Wireless Netw (2017) 23:693–702
DOI 10.1007/s11276-015-1166-y

Trust based Intelligent Routing Algorithm for Delay Tolerant Network using Artificial Neural Network

Ajay Vikram Singh[1] · Vandana Juyal[1] · Ravish Saggar[2]

Published online: 8 January 2016

Abstract In today's world, when every mobile device corresponds with human behavioral patterns. People often come across with various communities having patterns such as mobility, communication and groups. Trust is an intrinsic factor, which plays important role in formation of such communities. It is important to see the inherent risk involved in such socially active communities. Such factors motivate the use of trust as a routing factor in Delay Tolerant Networks (DTNs). This paper proposes a Trust based Intelligent Routing Algorithm, which exploits the Call Data Record from Call Detail Record. The function of Artificial Neural Network is to calculate and learn, trust value that can be shared among network devices. Our algorithm lowers the need of nodes resources like energy consumption, computation time and space overheads. The proposed algorithm enhances the routing performance in DTN. The earlier work claiming better efficiency generally ends up consuming network's resources. On the contrary our proposed algorithm provides in-built security, without any additional overhead. To the best of our knowledge the proposed work is the first of its kind, providing ingrained security feature to the DTN. This work gives vantage point to the researchers in the field over other schemes proposed in the past.

Keywords Delay Tolerant Network · Opportunistic Network · Trust Management · Artificial Neural Network · Routing algorithm · Performance evaluation

✉ Vandana Juyal
vandana.juyal@gmail.com

[1] Amity University, Noida, Uttar Pradesh, India

[2] BCIIT, Delhi, India

1 Introduction

Due to the need of any networking architecture which can be used for deep space communication as traditional TCP/IP protocol does not support such communication. NASA has worked on Delay Tolerant Network (DTN) that supports deep space communication [1]. DTN makes network communication possible via small as well as robust networked processing devices, distributed in our day to day life. Routing algorithms in DTN utilize a paradigm called store-carry-and-forward. When a node receives a message from one of its contacts, it stores the message in its buffer and carries the message until it encounters another node which is at least as useful as itself.

1.1 Routing in DTN

Routing in DTN is a challenging problem because an end-to-end path from a source to a destination is usually unknown. TCP/IP provides end-to-end process communication that exist between a data source and its peer(s), whose maximum round trip time is not excessive and packet drop probability is less. Since most of the conventional routing algorithm assumes that the links between nodes are stable and do not fail frequently, thus are not practically feasible in DTN scenarios. Some examples of such a challenged class of networks, which may violate some assumptions, and may not be served by the current TCP/IP are: Terrestrial Mobile Networks, Exotic Media Networks, Military Ad hoc Networks, and Sensor/Actuator Networks [2, 3].

1.2 What is trust?

According to the oxford dictionary, "Firm belief in the reliability, truth, or ability of someone or something" is known to be as Trust [4]. Trust can be characterized as subjective, dynamic, temporary, disproportional and asymmetric. In real world, this is often cited that in an organization, while moving from bottom to top level trust value is high and while moving from top to bottom, it is low. Trust involves continuous values and risk is an inherent property of it. Although the severity may differ, depending on the risk involved.

In the Fig. 1, the trust value depicted horizontally and it is non-transitive. On the contrary in an organization, it is usually observed that the level of trust is higher, of subordinates towards their bosses but the bosses may not trust their subordinates. Thus the trust value may be asymmetric. Also trust is context dependent and thus may vary in different scenarios.

For example, Susan and Mary working in an organization ABC, may or may not trust each other. In a scenario where decision making involves high risk factor, Susan may not trust Mary but in case of low risk involved, Susan may trust Mary. Thus it is easily perceived for trust, to have continuous values. Considering T(v) as trust value may be quantified as values between -1 to 1.

$$\begin{array}{ll} \mathrm{T(v)} & = -1,\ \text{Not Trusted} \\ & \quad\ \ 0,\ \text{Neutral} \\ & \quad\ \ 1,\ \text{Trusted} \end{array}$$

1.3 Motivation and contribution

The motivation for this research is the need to use human communication patterns for routing decisions. The trust is considered as an important factor for communication that can be incorporated for the formulation of the new routing algorithm. In this paper, researchers have made their contribution in terms of development of the Trust based Intelligent Routing Algorithm (TBIR) for DTN. It is formulated with acceptable level of risk thus provides intrinsic security. Section 1 introduces the fundamental concepts of routing protocol in DTN. It also lays emphasis on trust. How trust can be incorporated in the routing? Section 2, is about the literature review in the field of DTN. In Sect. 3, the proposed work including category of DTN node, design strategy for incorporation of trust and assumption made for Trust Management is discussed. Section 4, discusses the ANN based trust for computing and learning of trust value. In Sect. 5, for TBIR various scenarios set ups are illustrated. In Sect. 6, the performance evaluation is done. Finally, the researchers outline the conclusion made and the future work to be accomplished.

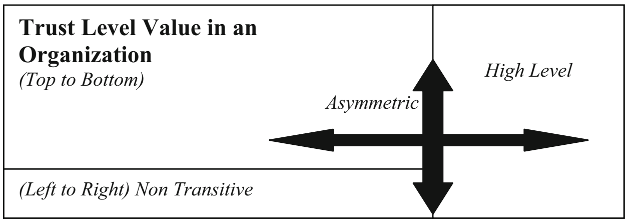
Trust Level Value in an Organization
(Top to Bottom)
High Level
Asymmetric
(Left to Right) Non Transitive

Fig. 1 Showing level of trust in an organization

2 Related work

This section briefly reviews and compares related works in broad domain of Wireless Ad hoc Networks as well as particularly about DTN. The recent studies shows that the cognitive radio networks [5] have focussed on multi hop secondary networks to achieve best routing options. The classification of the infrastructure less CRN attacks are exogenous attacks, intruding nodes and selfish nodes. The security threats faced by such networks are often of type external [6]. Same is the case with DTN. It also faces similar category of threats. Thus providing security is essential for such phenomena to work. It is evident for DTN to have proactive environment to handle such attacks. The quality of wireless links may get affected by many factors like collisions, fading or the noise of environment.

Some of the latest developments in field of routing protocols are suggested by using opportunistic routing (also known to be as DTN) and random linear network coding [7]. State of art development and analysis of routing algorithm is suggested for vehicular DTN [8–10]. Lot of work related to improve Quality of Service including the proposed work in which Quality of Routing can be enhanced using Nash Equilibria [11] has been performed but as DTN is a challenged class of networks thus improving the Quality of Service does not hold in this case. In past the phenomena of such challenged networks has often underrated QoS as performance criteria for DTN. Recently many genetic algorithms have been used to propose improved and optimized routes including spatial reusability-aware routing in multi-hop wireless networks for improving in end to end throughput [12]. In one of the study an algorithm is proposed which relies upon the usage of orthogonal channels for solving the Channel Assignment (CA) problem [13]. For DTNs, an alternative, highly agile approach called backpressure routing in which routing and forwarding decisions are made on a per-packet basis is proposed [14]. As delay and interference are constraints in Mobile Ad hoc Network (MANETs) and these constraints do not let MANETs work in its full capacity thus a delay-constrained topology control algorithm is proposed to improve the performance of the delay-constrained MANETs [15]. In MANETs, issues and challenges related to Quality of Service parameters like delay as well as guaranty to achieve QoS are discussed and in order to improve QoS based routing, an evolutionary-fuzzy prediction based mechanism is proposed [16–18].

On the contrary, the challenged class of networks like Delay/Disruption Tolerant Networks accepts delay. Delay is acceptable and thus the performance metrics of the DTN does not consider delay as a factor. That is the reason why it is popularly known as DTN applicable only in selected area of communication [19, 20].

Epidemic routing protocol is a flood based routing algorithm that replicates and spread messages to any node that is in the transmission range. SprayAndWait routing protocol is a routing protocol that limits the number of replication of a message to reduce the overhead of delivering a message. In First Contact routing protocol, messages are forwarded randomly to any node which comes first in the transmission range. As the name suggests, Direct Delivery routing protocol forwards only when the destination node is encountered. EpidemicOracle routing protocol, forward a message, if and only if there is some probability of connectivity in near future. Probabilistic ROuting Protocol using History of Encounters and Transitivity (PROPHET), considers the probability of node coming in close contact in near future to route message. Max-Prop routing protocol computes single source—all destination, shortest path algorithm. Among all of the six underlying DTN routing protocol, the Epidemic routing protocol has achieved better results over others [21].

In the past work, the protocol considers QoS and Social trust as important factors in an application driven environment. Indicating value from (0, 0.5, 1) as trust, ignorance and distrust respectively. The beta probability density function has been used in trust and reputation systems, to calculate trust value. Also trust value may be quantified in various ways. The protocol also claims to eliminate selfish behavior of the node [22]. On the contrary, the QoS factors don't apply well with the DTN network. The concept of DTN is to develop such a network where delay tolerance is an intrinsic property and any amount of delay is acceptable. The ultimate aim is to deliver a message to its final destination [23]. Researchers' identified dynamic characteristic of trust. The related work calculates trust, maintains it through rating system of each node, using modified Bayesian approach stating reputation fading and redemption mechanism [24, 25].

2.1 Trust based approach

As trust is a subjective phenomenon so for implementing trust in real network it is quite challenging. For this various processes like Trust Metric Identification, Trust Formation and Computation of Trust Value must be induced in the Node. Trust should be implemented in highly customizable way. It should not assume all nodes to be cooperative. In order to save node's own resources, selfishness is bound to occur. In case of limited resources and trade offs, like security, scalability and energy needs to be reconsidered.

2.2 Factors affecting trust

In general, Trust building is a continuous and interactive process between two entities. The value of trust changes drastically with the denial of service via intermediate node or destination node. For example messages dropped, connection aborted may have negative impact on the routing protocol. In case of such events, the trust value computed with the help of various parameters must be negated. For this a bias which is set as very high negative value is used. Trust metric which occurs as an outcome of recent event must have high impact i.e. the effect of any unfavorable event must have high impact. Reason being, it's more catastrophic in real world and the values learned in past may not be valid at all. Thus it is important to re-evaluate and re-establish the updated learned behavior. Although there is no proof of correctness, that trust will be honored as it is asymmetric. Implementation of trust as parameter requires information regarding successful number of exchanges made.

3 Proposed work

DTN nodes may be categorized into either those source node having direct or indirect connection with destination node. The design strategy for incorporation of trust in DTN is to identify trust metric for routing protocol. On the basis of trust metric quantification, it further identifies the trust worthiness of a node. So that the trust value computed for each node must be referred for making forwarding decisions.

3.1 Assumptions made for Trust based Intelligent Routing Algorithm

Trust value should be continuous while calculating and deploying the same in DTN. All nodes communicate via Bluetooth (shared wireless channel). It operates in non promiscuous mode, i.e. no node in the network having information of the whole network traffic. The individual node does not work in dedicated manner. Due to high mobility of such nodes, a network is characterized by abruptly, breaking many times. All nodes are identical in their physical characteristics. The node is characterized as pedestrian nodes, or nodes travelling in either public or private transport. The messages are routed on the basis of computed trust value as and when they come into the close proximity of each other.

4 Artificial Neural Network based trust model

Artificial Neural Network (ANN) is a soft computing technique used for computation and learning. In socially active networking domain, Researchers' often come across with mobility patterns [26]. And thus the same can have communication pattern that can be quantified, on the basis of Call Data Record (CDR) information. The parameters of CDR like time, duration and frequency [27] are mapped to compute the trust value to enhance routing efficiency in DTN.

4.1 Mapping

The computation of trust value by using Trust Metric can be done after mapping CDR parameters with DTN Routing parameters (Table 1).

Suppose for node identification, the intermittent network is comprised with nodes as a_1, a_2, a_3, a_4 and so on. The initial trust value is defined as follows: a_1, a_2, a_3 as $T(a_1) = T(a_2) = T(a_3) = 0$. Initially the value of trust for all nodes in the network is zero. The destination is searched after sending first data packet from source to destination.

4.2 Computation and learning

The computation and learning of trust values for each node in the network is based upon Trust Function:

$$f(a_1) = <\mathit{Time\ Difference\ between}\ \mathrm{Recent}\ \mathit{Connection\ and\ Last\ Connection}\ P_1,\ \mathit{Frequency\ of\ Calls}\ P_2,\ \mathit{Total\ Duration}\ P_3 >$$

In Fig. 2, the parameters P_1, P_2, P_3 having weight as w_1, w_2, w_3 are assigned to the Binary Activator Function [28]. Where $w_0 = 1$, $P_i = \mathit{Trust\ Parameters}$, $w_i = \mathit{Weight\ assigned\ to\ each\ parameter}$, $b = -999$, $P_1 = (\mathit{Current\ Time—Last\ Connection\ Time})$, $P_2 = \mathit{Frequency\ of\ Calls\ from}\ a_i\ \mathit{to}\ a_j,\ \mathit{where}\ i \neq j\ \mathit{and}\ i, j \in N\ P_3 = \mathit{Total\ Duration\ of\ Calls}$, and $\mathit{Weights}\ w_1 = 1/P_1$, $w_2 = w_3 = 1$.

For each node a_i this function will activate for remaining nodes i.e. for all a_1, $a_2 \ldots a_{i-1}$ and for all a_{i+1}, $a_{i+2} \ldots a_n$.

$$f(u) = \sum_{i=0}^{3} P_i W_i \tag{1}$$

$$v = u + b \tag{2}$$

$$Y = \varphi(v) \tag{3}$$

$$Y = \begin{cases} 0, & \mathit{if}\ v < 0 \\ 1, & \mathit{if}\ v \geq 0 \end{cases} \tag{4}$$

The reason for keeping the weight $w_2 = w_3 = 1$ for parameter P_2 and P_3 is to get actual values of P_2 and P_3 for further computation. In the case of any unfavorable event, the bias value b is activated. Bias b is assigned with a high negative value. The trust value is computed on 1:1 basis. The value of parameter P_1 is inversely proportional to the value of trust. If the value of the P_1 parameter is high, then the trust is less and vice versa. Trust value is a part of the Route Cache (RC). All values taken are absolute.

Notation:

Node—a_i to a_n
T_{old}—Trust value old
T_{new}—Trust value new
CDR—Call Data Record
RC—Route cache
P_1—Time difference between recent connection and last connection
P_2—Frequency of calls between a_i and a_j
P_3—Total duration call initiated from a_i to a_j
b = Bias (−999)

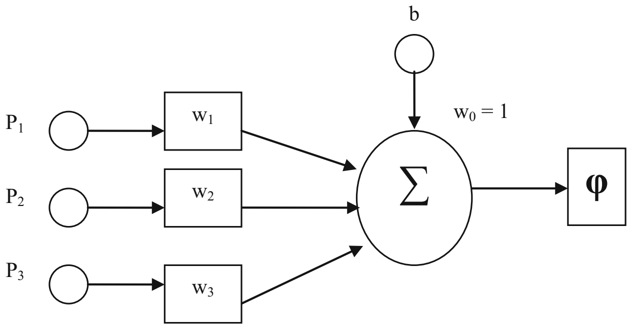

Fig. 2 Binary Activation Function with trust parameters [28]

Table 1 Call Data Record parameters mapped to DTN routing parameters [27]

Actual parameter	Parameters identified
Phone number of calling party	Msg_Source_ID
Phone number of receiving party	Msg_Dest_ID
Call start time	Conn_Time
Call duration	Duration
Unique number identifying the record	Conn_Time
Call event	ActionID (like create, abort, connection up and down) uniquely identifying the transmission
The route by which the call entered the exchange	If intermediate node check the trust metric value
The route by which the call left the exchange	If intermediate node check the trust metric value
Call type (voice, SMS, etc.)	Connection type will remain identical
Any other fault condition encountered	If any fault condition is encountered, set Trust value = −999

Precondition: In DTN, communication between any two nodes a_1 and a_2 is one to one basis

Algorithm 1: Inital Trust based Intelligent Routing Algorithm

```
Steps:
Using CDR, Fetch $\boldsymbol{P_1, P_2, P_3}$
Compute $Y$
Using RC, Fetch $T_{old}(a_i, a_j)$
    if $Y=0$ do
        $T_{new}(a_i, a_j) \leftarrow T_{old}(a_i, a_j)$
        else if ($Y=1$ & $T_{old}(a_i, a_j)$) is not present in RC do
            $T_{new}(a_i, a_j) =1$
            else if $Y=1$ & $T_{old}(a_i, a_j)$ is in RC and has some value do
                $T_{new}(a_i, a_j) \leftarrow T_{old}(a_i, a_j) +1$
            end if
        end if
    end if
Repeat the process for all intermediate nodes till destination node is not found
```

Algorithm 2: Trust based Intelligent Routing Algorithm for Intermediate Node

```
Steps:
Using RC, check if $a_i$ is an intermediate node
Compute Trust Values $T_{new}(a_i, a_j)$ for all $a_1, a_2 \ldots a_{i-1}$ and for all $a_{i+1}, a_{i+2} \ldots\ldots a_n$.
Select that node as next intermediate node having highest Trust Value
    else if check RC of $a_i$, if more than one node has same highest equal Trust Values
        then using CDR of $a_i$, $\forall$ nodes Trust Values are equal, fetch $P_1$ values
                Select that node as next intermediate node which is having less $P_1$
            else if two or more than two nodes have equal $P_1$ values with respect to $a_i$
            then randomly select any node as next intermediate node
            end if
    end if
end if
Repeat the process for all intermediate nodes till destination node is not found
```

5 Scenario setup

5.1 Conceptual instances I

The initial trust value of all the nodes $a_1 \ldots a_4$ in transmission range is 0. The routing protocol will work normally without using trust value for the first time.

Here in Fig. 3, the trust value of node a_1, a_2, a_3 remains 0 but the trust value of node a_4 is set to minus infinity ($-\infty$). Reason being, the node a_4 is in isolation and is not in transmission range with others.

$$T(a_1, a_2) = T(a_1, a_3) = and\ T(a_1, a_4) = -\infty$$

Like this node a_2 have some values in its routing cache for $T(a_2, a_1) = T(a_2, a_3) = and\ T(a_2, a_4)$

For communication initiated from a_1 to a_2, the corresponding Table entries of node a_1 are as follows (Table 2).

The trust value for node a_1 to itself is not evaluated, thus it is considered as nil.

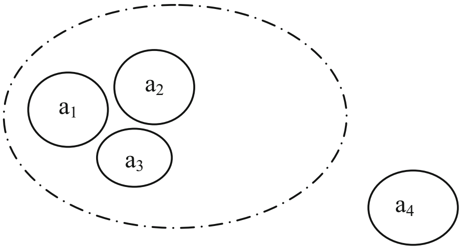

Fig. 3 At time t_0

5.2 Conceptual instances II

In this case node a_1 initiates communication with node a_2; the corresponding Trust value increases respectively by using ANN based learning (Fig. 4).

The table entries for node a_1 changes accordingly. With respect to the previous Trust value for communication between a_1 and a_2, the value increments by 1 (Table 3).

5.3 Conceptual instances III

In case of the nodes a_2, a_3, a_4 comes in transmission range of the node a_1 at time t_2. Then the corresponding Trust values will be computed as follows:

$$T(a_1, a_2) = T(a_1, a_2) + 1$$

$$T(a_1, a_3) = T(a_1, a_4) = 0$$

Here in Fig. 5, the Trust value of node a_1, a_2, a_3, a_4 is recomputed for each other in slate time. The Trust value for node a_4 is 0 as it is in transmission range with other nodes. For communication initiated from a_1 to a_2, the corresponding Table entries of node a_1 are as follows.

Table 2 Table entries of initial trust values of node A_1

Source node	Destination node	Trust value
a_1	a_1	–
a_1	a_2	0
a_1	a_3	0
a_1	a_4	$-\infty$

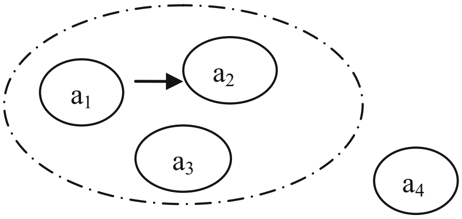

Fig. 4 Connection initiated from a_1 to a_2 at time t_1

Table 3 Table entries of computed trust values of node A_1

Source node	Destination node	Trust value
a_1	a_1	–
a_1	a_2	$T(a_1, a_2) + 1$
a_1	a_3	0
a_1	a_4	$-\infty$

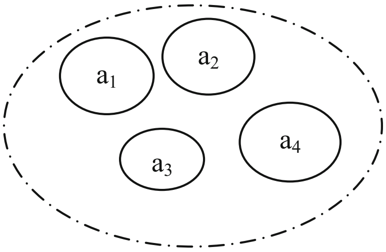

Fig. 5 Nodes within transmission range of node a_1 at time t_2

Table 4, depicts the change of Trust value, the moment node a_4, and is in transmission range of its peers.

5.4 Conceptual instances IV

The conceptual instance IV illustrates many direct or indirect paths at a given point of time. The process of choosing an intermediate node is further categorized into two cases. In first case, only one intermediate node has higher Trust value. And in second case, more than one node has the same high Trust value (Fig. 6).

Table 4 Table entries of computed trust values of node A_1

Source node	Destination node	Trust value
a_1	a_1	–
a_1	a_2	$T(a_1, a_2) + 1$
a_1	a_3	0
a_1	a_4	0

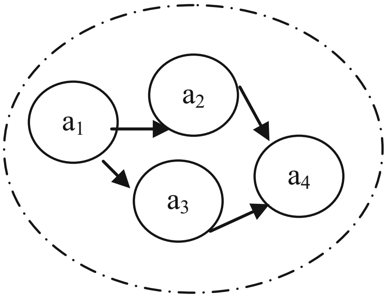

Fig. 6 Depicts two communication paths available from source node a_1 to destination node a_4

Table 5 Corresponding table entries of computed trust value of node A_1

Source node	Destination node	Trust value
a_1	a_1	–
a_1	a_2	3
a_1	a_3	3
a_1	a_4	0

Here Table 5, illustrates the corresponding Trust value entries in the Route Cache of source node a_1. At a given point of time, the source node a_1 encounters two intermediate nodes with the same highest Trust value i.e. 3. In this case, to route a message via one of these available paths, the TBIR makes forwarding decisions on the basis of its computed Trust value and latest connection time in DTN.

6 Performance evaluation

The simulation of the proposed algorithm has simple broadcast interface for Bluetooth, having transmission speed of 250 k and range of 10 m. The shortest path map based movement model is used. There are six groups comprising of two pedestrian groups, cars, three trams groups to generate the metropolitan city like node mobility pattern. The performance evaluation of the TBIR is based on parameters like number of messages started, delivered, aborted, dropped, and it's delivery probability.

The performance evaluation is done based on other two DTN routing protocol namely Epidemic and First Contact. Epidemic routing protocol is flood based routing protocol. The reason for choosing Epidemic routing protocol for the comparison is ability of the protocol to deliver higher number of messages. Also the First Contact routing protocol is forwarding based routing protocol having minimum overhead ratio. The reason for choosing First Contact routing protocol is its lesser aborted and dropped events occurrence. The simulation performed for the Epidemic, First Contact routing protocol and TBIR, using open sourced, Opportunistic Network Environment Simulator (ONE) [29], dedicated to the DTN (Fig. 7, 8, 9, 10, 11).

TBIR has larger number of messages started. It outperforms, in terms of total number of messages delivered. Also the lesser number of drops indicates the maximum resource utilization of the DTN network.

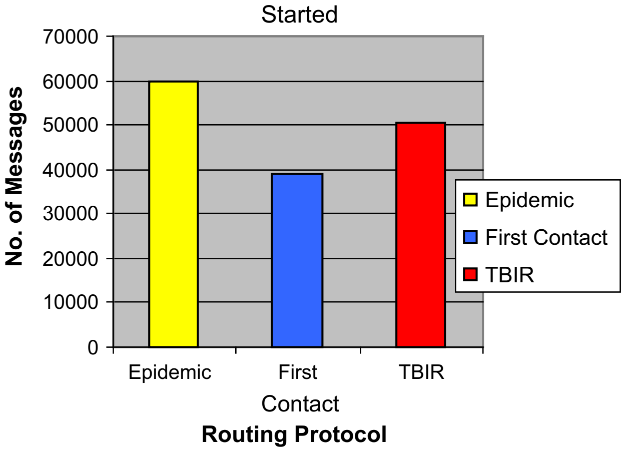

Fig. 7 Total number of messages started

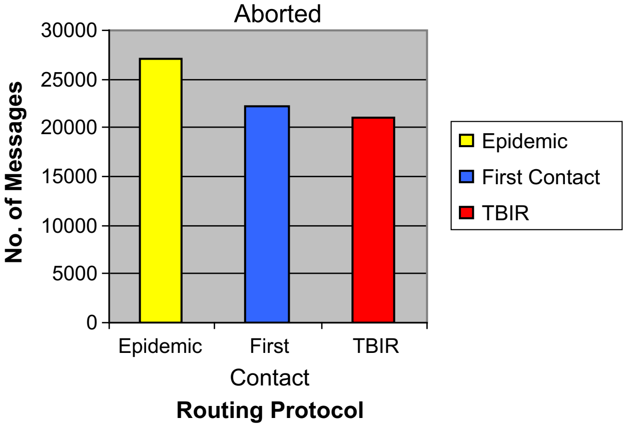

Fig. 8 Total number of messages aborted

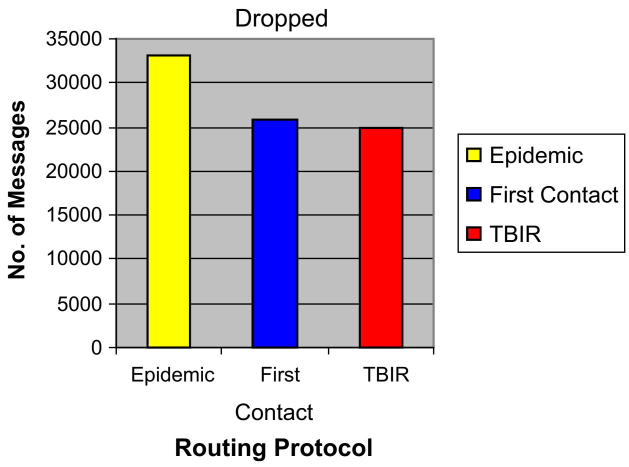

Fig. 9 Total number of messages dropped

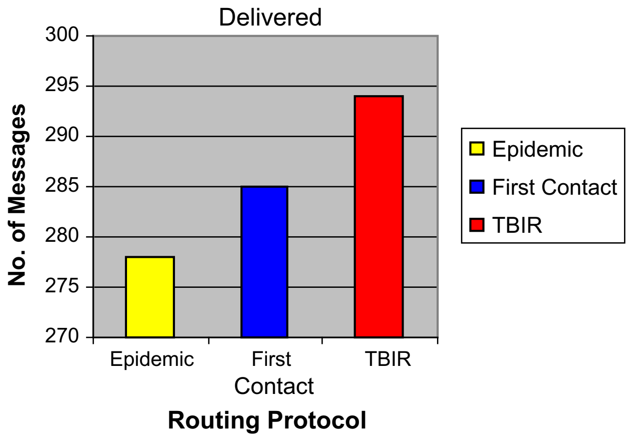

Fig. 10 Total number of messages delivered

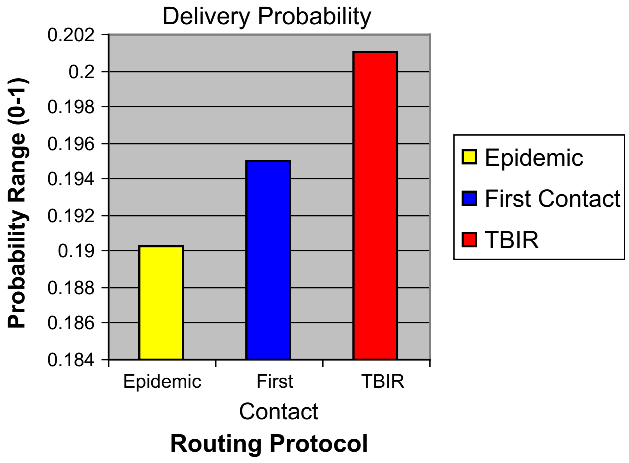

Fig. 11 Delivery probability

7 Conclusion

In this paper researcher makes use of ANN based model for the implementation of the Trust value disseminated in the entire network. TBIR is forwarding based modernistic approach. The intrinsic risk involved is context dependent and acceptable to the nodes. DTN is intermittently connected network. DTN may learn to trust via gradual process and has ability to form dynamic groups. The algorithm is light weight and thus results in lesser security overheads. Also the implementation of such approach is more practical. This algorithm will also be beneficial in providing light weight security in the real world where some amount of risk is acceptable. It also eliminates the requirement of authorization/authentication process, necessary for the communication in real world. Such approach saves computation time, resource's energy and space overheads of each node in DTN. The applicability of trust as a metric for routing messages in the DTN has advantages like less security overheads, lesser routing overheads, learning of the entire network based on trust.

8 Future work

Trust can be considered as an intrinsic factor for service configuration and traffic distribution in composite radio environments. The algorithm proposed can be implemented for failure detection in Composite Radio Environments. The future work may involve exploring the applicability of the TBIR in DTN in real world scenarios.

Acknowledgments Researchers wishes to express sincere gratitude to the administration of M.C.A Department of Banarsidas Chandiwala Institute of Information Technology (BCIIT), affiliated to G.G.S.I.P. University, Delhi, India and Amity Institute of Information Technology (AIIT), Amity University Uttar Pradesh (AUUP), India, for providing the academic environment to pursue research activities.

References

1. Sun, X. (2013). Performance of DTN protocols in space communications. *Wireless Networks, 19*(8), 2029–2047.
2. Jones, E. P. C., Li, L., Schmidtke, J. K., & Ward, P. A. S. (2007). Practical routing in delay-tolerant networks. *Mobile Computing, IEEE Transactions, 6*(8), 943–959. doi:10.1109/TMC.2007.1016.
3. Yang, Z., Wang, R., Li, H., & Vasilakos, V. (2014). On storage dynamics of space delay/disruption tolerant network node. *Wireless Network, 20*(8), 2529–2541. doi:10.1007/s11276-014-0756-4.
4. Oxford Dictionary [Online]. Available: http://www.oxforddictionaries.com/definition/english/trust#.

5. Youssef, M., Ibrahim, M., Abdelatif, M., Chen, L., & Vasilakos, A. V. (2014). Routing metrics of cognitive radio networks: A survey. *Communications Surveys and Tutorials, IEEE, 16*(1), 92–109. doi:10.1109/SURV.2013.082713.00184.
6. Esch, J. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. *IEEE, 100*(12), 3170–3171. doi:10.1109/JPROC.2012.2219194.
7. Li, Peng, et al. (2012). CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding. *INFOCOM, 2012*, 100–108.
8. Liu, J., et al. (2015). A survey on position-based routing for vehicular ad hoc networks. *Telecommunication Systems*. doi:10.1007/s11235-015-9979-7.
9. Yuanyuan, Z., et al. (2013). Directional routing and scheduling for green vehicular delay tolerant networks. *Wireless Networks, 19*(2), 161–173.
10. Busch, C., et al. (2012). Approximating congestion + dilation in networks via "quality of routing" games. *IEEE Transactions Computers, 61*(9), 1270–1283.
11. Yen, Y. S., et al. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. *Mathematical and Computer Modelling, 53*(11–12), 2238–2250.
12. Tong, Meng, et al. (2015). Spatial reusability-aware routing in multi-hop wireless networks. *IEEE TMC*. doi:10.1109/TC.2015.2417543.
13. Duarte, P. B. F., et al. (2012). On the partially overlapped channel assignment on wireless mesh network backbone: A game theoretic approach. *IEEE Journal on Selected Areas in Communications, 30*(1), 119–127.
14. Dvir, A., et al. (2011). Backpressure-based routing protocol for DTNs. *ACM SIGCOMM Computer Communication Review, 41*(4), 405–406.
15. Zhang, X., et al. (2015). Interference-based topology control algorithm for delay-constrained mobile Ad hoc networks. *IEEE Transactions on Mobile Computing, 14*(4), 742–754.
16. Singh, V.A., Singh, B., Alam, A. (2011). Issues and challenges associated with secure QoS aware routing in MANETs. *International Journal of Research and Reviews in Ad Hoc Networks (IJRRAN)*, *1*(3), 73–76, ISSN: 2046-5106, Science Academy Publisher, United Kingdom.
17. Vasilakos, A., et al. (1998). Evolutionary-fuzzy prediction for strategic QoS routing in broadband networks. *IEEE International Conference on Fuzzy Systems Proceedings, 2*, 1488–1493.
18. Xiong, N., et al. (2009). Comparative analysis of quality of service and memory usage for adaptive failure detectors in healthcare systems. *IEEE Journal on Selected Areas in Communications, 27*(4), 495–509.
19. Delay-Tolerant Networking TCP Convergence-Layer Protocol. (2014). RFC 7242 [Online]. Available: https://tools.ietf.org/html/rfc7242.
20. DTN architecture. (2007). RFC 4838 [Online]. Available: https://tools.ietf.org/html/rfc4838.
21. Juyal, V., Singh, A.V., Saggar, R. (2015). Message multicasting in near-real time routing for delay/disruption tolerant network. In: *IEEE International Conference Computational Intelligence and Communication Technology (CICT)* (pp. 385–390). doi: 10.1109/CICT.2015.79.
22. Chen, I., Bao, F., Chang, M., & Cho, J. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. *Parallel and Distributed Systems, IEEE Transactions, 25*(5), 1200–1210. doi:10.1109/TPDS.2013.116.
23. Juyal, V., Johari, R. (2012). Node reachability in DTN for Indian Scenario. *Proceedings of IJEST*, *4*(6), 2560–2566. ISSN 0975-5462.
24. Cho, J., Swami, A., & Chen, I. (2011). A survey on trust management for mobile ad hoc networks. *Communications Surveys and Tutorials, IEEE, 13*(4), 562–583. doi:10.1109/SURV.2011.092110.00088.
25. Paliszkiewicz, J. (2011). Trust management: Literature review. *Management, 6*(4), 315–331.
26. A community resource for archiving wireless data at dartmouth (CRAWDAD) [Online]. Available: http://www.Crawdad.org.
27. Horak, R. (2007). Telecommunications and data communications handbook. In: Hoboken: Wiley-Interscience. pp. 110–111. ISBN 0470127228.
28. Lippmann, R. P. (1987). An introduction to computing with neural nets. *ASSP Magazine, IEEE, 4*(2), 4–22. doi:10.1109/MASSP.1987.1165576.
29. The ONE Simulator [Online]. Oppourtunistic Network Environment. Available: http://www.netlab.tkk.fi/tutkimus/dtn/theone/qa.html#routing.

Dr. Ajay Vikram Singh has received his Ph.D. in Computer Science from Jamia Hamdard University, Delhi, India. He has completed his Masters in Computer Application from IIT-Roorkee, India. His area of research are Ad hoc Networks, Internet of Things and Soft Computing Techniques. He has 12 years of teaching experience and currently he is working as a faculty member in Amity Institute of Information Technology (AIIT), Amity University, Noida, U.P, India.

Ms. Vandana Juyal is a research scholar of Amity University, Noida, U.P, India. She has received her M.Tech. in Information Technology and Masters of Computer Applications from G.G.S.I.P University, Delhi, India. Her major areas of interests include Mobile Ad hoc Networks. She has many research publications in area of Mobile Ad hoc Networks published in National/International Conferences and International Journal to her credit. She has consistently maintained percentage above distinction throughout her academic career. She has over eight plus years of teaching experience at post graduate level and currently working as a faculty member in Banarsidas Chandiwala Institute of Information Technology (B.C.I.I.T), affiliated to G.G.S.I.P University, Delhi, India.

Prof. (Dr.) Ravish Saggar has received his Ph.D. in Computer Science from Sighania University, Rajasthan, India, under the guidance of Prof. M.N Doja of Jamia Milia Islamia, Delhi, India. He has done B.Tech. (Computer Technology) from Nagpur University, India and M.Tech. (IT) from G.G.S.I.P University, Delhi, India. His area of research is Wireless Networks. He has sixteen plus years of teaching and 2 years industry experience. He has many research publications in the area of Wireless Networks published in International Conferences and International Journal to his credit. He is currently working as Director in Banarsidas Chandiwala Institue of Information Technology (BCIIT), affiliated to G.G.S.I.P. University, Delhi, India.