A Survey Paper on Efficient Reputation-Based Trust Assurance model for delay tolerant network

Vidya U, Dr. Bhat Geetalaxmi Jairam

[*]Student(M.Tech), [#]Associate professor, The National Institute of Engineering, Mysuru, India,

[*]vidyau95@gmail.com, [#]bgj@nie.ac.in

Abstract-Examining the trust worthiness of node is an important mission to be done before data transmission. The mobility of nodes in delay tolerant network leads to many demanding situations. This paper describes several methods, which was developed by many researchers to overcome these issues. It also explores different routing schemes used on delay tolerant network. It additionally covers a comparative assessment among multiple routing schemes against Reputation Based Trust Assurance model that directs exact trust assessment of network nodes and amplifies the integrity of message delivered while minimizing the communication delay.

*Keywords —**A Bayesian way, Delay Tolerant Network, petrinet model, RBTA, reputation, trustworthiness***

I. INTRODUCTION

Basic requirement to have communication in network is end to end continuous connectivity. The reliable transmission expects end to end acknowledgements. However, nature and attacks at critical conditions breaks the network display. Because of which the transmitted packet may neglect to achieve its goal. Delay tolerant networks are mobile wireless networks. The path between source and destination is not always fixed due to the mobility of nodes[1], [2]. Subsequently the topology of system continues changing and experiences the ill effects of regular separation between nodes. The aggregate of total delay at each node from source to destination indicates the end to end delay. Delay time incorporates transmission, waiting and queuing time [3]. Queuing time plays an important role in this delay and is caused due to the frequent fragmentation in network. To overcome these problems researchers have worked and proposed various solutions over the past decade. The routing technique in this network is distinctive compared to other wireless network. In typical correspondence, due to some problem the link goes down and transmitted packet will be lost. But delay tolerant network utilizes steering nodes with storage capability to protect the data from being lost when the connection is low. The data is stored in node's buffer until the following hop is re-established. Once the connection is strong, it is forwarded to next hop. This technique is called as store and forward. Therefore, there isn't vital that end nodes ought to necessarily be associated.

NASA has invented a new technology using DTN through which internet can be accessed even at space. Researchers of NASA stated that, this was the initial move towards the interplanetary web claimed by them. In this technology, DTN works on the basis of store and forward method as discussed before, where the partial data bundles along with the communication path information is retained in the node's buffer and later re-transmitted to destination either on earth, or at the robotic spacecraft in deep space. On earth, series of communication points are used to spread the information on internet. Each transitional focuses ought to be accessible to exchange the data from one point to other. But in space, all nodes are not constantly accessible on account of their mobility. Additionally, NASA has stated using this network, which allows the data transmission to be more reliable and efficient. It additionally permits to set needs to various kinds of information and the most vital are gotten first.

There are many challenging issues in DTN [4]. Nodes within this network have finite resources such as limited bandwidth, battery power, processing power, memory. Researchers have stated that the wireless bandwidth in mobile nodes is very much restricted when compared stationary nodes. In other words, the capacity in wired links is much higher than that of wireless, due to consequences of signal interference, multiple accesses, multi-path routing and many more. It is observed that the network bandwidth is mostly devoured by control traffic. If the routing protocol is experiencing intemperate network traffic, at that point it prompts decline in correspondence performance. The communication capability of node is not the only reason for performance degradation, but also it is due to the finite battery power. Most of the mobile will be powered with restricted battery lifetime. Each node in the communication path should meet minimum battery requirement. Router at same time will allocate additional energy demands of nodes. General solution for this is to enable power management skill at hardware level. Since battery and bandwidth are constrained, it impacts the processing power of node.

 DOI : 10.35291/2454-9150.2019.0132

Mobile nodes have limited size and power requirement, hence the storage capacity is limited. This posture numerous issues. For instance, if an application has generated large amount of data, the node needs to store this information in its memory before sending, if any issues in transmission. Along with this, network information generated during the transmission is also stored. Since the capacity limit of node is confined, the odds of data misfortune are more. To conquer this issue, the transmitted data and network information must be compressed into smaller files.

Reputation Based Trust Assurance model can overcome these problems to some degree. Nodes in DTN are sparsely scattered and henceforth have very less contact time among them. This in turn prompts trouble in trust assessment of a node in network. If node has to assess trust value of its neighbour node, it can check the history of that node [5]. This information will be provided by Reputation Based Trust Assurance model.

II. RELATED WORK

In wireless mobile networks, the routing of incoming data is executed at network layer. Here some of the routing difficulties and design issues that affect routing procedure in this network is been delineated. Authors of [6] have focused on discovering the location information of destination node, with less communication overhead. Generally, nodes share the location information explicitly through message exchange, which extends the communication cost. To overcome this problem, they developed EASE(Exponential Age SEarch) algorithm. It comes under LER(Last Encountered Routing) algorithm. It says that, the routes are computed completely on the basis of last encounters. The node should know the location of its own and its neighbor to select the route to destination. Here each node will maintain a database about the location and time about the last encountered node in the network. EASE consists of two shifts. To start with, when packet achieves the node, it executes the local search near to it to find the next hop. Second, current position based routing is used. Another algorithm is discussed in this paper that is, GREASE(GReady EASE). In this algorithm, the age of destination's previous encounter is checked. If the encountered node is estimated to be more recent with the destination's location, then the packet will be directed to that node. On the off chance that, if the node has jumped to some other area of interest, then at that point the gathered location information about the node is of no use. Furthermore, if nodes are increasingly portable, at that point LER gets troublesome.

Authors of [7] have focused on selecting the efficient routing scheme to obtain best performance in presence of selfish users. The node that is chosen as next hop, might possibly wish to advance the packet further to their neighboring nodes. To overcome this issue, Social Selfish Aware Routing (SSAR) algorithm is used here. Two perceptions are made on selfish user nodes in SSAR. These selfish users generally wish to transmit the message to different clients, who are socially tied with them. When a node has limited resource, it forwards only the packets that are received from strong ties. But when received from weak social ties, the chances of forwarding to destination are less. To maintain good routing performance SSAR checks whether the node is willing to forward or not. Additionally, allocates the bandwidth and buffers based on packet priority. Each node will have different priorities of willingness for further transmissions. If the node is willing to forward, a value will be assigned as one, on the off chance that not, at that point zero. The default value for stranger is set to be zero. If in case, the next hop to be examined is genuine, yet isn't experienced earlier, then the priority of packet to be sent will be diminished. This prompts delay in transmission.

Authors of [8] developed routing scheme on intermittently connected mobile network (ICMN). It is a wireless network with no ensured path between source and destination. If any path discovered, we cannot say it is the stable one, since the nodes are not steady. Researchers suggested making use of a routing method known as flooding based routing scheme, to deal with such network. This technique prompted wastage of lot of energy and bandwidth, which was the purpose behind performance degradation. To take care of this issue, another routing strategy was proposed called as spray and wait. This overcomes the problem of delays and lack of energy efficiency. To achieve the average delay, the number of message copies that spray and wait phase require is calculated by using an analytical method called binary spray and wait. Initially, certain exact number of message copies are generated and forwarded to the same number of nodes. In spray phase, the source node starts forwarding the messages until it perceives enough message copies are forwarded that guarantees, at least one of those received node would be the destination. If destination node is not found even after spray phase, wait phase is executed. Every node that had gotten the duplicate of message will currently transmit message straightforwardly to its destination. But, if one or more node is in contact with destination, then the end node receives duplicate copies, due to which the buffer and energy is squandered.

Flooding based routing scheme have many drawbacks, hence author of [9] have focused on single copy routing methods. In this strategy the message is replicated just once. It is useful when the nodes in the network have limited resources. Also to design multiple copies routing schemes. Above all the drawbacks of DTN, there are few preferences like store and forward mechanism. Routing is a successive independent forwarding decision made on the basis of current and future connectivity information. Based on the number of times the message is replicated to forward into

 DOI : 10.35291/2454-9150.2019.0132

network, routing is classified into single and multiple copy schemes. In single copy scheme, the message is imitated just once and single node can carry it at a time. The node which holds the message is called custodian. The current custodian can forward the message to next hop, which turns into the new custodian of the message. This proceeds until the message reaches the destination node. But if any selfish nodes are present in the network, then there is a chance that the message never reaches its destination. In multiple-copy scheme, the message undergoes many replications and all the copies are flooded into the network. For this situation the message might be dropped, because of exceptionally high traffic load of network.

Authors of [10] have used quota based routing, which demonstrates great execution in delay tolerant network. Initially, the network should be examined for active nodes, which can be evaluated by metric called contact density. Each message here is given with a quota value. These values will help in restricting the intemperate message replication. In this routing, initial quota values for messages will be generated by source node. Each node in the path duplicates the message in its buffer and forwards the copy to the next hop. When the message reaches its quota value, it cannot be further replicated and is directed to destination. To get better routing performance the assignment of initial quota value plays an important role. The value depends on load of network and gradually decreases as relayed. Since the topology of network is not stable, assigning the value is a troublesome assignment. Hence, they have considered Dynamic quota based routing protocol. In this protocol the custodian can adjust the quota value of message. Adjustments are made based on the network condition. If the quota values are assigned more, than number of replication exceeds. Assuming less, then reaching destination would be difficult.

Few drawbacks of delay tolerant network are tackled by the models discussed above. serious issues like, increase in communication cost, presence of malicious nodes in network, delay in packet transmission and so on, are considered individually in above methods and illuminated to some extent. But Reputation based framework can overcome all these problems by its trust model. In reputation model, before transmitting the data to next hop, the custodian examines the history of its next node. This solves the issues of malicious users. In light of this, the number packet loss in network will be diminished, which in-turn decreases the communication cost, since re-transmission of the packet isn't vital. To characterize delay and ratio of current message delivery, more comprehensive set of performance metric is considered.

III. PRELIMINARY

Reputation based model intends to accomplish accurate end node's trust evaluation and exceed the number of correct messages conveyed to the destination. By recognition and perception towards the previous message carrier, RBTA will appreciably reduce the communication cost. Exact trust calculation in the network like DTN is meagrely difficult. Direct interactivity between nodes is very less experienced in this environment. Due to which continuous evidence collection is preposterous. Hence, the calculation of trust results in error. Rather, reputation based model allows collection of information either by direct or indirect evidence. These evidences are treated in a Bayesian way and are collected through message exchange, even for nodes that are not met for long stretch of time. In this method, the evidence is viewed as positive, negative or neutral on trust scale [0,1]. If node is not trustworthy, the value will be zero (negative) and the other way around. But, if the node could not monitor its neighbour in short contact time, then it is uncertain. Multidimensional trust is used to characterize a DTN node, which incorporates trust dimensions like, competence, availability and integrity using reputation based information. Few attack scenarios that occurs in DTN are discussed. Specially, in cases like the reputation information are modified by the attacker, or may be dropped [11]. Stochastic petrinet model is used here, to identify the trust threshold value of message carrier to accomplish trust dimensions.

IV. CONCLUSION

In this paper, diverse issues under DTN and methods developed by various authors to overcome the network problems are investigated. The proposed Reputation Based Trust Assurance model acquire better trust appraisal for assessing the trust by leveraging the reputation information provided by intermediate message carrier during transmission. As a future work, we focus on accomplishing higher performance of correct message conveyance.

REFERENCES

[1] Thrasyvoulos Spyropoulos, Rao Naveed Bin Rais, Thierry Turletti, Katia Obraczka, Athanasios Vasilakos. Routing for Disruption Tolerant Networks: taxonomy and design. *Published at Springer*. September 2010

[2] Paritosh Puri, M.P Singh. A Survey paper on Routing in Delay-Tolerant Networks. *National Institute of Technology, Patna*. June 2013.

[3] Vania Conan, Jérémie Leguay, and Timur Friedman. Fixed Point Oppurtunistic Routing in Delay Tolerant Networks. *IEEE JOURNAL ON SELECTED COMMUNICATIONS*. June 2008.

[4] Elizabeth M. Daly, Mads Haahr. The Challenges of disconnected delay-tolerant MANETs. *IEEE/Department of Computer Science, Dublin, Ireland*, August 2009.

[5] Jin-HEE Cho, Ing-Ray Chen. PROVEST: Provenance-Based Trust Model for Delay Tolerant Networks. *IEEE*

 DOI : 10.35291/2454-9150.2019.0132

Transaction on Dependable and secure Computing. February 2018.

[6] M. Grossglauser, M. Vetterli. Locating Mobile Nodes With EASE: Learning efficient Routes From Encounter Histories Alone. *IEEE/ACM Transaction on Networking.* June 2009.

[7] Qinghua Li, Sencum Zhu, Guohong Cao. Routing in Socially Selfish Delay Tolerant Network. *IEEE/San Diego, CA, USA*. May 2010.

[8] Thrasyvoulos Spyropoulos, Cauligi S. Raghavendra, Konstantinos Psounis. Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks. *Proceedings of ACM SIGCOMM workshop on DTN*.

[9] Thrasyvoulos Spyropoulos, Konstantinos psounis, Cauligi S. Raghavendra. Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case. *IEEE/ACM TRANSACTION ON NETWORKING*. February 2008.

[10] Shou-Chih Lo, Wei-Rong Liou. Dynamic Quota-Based Routing in Delay-Tolerant Networks. *IEEE 75th Vehicular Technology Conference*. July 2012.

[11] Yue Cao, Zhili Sun, Naveed Ahmad, Haitham Cruickshank. A Mobility Vector Based Routing Algorithm for Delay Tolerant Networks using History Geographic Information. *IEEE/Research University of Surrey, Guildford, UK*. 2012.

 DOI : 10.35291/2454-9150.2019.0132