A NEW DYNAMIC TRUST SECURE ROUTING IN WIRELESS SENSOR NETWORK

R. Chitra, M.Sc.,(Maths), PGDCA, B.Ed., M.Sc., IT., M.Phil (CS)
Assistant Professor, Department of Computer Science, MCA and IT & Applications,
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

P. KavithaPrincy
Research Scholar, Department of Computer Science
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

Abstract

Networking technology is playing a major role in daily life for communicating each other. Security is the most important issue in wireless networks.Recently, trust and reputation mechanisms are used for providing security throughmonitoring the behavior. However, the existing works lack in providing reliablesecurity to wireless networks. In this paper, we propose an intelligent dynamic trust model (IDT) for providing security in wireless networks.This model is the combination of dynamic trust and beta reputation trust forsecure routing in wireless networks.

Keywords: Wireless Network, Secure Routing, Dynamic Trust Model, IDT (Intelligent Dynamic Trust)

1.   Introduction

Wireless networks are useful for sharing knowledge and information mutually in this real world. Rapid growth of this computer network utilization and securityissues are also increasing simultaneously due to the huge number of users. Moreover,wireless networks consist of a large number of nodes without physical connection.The applications of wireless networks such as medical, computer security, defense and surveillance are useful and essential component of human life.Moreover, the data gathered by the nodes are forwarded and routed to the basestation either directly or through neighbouring nodes. In such a scenario, each nodeof the network is capable of

providing service within their transmission range. In wireless networks, data are gathered from nodes and are sent to the base stationwhich is called as the sink node.

In wireless network, trust specifies the reliability or trust worthiness of node. Trust mechanism can be classified in different ways based on how the trust valuesare calculated. Trust is subjective based on individual node behaviour in a group ornetwork. Trust mechanism is classified into two: namely direct and indirect trustmechanisms [1]. Direct trust is considered as a basic opinion about the particular node.

Indirect trust is considered as a second opinion which is collected from someother nodes that are located as neighbour. Direct trust values are calculated betweennodes. Indirect trust values are calculated between the node and neighbour nodes.Dynamic trust mechanism is helpful to know the current trust value of the particularnode in ad hoc networks [2]. Moreover, trust and reputation are multidisciplinaryconcepts with different definitions and evaluations in various fields [3, 4].

In this paper, a new intelligent dynamic trust model (IDT) is proposed and implemented for effective communication in wireless networks.The proposed system calculates the dynamic trust value by using the direct trust for providing secure routing.

2.   Proposed Methodology

In this work, an intelligent trust model called intelligent dynamic trust (IDT) is proposed for effective secure communication. A widely used way to map the observed information from the evidence space to the trust space is the beta distribution. Let s and f represent the total amount of positive and negative feedbacks in the evidence space about target entity, then the trust worthiness t of a subject node is then computed as,

$$t = s + 1/f + s \qquad \text{Eq. (1)}$$

DyT = Dynamic Trust (t, <t1,t2>)

IDT is the combination of Dynamic Trust (DyT).Intelligent Dynamic Trust model is used for calculating the beta direct trust valueusing intelligent agents. Here, the

intelligent agents are used for monitoring thenode trust during particular time duration dynamically. The proposed intelligentsystem demonstrates the behaviors of each individual node as abinary event. This binary event is modeled by the distribution which iscommonly used to represent the posterior probability of a binary event usingintelligent agents. Dynamic trust model of each node is evaluated by thefeatures provided by the beta distribution that acts as a basis. The family ofprobability density functions (PDFs) is a set of continuous function indexed by twoparameters α and β. In beta reputation system, α is assigned as the number Np of positive ratings plus 1 and β is assigned as the number Nn of negative ratings plus1. Initially, dynamic trust is the expectation of positive behavior from a node. Infuture interactions, the trust worthiness value is calculated as,

$$\frac{\alpha}{\alpha+\beta} \equiv \frac{N_P+1}{N_P+N_n} + DyT \qquad \text{Eq. (2)}$$

P represents the decay factor or forgetting can be applied to assign more weightto new ratings and gradually the older ratings are decreased. Intelligent beta reputationand dynamic trust value is calculated as follows:

$$IDT = \frac{S+1}{F+S+2} + \frac{dS+1}{dF+dS} + DyT \qquad \text{Eq.(3)}$$

IDT is the combination of dynamic trust. Theproposed intelligent beta reputation model is used for calculating the trustvalue dynamically. The proposed work consists of a trust-based secure routingalgorithm that works in three phases namely trust score evaluation, threshold setting,and routing based on the trust values. This proposed work focuses on important aspect namely dynamic trust based secure routing.The trust-based secure routing algorithm is the main focus of this work. The stepsof the proposed secured routing algorithm are as follow:

Dynamic trust based secure routing algorithm

Step 1: Let $T_v(n_1, n_2…n_m) = 0$. //T_v indicate trust value, n_1, n_2, …n_m are nodes.

Step 2: Every node (n_1, n_2…n_m) are considered as source node in different time duration (t_1, t_2).

Step 3: Send messages to the neighbour nodes.

Step 4:HC = HC + 1

Step 5: Start the Scheduler Class to execute the simulation.

Step 6: If it received the request from neighbour nodes then

ensure that the node is destination node

Else If it is destination then

It sends the acknowledgement to its neighbouring nodes.

Step 7: Compute the trust score for all the nodes using Eq. 1.

Step 8: Compute the dynamic trust score for all the nodes using Eq. 2.

Step 9: Compute the overall trust score for all the nodes using Eq. 3.

Step 10: If Minimum value (T_{kc}) < Threshold then

Detect the malicious node

Else

Update the routing table with new node.

Step 11: Perform routing performance

The proposed secure routing algorithm calculates the trust value dynamically. The trust values are calculated during different time intervals for all the participantnodes of the network scenario. The participant nodes ensured the proper destinationnode by receiving the acknowledgement for their messages. Similarly, the trust score and dynamic trust score have been calculated for the individual nodes usingthe Eqs. (2) and (3).

Threshold values are fixed by the intelligent agents andchecked with the dynamic trust scores of all nodes in the network scenario. If thedynamic score of the particular node is less than the threshold value, then theparticular node must be considered as malicious node and it is also avoided forperforming routing. Finally, the routing process is performed with all other nodeswhich are having the dynamic scores above the threshold.

3.   Result and Discussion

We have implemented the proposed routing algorithm using NS2 (Version 2.34.1) by using the existing AODV routing protocol. The topology of the wireless networkdepends on the pause time and mobility speed and also it changes its topologyfrequently when pause time is less and mobility speed is more. The performance ofAODV protocol in presence of malicious node is compared with the performance ofproposed technique in this work. Figure 1 describes the trust score variationbetween the existing and proposed system. From Fig. 1, it can be seen that theproposed system performs well than the existing system. This is due to the use ofintelligent reputation mechanism and dynamic trust value calculation.
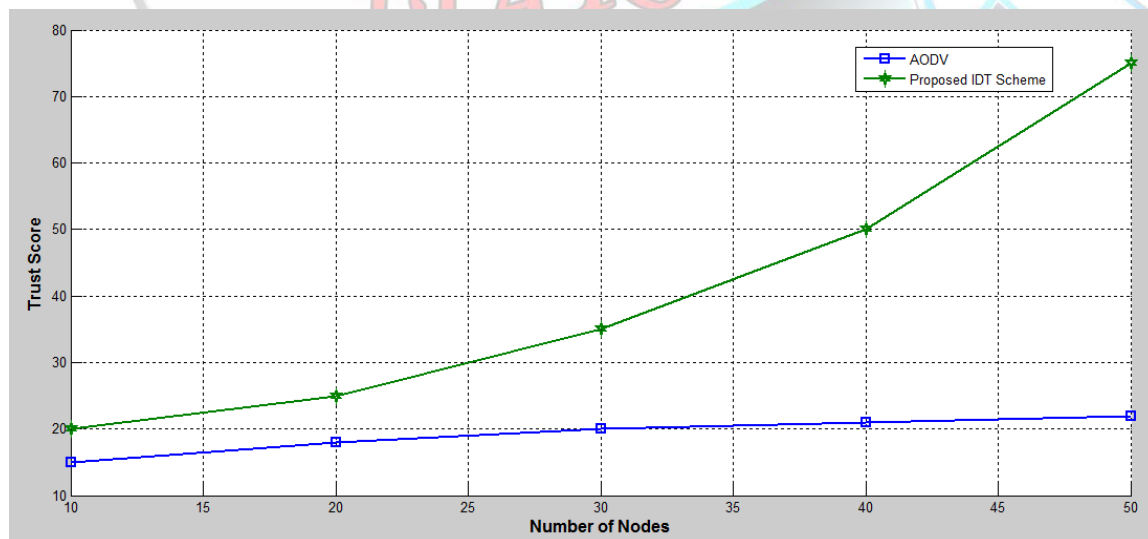

Figure 1: Average Trust Score analysis in percentage

Figure 2 shows the delay analysis of the proposed system and the existing AODV protocol. From Fig. 2, it can be observed that the performance of theproposed system is better than the existing protocol in terms of delay.Figure 3 shows the packet drop ratio analysis of the proposed routing algorithm and the existing AODV.
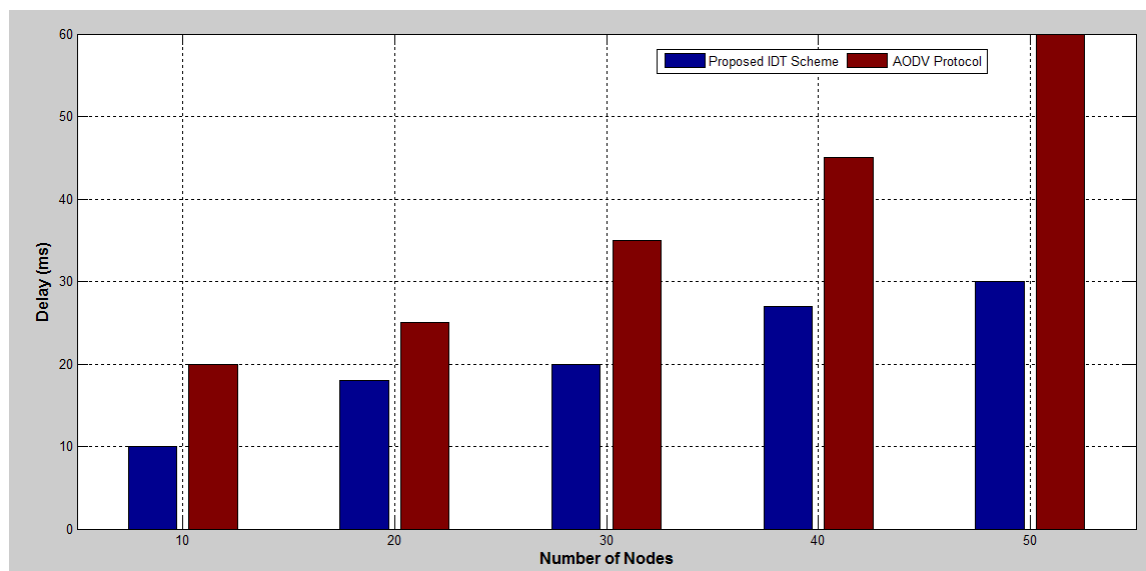

Figure 2: Delay Analysis of Proposed IDT Scheme with existing AODV Routing protocol

From Fig. 3, it can be observed that the packet drop ratio gradually decreases in this proposed IDT when it is compared with AODV with the minimum numberof malicious nodes are present in the network. This is due to the use of intelligent agent, dynamic trust and the beta reputation system.
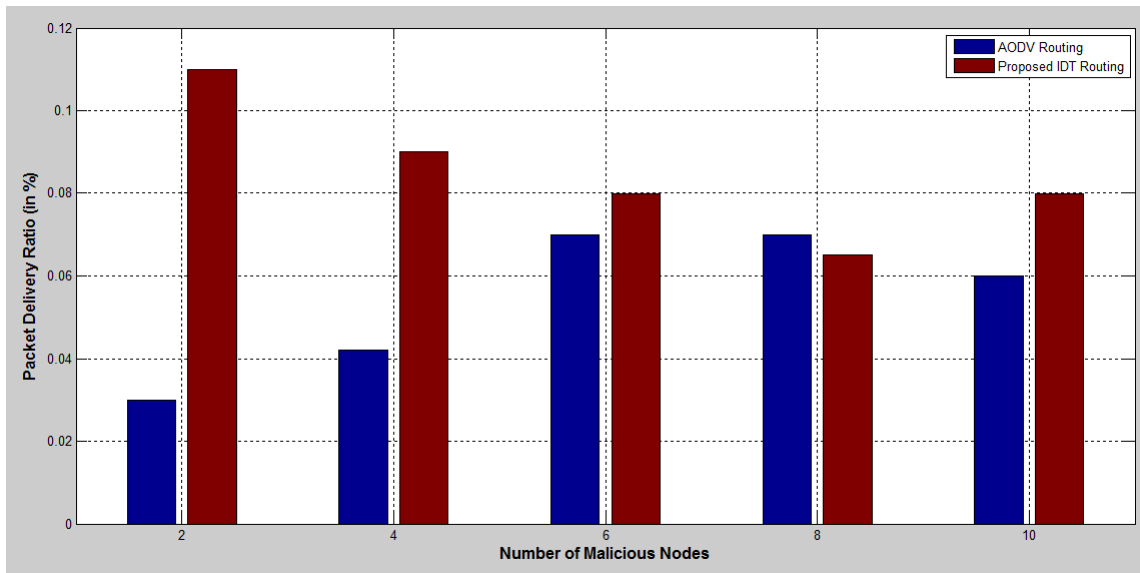
Figure 3: Analysis of the Packet Delivery ratio based on Number of malicious node using Proposed IDT scheme and AODV protocol

4.   Conclusion

An intelligent beta reputation and dynamic trust model is proposed and implemented for effective secure communication. Moreover, an intelligent secure routingalgorithm has been proposed, discussed and implemented in this research work.From the experiments conducted using this secure routing algorithm, it has beenshown that the trust and reputation calculation and management for secure communicationin wireless networks.

References

[1] Zhu, C., et al.: An authenticated trust and reputation calculation and management system forcloud and sensor networks integration. IEEE Trans. Inf. Forensics Secur.**10**(1), 118–131(2015)

[2] Das, A., Islam, M.M.: Secured trust: a dynamic trust computation model for securedcommunication in multi agent systems. IEEE Trans. Dependable Secure Comput.**9**(2), 261–274 (2012)

[3]Ganeriwal, S., Balzano, L.K., Srivastava, M.B.: Reputation-based framework for highintegrity sensor networks. ACM Trans. Sens. Netw.**4**(3) (2008)

[4]Josang, A., Ismail, R.: The beta reputation system. In: Proceedings of 15th Bled ElectronicCommerce Conference, 2002, pp. 324–337

[5]Bao, F., Chen, I.-R., Chang, M., Cho, J.-H.: Hierarchical trust management for wireless sensornetworks and its applications to trust-based routing and intrusion detection. IEEE Trans.Netw. Serv. Manage. **9**(2), 169–183 (2002)

[6] Geetha, G., Jayakumar, C.: Implementation of trust and reputation management forfree-roaming mobile agent security. IEEE Syst. J. **9**(2), 556–566 (2005)

[7]Chae, Y., Dipippo, L.C., Sun, Y.L.: Trust management for defending on-off attacks. IEEETrans. Parallel Distrib. Syst. **26**(4), 1178–1191 (2015)

[8]Mousavifar, S.A., Leung, C.: Energy efficient collaborative spectrum sensing based on trustmanagement in cognitive radio networks. IEEE Trans. Wireless Commun.**14**(4), 1927–1939(2015).

[9]Kraounakis, S., Demetropoulos, I.N., Michalas, A., Obaidat, S.M., Sarigiannidis, P.G., Louta,M.D.: A robust reputation-based computational model for trust establishment in pervasivesystems. IEEE Syst. J. 9(3), 878–891 (2015)

[10]Muneeswari, S.J., Ganapathy, S., Kannan, A.: Intelligent data gathering and energy efficientrouting algorithm for mobile wireless sensor networks. Asian J. Inf. Technol. 15(5), 921927(2016)

[11] Logambigai, R., Kannan, A.: Fuzzy logic based unequal clustering for wireless sensornetworks. Wireless Netw.22(3), 945–957 (2016)

[12] Al-Jarrah, O.Y., Alhussein, O., Yoo, P.D., Muhaidat, S., Taha, K., Kim, K.: Datarandomization and cluster-based partitioning for Botnet intrusion detection. IEEE Trans.Cybern. 46(8), 1796–1805 (2016)

[13]Rajeshwari, A.R., Kulothungan, K., Ganapathy, S., Kannan, A.: Malicious nodes detection inMANET using back-off clustering approach. Circuits Syst. 7, 2070–2079 (2016).