the proposed system uses two linguistic variables based on the base station and the current credit score of the node. The fuzzy input variables and its linguistic variables used for competition radius computation are given below. The third variable Node degree is newly proposed in this work.

Distance-BS-(Very-close, medium-close, close, medium, far, very-far)

Node Degree-(very low, low, medium, high, very high)

The trapezoidal membership function is used for boundary variables and triangular membership function is used for intermediate variables. The fuzzy output variable is competition radius of the temporary cluster head. The nine linguistic variables used for output variable are very close,

medium close, close, medium, far, very far, very low, low, medium, high and very high for finding the distance between the nodes and base station and also finding the node degree.

Fuzzy beta reputation system using dynamic trust

In this work, an Intelligent Trust model called Fuzzy Beta Reputation and Dynamic Trust (FBRDT) is proposed for effective secure communication. Here, we have used the fuzzy logic based cluster formation for applying beta reputation trust model. The proposed beta reputation system is also the combination of dynamic trust and the beta reputation system. The dynamic trust value is calculated for each participating nodes in a cluster.

Dynamic trust: The trust score is calculated for each and every participating node in a network. First, all the participating nodes are sending the Hello message to the neighbour nodes. Based on their acknowledgement, the particular node will increase the destination score. All the participating nodes are calculated their neighbour node trust values dynamically. Here, any particular time interval can measure the trustworthiness for taking decision over the node dynamically. Similarly, the proposed protocol used e-healthcare applications check the users whether they are authorized person or not.

Beta reputation model: Beta reputation model is functioning based on the trust. The most used method to map with the observed information from the evidence space to the trust is the beta distribution. Let p and n indicates the total number of positive feedbacks and the total number of negative feedbacks in the evidence space. The trust worthiness of a subject node is then computed by using the Equation 2.

$ts=P+1/N+P+2 \rightarrow (2)$

The Dynamic Trust (DT) value is calculated by using the Equation 2 and time intervals starting time and ending time. Here, starting time means when the simulation process started and ending time indicates the end of the simulation process.

DT=Dynamic Trust (ts, $<t_1, t_2>$) → (3)

Where, t_1 indicates the starting time of the simulation process and t_2 indicates the ending time of the simulation. In real time scenario, the *t1* and t_2 can be fixed by the administrator and calculate the DT value. Based on the present dynamic trust (DT) value the users can be allowed to access the healthcare applications if the person is authorized otherwise will not be allowed for accessing the healthcare applications.

The proposed fuzzy beta reputation score is the combination of Dynamic Trust (DT) score and the Beta Reputation Trust score. Here, fuzzy rules are also used for forming a cluster. Fuzzy Beta Reputation model is used for calculating the Beta Direct trust value using intelligent agents. Here, the intelligent agents are using for monitoring the node trust during particular time duration dynamically. The proposed Fuzzy Beta Reputation System shows the characteristics of each and every individual node as a binary event. This binary event is modelled by the beta distribution which is commonly used to represent the posterior probability of a binary event using intelligent agents. Dynamic Trust and Reputation of each node is evaluated by the features provided by the Beta distribution that acts as a basis. The beta family of Probability Density Functions (PDF's) is set of continuous function indexed by two parameters α and β. In beta reputation system, α is assigned as the number N_p of positive ratings plus 1 and β is assigned as the no N_n of negative ratings plus 1. Initially dynamic trust is the expectation of positive behaviour from a node. In future interactions, the trustworthiness value is calculated using the Equation 4.

$$\frac{\alpha}{\alpha+\beta} = \frac{N_P}{N_P + N_n + 2} + DT \rightarrow (4)$$

p indicates the decay factor or forgetting can be applied to assign more weightage to new ratings and gradually the older ratings are decreased.

Fuzzy Beta Reputation and Dynamic Trust value is computed using the Equation 5.

$$FBRDT = \frac{P+1}{N+P+2} + \frac{dP+1}{dN+dP+2} + DT \rightarrow (5)$$

FBRDT is the combination of dynamic trust and Beta Reputation Trust. The proposed Fuzzy Beta Reputation model is used for calculating the beta trust score dynamically. The proposed algorithm consists of a trust based secure routing algorithm which is works in three phases such as trust evaluation, threshold and routing based on the trust values. The proposed model focuses on two major aspects such as Beta Reputation and Dynamic trust based secure routing. The steps of the proposed dynamic trust based secure routing algorithm are as follows:

Dynamic trust based secure routing algorithm

Step 1: Let TRv (n_1, $n_2 ... n_m$)=0//*TRv* indicates Trust Value, n_1, $n_2 \ldots n_m$ are nodes.

Step 2: All the nodes are considered as source node $S_i$in$<t_1, t_2>$

Step 3: S_n send messages to their neighbour nodes

Step 4: *HC=HC+1*

Step 5: Initiate the scheduler class to execute the simulation

Step 6: If Received the request from neighbour nodes Then

Ensure that the node $S_i$is destination node

Else If S_i is destination Then

Node S_i sends the acknowledgement to its neighbouring nodes.

Step 7: Calculate the trust score ts for all the nodes using Equation 2.

Step 8: Calculate the dynamic trust score DT for all the nodes using Equation 3.

Step 9: Calculate the overall trust score t_s for all the nodes using Equation 4.

Step 10: Apply fuzzy rules for fixing the Threshold value.

Step 9: IfMin (Tkc)<Threshold then

Detect the malicious node

Else

Update the routing table with new node

Step 12: Perform the routing process using AODV

The proposed secure routing algorithm is incorporated with AODV protocol for perform the routing process in the network. Moreover, beta reputation model is used to identify the malicious nodes in the network. In addition, fuzzy rules are useful for making effective decisions over the malicious nodes. In this work, e-healthcare application is used this proposed protocol for secure communication.

Results and Discussion

For simulating the proposed routing protocol, NS2 (Version 2.34.1) has been used. The AODV routing protocol is used for all simulation and the simulation parameters. The topology of the MANET depends on the pause time and mobility speed and also it changes its topology frequently when pause time is less and mobility speed is more. The performance of Ad-hoc on demand Trust based Distance Vector (AOTDV) protocol in presence of malicious node is compared with the performance of proposed technique in this work.

Table 1 shows the trust score differentiation between the proposed FBR-AODV protocol and the existing protocols such as AODV and AOTDV.

Table 1. *Average trust score in percentage for clusters.*

No. of nodes	No. of clusters	Trust score (%)		
		AODV	AOTDV	FBR-AODV
100	5	71.2	78.4	87.5
200	10	67.3	79.3	88.3
300	15	56.5	80.7	82.6
400	20	52.5	79.8	89.5
500	25	63.2	74.5	79.6
600	30	62.8	84.6	90.6
700	35	64.5	73.7	89.7
800	40	61.3	80.3	90.5
900	45	68.8	81.2	89.8
1000	50	63.7	86.8	91.5

From this Table 1, it can be seen that all the trust score value of the proposed FBR-AODV protocol gradually increases when it is compared with the existing algorithm namely AODV and AOTDV. This is due to the fact that the use of intrusion detection system feedback in the proposed model and also due to the fuzzy clustering.

Table 2 shows the delay analysis of the proposed system and the existing protocols namely AODV and AOTDV.

Table 2. *Delay analysis.*

Algorithms	No. of packets sent					
	6000	8000	10000	12000	14000	16000
Delay in AODV (ms)	0.7	1.8	2.9	3.2	3.4	3.7
Delay in AOTDV (ms)	0.695	1.79	2.89	3.12	3.27	3.54
Delay in FBR-AODV (ms)	0.54	1.55	2.34	2.87	2.91	3.12

From this table, it can be seen that the performance of the proposed system is better when it is compared with the existing systems such as AODV and AOTDV.

Figures 1 and 2 show the packet drop ratio in existing protocol and proposed trust based protocol with the maximum and minimum number of malicious nodes presence in the network.

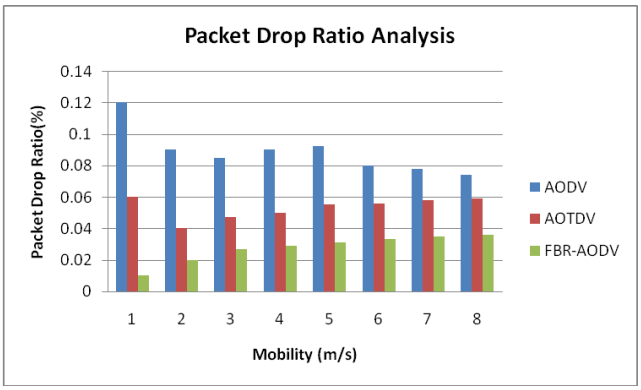

Figure 1. *Packet drop ratio for FBR-AODV with malicious.*

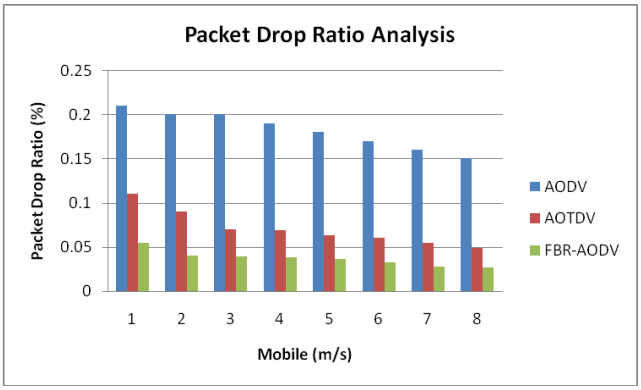

Figure 2. *Packet drop ratio analysis.*

From this Figure 1, it can be observed that the packet drop ratio gradually decreases in this proposed FBR-AODV when it is compared with AODV and AOTDV with the minimum number of malicious nodes are present in the network. From Figure 2, it can be observed that the packet drop ratio also decreases in this proposed FBR-AODV when it is compared with AODV and AOTDV with the maximum number of malicious nodes present in the network.

Figure 3 shows the overall network performance of the proposed FBR-AODV protocol with the presence of malicious nodes and the existing protocols such as AODV and AOTDV protocols with the presence of malicious nodes.

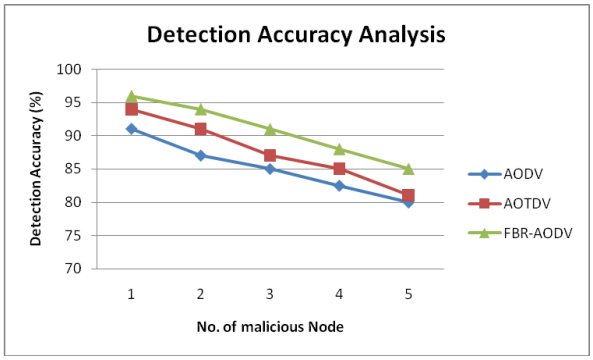

Figure 3. *Detection accuracy analysis.*

From Figure 3, it can be seen that the proposed FBR-AODV protocol with malicious nodes perform well when it is compared with the existing protocols such as AODV and AOTDV. This is due to the fact that the use of beta reputation mechanism, fuzzy rules and intelligent agents.

Figure 4 shows the delay analysis of the proposed FBR-AODV protocol and the existing protocols namely AODV and AOTDV.

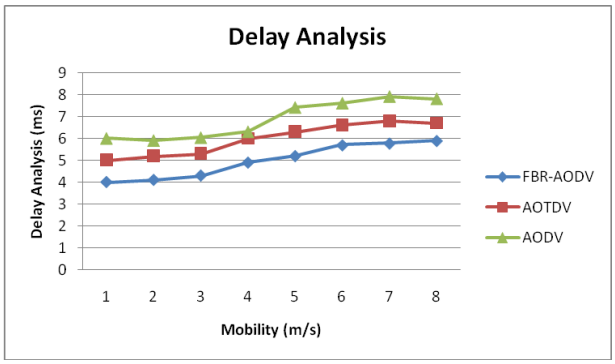

Figure 4. *Delay analysis for FBR-AODV.*

From Figure 4, it can be seen that the delay analysis of the proposed FBR-AODV protocol is less when it is compared with the existing protocols namely AODV and AOTDV. This is due to the fact that the use of beta reputation system, fuzzy rules and intelligent agents for effective malicious node detection.

Figure 5 shows the throughput analysis for the proposed system and the exiting protocols namely AODV and AOTDV with different mobility speeds.

From Figure 5, it can be observed that the throughput analysis of the proposed FBR-AODV protocol is better than the existing protocols such as AODV and AOTDV with different mobility speed. This is due to the fact that the use of intelligent rules, fuzzy rules, dynamic trust and beta reputation model. These are very much useful for detecting malicious nodes effectively in this network. In this work, the peer-to-peer healthcare service application is successfully running without any interruption in the network.

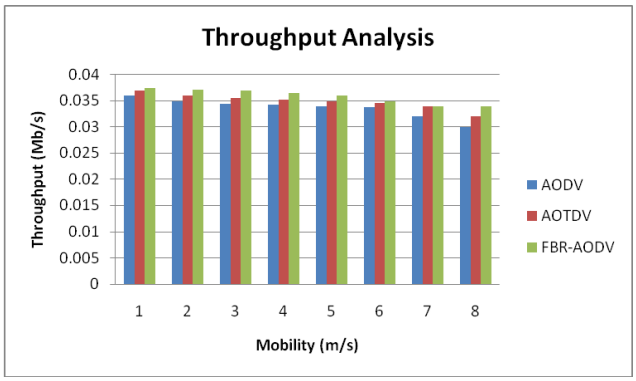

Figure 5. *Throughput analysis.*

Conclusion and Future Works

In this paper, a new Fuzzy logic based Beta Reputation model based AODV routing protocol has been proposed and implemented for secure communication in networks. In addition, a new fuzzy logic based cluster formation algorithm also introduced for effective clustering and dynamic trust score is also calculated for finding the beta trust score for finalizing the malicious nodes over the networks. Moreover, fuzzy rules are used for making effective decision over the malicious nodes while performing the routing process. From the experiments conducted for the proposed fuzzy beta reputation model based secure routing algorithm, it has been shown that the dynamic trust, reputation calculation and management helps to perform secured communication in wireless networks by enhancing the security, throughput, packet delivery ratio and by reducing the delay. Through the secured communication, all kinds of emerging applications including healthcare applications are able to perform well by using this new protocol in terms of security. Future works in this direction can be the use of fuzzy rough set theory to handle uncertainty effectively in the peer-to-peer health care services.

References

1. Nemat R. Taking a look at different types of e-commerce. World Appl Prog 2011; 2: 100-104.
2. Pujol JM, Sanguesa R, Delgado J. Extracting reputation in multi agent systems by means of social network topology. Proc 1st Int Joint Conf Auton Agents Multiagent Syst 2002; 467-474.
3. Josang M, Ismail R. The beta reputation system. Proc 15th Bled Electron Commerce Conf 2002; 324-337.
4. Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks. ACM Transact Sens Netw 2008; 4.
5. Qin T, Yu H, Leung C, Shen Z, Miao C. Towards a trust aware cognitive radio architecture, ACM SIGMOBILE Mobile Computing. Commun Rev 2009; 13: 86-95.
6. Chunsheng Z. An authenticated trust and reputation calculation and management system for cloud and sensor

networks integration. IEEE Trans Inform Forens Secur 2015; 10: 118-131.

7. Anupam D, Mohammad MI. Secured trust: a dynamic trust computation model for secured communication in multiagent systems. IEEE Trans Depend Secur Comput 2012; 9: 261-274.
8. Dang H, Wu H. Clustering and cluster-based routing protocol for delay-tolerant mobile networks. IEEE Trans Wirel Commun 2010; 9: 1874-1881.
9. Ruitao X, Xiaohua J. Transmission-efficient clustering method for wireless sensor networks using compressive sensing. IEEE Trans Parall Dist Sys 2014; 25: 806-815.
10. Ganapathy S, Sethukkarasi R, Vijayakumar P, Yogesh P, Kannan A. An intelligent temporal pattern classification system using fuzzy temporal rules and particle swarm optimization. SADHANA Proc Eng Sci Spring 2014; 39: 283-302.
11. Hui L, Li X, Yi M, Wei W. A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing, Fut Gener Comp Sys 2015; 52: 125-136.
12. Moosay, Mahdi A. BotGrab: A negative reputation system for botnet detection. Comp Electr Eng 2015; 41: 68-85.
13. Edy P, Andreas M, Philippe CM, Witold P. FORA–A fuzzy set based framework for online reputation management. Fuzzy Sets Sys 2015; 269: 90-114.
14. Heba AK. HonestPeer: An enhanced Eigen-trust algorithm for reputation management in P2P systems. J King Saud Univ Comp Inform Sci 2015; 27: 315-322.
15. Hayam M, Sonia BM, Omar H, Osama Y, Mohiy H, Lionel B. Trust management and reputation systems in mobile participatory sensing applications: A survey. Comp Netw 2015; 90: 49-73.
16. Riccardo P. S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia. Comp Netw 2016; 94: 205-218.
17. Josep DF, Oriol F, Sergio M, David SJC. Self-enforcing protocols via co-utile reputation management. Inform Sci 2016; 367-368.
18. Kamvar SD, Schlosser MT, Garcia-Molina H. The EigenTrust algorithm for reputation management in p2p networks. Proc 12th Int Conf World Wide Web 2003; 640-651.
19. Lua EK, Crowcroft J, Pias M, Sharma R, Lim S. A survey and comparison of peer-to-peer overlay network schemes. Commun Surv Tutor 2005; 7: 72-93.
20. Xiong L, Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans Knowl Data Eng 2004; 16: 843-857.
21. Jothimuneeswari S, Ganapathy S, Kannan A. Intelligent data gathering and energy efficient routing algorithm for mobile wireless sensor networks. As J Inform Technol 2016; 15: 921-927.
22. Logambigai R, Kannan A. Fuzzy logic based unequal clustering for wireless sensor networks. Wirel Netw 2016; 22: 945-957.

*Correspondence to

Mary Subaja Christo

Research Scholar

Sathyabama University

India