International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

Multipath Routing based Reliable Delay Tolerant Network

Kanika Bhatia
Dept. of Computer Science & Engineering
NIIST, RGPV University
Bhopal, India

Mr. Ankur Taneja
Dept. Computer Science & Engineering
NIIST, RGPV University
Bhopal, India

Abstract **– Several nodes are included in a network, few nodes indicates the malignant and selfish properties. This provides the huge risks for routing in the Delay Tolerant networks (DTNs). The Delay Tolerant networks may have identical features so developing a misbehavior detection model is so complicated. Implementation of the DTN consists of the vehicular networks and the sensor networks in various sub-urban and the rural areas. This paper provides help to understand about DTN network and information regarding the misbehaviors and the issues in the DTN network along with the new method for DTN. This method is implemented in NS2. The results show the better performance of the proposed work over existing work.**

Index Terms—Delay, Tolerance, Network, Trust, NS2.

I. INTRODUCTION

Along with the uncontrollable development in the wireless devices, several new environments of network have been raised. Few of those environments consist of the military/tactical, satellite and interplanetary, disaster rescue networks and disconnected remote village. Those types of fresh environments have now evolved into more conspicuous along with the current natural calamities. The requirement to develop the interaction to help the applications which gets executed in those types of severe environments has not been very clear.

This is resulting in an advance set of the presumption requirements that are to be taken into account like intermittent connectivity, large delays and the destination as the most significant one. These types of new issues and the presumptions have prompted so many researches in these severe and portable environments. Researchers in the Mobile Ad Hoc NETworks (MANETs) have been handled portability issues with the main target on the routing in MANETs, although, it fails to refer all the arising issues in absence of the end-to-end path from the source, as they consider only the scenarios in which the end-to-end path presents from the source to the destination.

Within the delay tolerant network the interaction is allowed only even if the end-to-end link is not found to be achievable. Nodes of DTN that are exploiting the mobility and using the store-carry-forward pattern, DTN is one of the new type of the network that are separate from the other types of networks. Delay-tolerant networking (DTN) is a method to the architecture of computer network which searches to refer the technical problems in the heterogeneous networks which may short of the continuous network links.

DTN is also an ad hoc wireless network and it has the features like long or variable delay, intermittent connectivity and the low delivery ratio. Therefore, the routing in these kinds of the network is complicated. In the sparse mobile adhoc network, the mobile density is very low and there is also the links in between the nodes in the network which doesn’t found continuously therefore the network graph is connected rarely. Message delivery in the delay tolerant network should be delay tolerant. DTN structure needed to store the messages in the non-volatile memory types when the reliable delivery of the message is needed.

II. MANET

This method is an ad-hoc networking in between the users who are wishing to interact with each other. Packets gets delivered from the source to the destination in the ad-hoc network are limited in the range than to the cellular network but it has many merits over the cellular network. Mobile ad-hoc network (MANET) is a type of self-organizing mobile network where every device is independent to revolve freely in any of the direction and also modifies its links to the other devices regularly.

The ad-hoc networks are never dependent on any of the pre-established architecture hence they may be even gets installed on any places having no infrastructure. These types of networks suppose that an end to end path in between the nodes is present. They are mostly designed on-the-fly or for one-time or for using temporarily. They also assume their uses in the various special applications such as disaster relief, military, etc which are in the requirement of creating a fresh infrastructure less network along with the entire previous infrastructure that are being get destroyed.

III. VARIOUS ISSUES OF MANET

The network MANETS fixed some new issues for the security of network and their requirement of a specific type is to give more attention to security issues which affected on network. Below are few of the related issues in the security of the mobile ad hoc networks:

1. Nodes Acting as Routers: As the nodes themselves are taking part in the forwarding of the messages, then any of the malignant nodes in network may get misused easily the traffic of message either by dropping the messages or by creating the false messages etc.
2. Limited Resources: Because of the limitation of the resources of network in the mobile ad hoc networks, several cryptographic solutions are applicable to the wired networks that are not applicable directly. Hence there is a requirement for the new solutions for security that may find in their application within this complex domain.
3. Mobility of Nodes: Changing the network topology dynamically may results in the more chances for the malignant nodes to the attack.

4. Location of Nodes: As the Ad hoc networks are created for the purpose of the deployment of environment that may not be much secured. As an example, the nodes that are deployed in battlefield or in forests for tracking the wild animals etc. can invite various security issues and various attacks.
5. Wireless Medium: Interoperability is one of the very easy patterns in the wireless medium. Hence, there is shortage of the privacy and some important messages may be got eavesdropped and get modified easily.
6. Delay Tolerant Network: To control the misbehavior of the nodes in the fundamental mobile ad-hoc network uses various techniques like destination acknowledgement or neighborhood monitoring. These will decreases the rate of packets delivery and also generates a big issue against the network performance of the DTNs [11].

IV. LITERATURE REVIEW

Delay-Tolerant Networks (DTNs) are one of the special kinds of the network environments which are subjected to the delays and the disruptions. Many efforts of the researches on DTN routing issues are targeted on the unicast routing but not on the multicast routing. Additionally the previous DTN multicasting methods are not effective and flexible. In this paper, it is suggested a new method of multicast routing method that cannot achieve only a high delivery rate but it also accept to the network situations. Very importantly, the suggested method required not to maintain the group membership.

Also it can be present that any of the interested users may join independently and leave any of the multicast groups, and these properties are properly suits into the DTN environments. In this paper, it is suggested an ideal multicast routing protocol for the DTNs. This protocol also has an extreme property in which the cost of maintenance of the group membership is not required. That is what this suggested protocol does not participate in the process of the joining invitations and also for leaving notifications.

Consequently, it also takes an advantage of contact behavior in the environments of DTN to anticipate the good nodes for relaying message which can help to forward the messages to their destination places. The suggested quota-based routing may got adjust dynamically with the number of copies of the message which are generated based on the current situations of the network [1].

A network of communications which is have the ability of temporarily storing the multiple packets in the intermediate nodes, till the time of an end-to-end route is get established again or get regenerated is called as the delay tolerant network (DTN). The routing of packets in the DTN is dependent on the store-carry-and forward pattern. When the node get receives a message but there is no availability of the paths towards the destination node, then the message must be get buffered in current node and also wait for the chance to get encounter to the other nodes.

In this paper, it was introduced a delay tolerant network along with their properties like the intermittent connectivity or the limitation of resource and heavy delay rate. And here also suggested the open routing challenges in the security of Delay Tolerant Network. The previous routing protocols in the DTNs are further categorized into their strategies for controlling the message copies and for making the forwarding decision. Here also has made a brief analysis in the performance of the efficient routing protocols. [2]

By gathering the routing proves from the given nodes, the TA can checks the node regarding its nature then it performs the suitable actions associated with the behavior of the nodes. TA provides the security of the DTN routing at a lower cost. The probability of detection is associated with the reputation of node which provides the dynamic detection probability dependent on trust of the users. The result of the simulation presents that suggested model is effective for establishing the trust with DTNs.

The proposed probabilistic misbehavior detection scheme (iTrust), which reduces the misbehavior detection overhead effectively. The scheme is modeled as the inspection game and shows the appropriate probability setting and gives the security of DTNs at lower overhead and provides the trust in the path of DTNs. The simulation results can gives the reduced transmission overhead provided by misbehavior detection and detects the malicious nodes effectively. The future work will focus on the extension of iTrust to other kinds of networks.[3]

Probabilistic routing has limited local view of the network. So, most of the time, it cannot select better forwarder to route the message. Epidemic routing floods the message into the network. It requires more network resources. In social based routing, each node possesses a social map of its surrounding social network to select the forwarder.

In this paper we have discussed different routing algorithm in delay tolerant network. Routing algorithm such as social based routing where nodes social network is created. Each node maintains its social map of surrounding social network. Social network is used to select the forwarder in a network. This algorithm selects better forwarder than the other routing algorithms. [5]

The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme. Delay Tolerant Network(DTNs) are a class of unique network characterized like lack of guaranteed connectivity ,typically low frequency between DTN nodes and long propagation delay within the networks.[5] Existing routing algorithms for DTN assumes that nodes are willing to forward packets for others but in real word selfish and malicious behaviors occurs while forward packets for nodes.

Due to unique characteristics the message propagation process DTNs follows a Store-Carry and Forward manners. We model it as the inspection game and show that an appropriate probability setting could assure the security of the DTNs at a reduced detection overhead. Our simulation results confirm that iTrust will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively. Our future work will focus on the extension of iTrust to other kinds of networks.[6]

Probabilistic routing performs well in such networks and has been the dominant focus of research in this area. However, creating efficient routing protocols is challenging because to reduce latency, one often needs to replicate messages thus increasing routing overhead. Network co ding has been explored as a way to increase throughput in DTNs without a significant increase in overhead, and network coded routing approaches have shown promising results.

Additionally, we intend to improve the scheduling of receive and send processing, since our current implementation tends to fall behind processing received bundles. Also the initial bundle fragmentation and decoding tasks could be moved outside the event thread, which currently slows sending and processing bundles. Finally, when a link becomes available, we use a fairly na¨ıve algorithm to select the collection from which to generate an encoded fragment. [7]

In this paper, we study DTNs in which malicious nodes are present, to which we refer to as *compromised DTNs*. We discuss and analyze the effects of presence of malicious nodes on routing of messages in compromised DTNs. We propose a two period routing approach which aims at achieving the desired delivery ratio by a given delivery deadline in presence of malicious nodes.

Our simulation results with both random networks and real DTN traces show that, with proper parameter setting, the proposed method can achieve delivery ratios which surpass those reached by other algorithms by a given delivery deadline.[8]

V. PROPOSED WORK

To improve the performance of the network against the delay in network, there is variety of works. This proposed work is meant for the MANET environment. In this work, we have giving emphasis on the reliability of the protocol while handling the delay tolerance in the network.

The proposed work architecture is shown in figure 1.

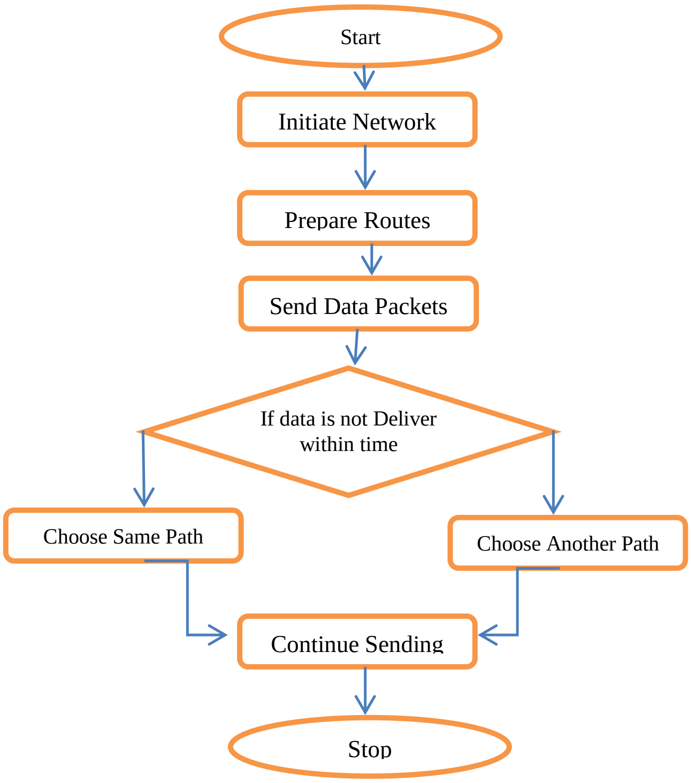


Figure 1: Proposed Architecture

VI. SIMULATION AND RESULTS

This simulation is done on NS2. The simulation area is 1000m * 1000m. Beside of this there are some more influencing parameters which are describe in table 1.

Table 1: Simulation Parameters

Property	Values
set val(chan)	Channel/WirelessChannel
set val(prop)	Propagation/TwoRayGround
set val(netif)	Phy/WirelessPhy
set val(mac)	Mac/802_11
set val(ifq)	Queue/DropTail/PriQueue
set val(ll)	LL
set val(ant)	Antenna/OmniAntenna
set val(ifqlen)	100
set val(nn)	40
set val(rp)	AODV
set val(x)	1000
set val(y)	1000
set val(stop)	60

This simulation runs for 60 seconds and there are total 40 nodes in the MANET.

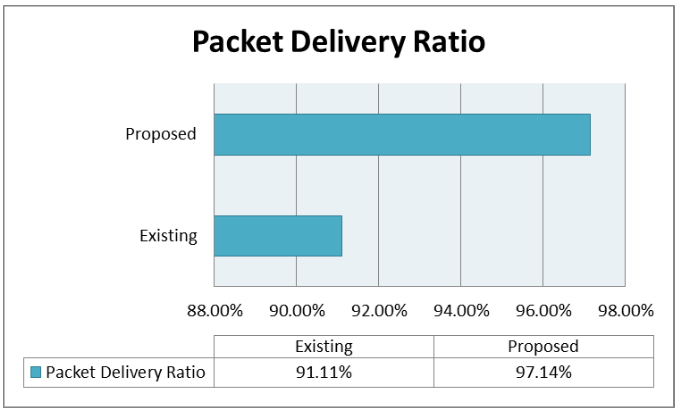
We have compared the performance of the proposed work on following parameters:

1. Packet Delivery Ratio
2. Routing Overhead
3. Throughput of the network
4. Average End-to-End delay

Table 2 show the PDR of proposed work with respect to existing work.

TABLE 2: Comparison of Packet Delivery Ration

	Existing	Proposed
Packet Delivery Ratio	91.11%	97.14%

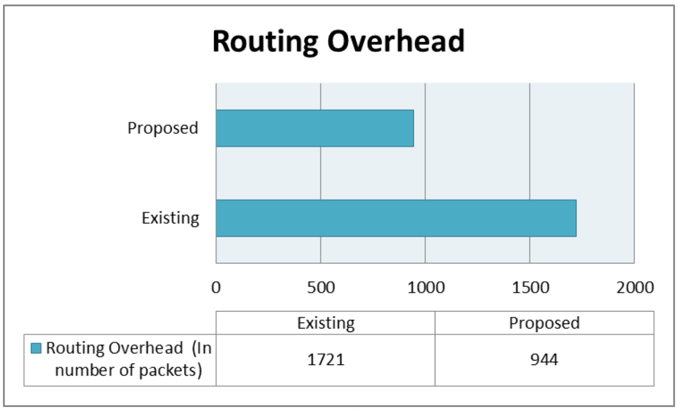


Graph 1: Comparison of Packet Delivery Ratio

Table 3 shows the Routing Overhead of proposed work with respect to existing work.

TABLE 3: Comparison of ‘Routing Overhead’

	Existing	Proposed
Routing Overhead(In no. of packets)	1721	944

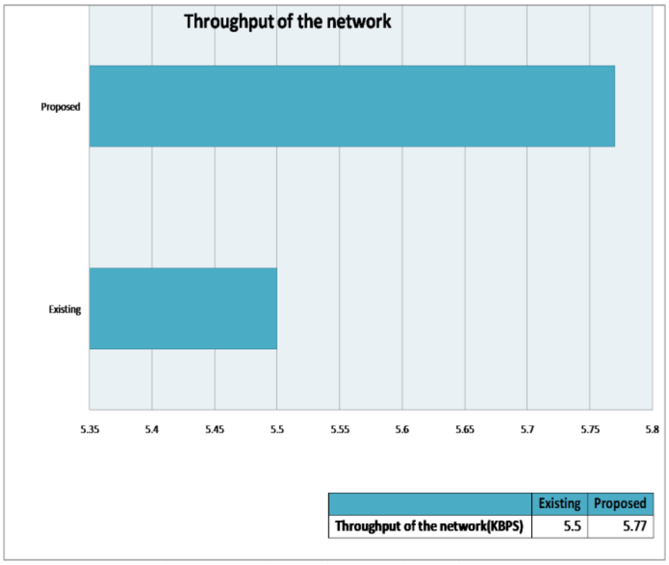


Graph 2: Comparison of ‘Routing Overhead’

Table 4 shows the ‘Throughput of Network’ of proposed work with respect to existing work.

TABLE 4: Comparison of ‘Throughput of Network’

	Existing	Proposed
Throughput of the network(KBPS)	5.5	5.77

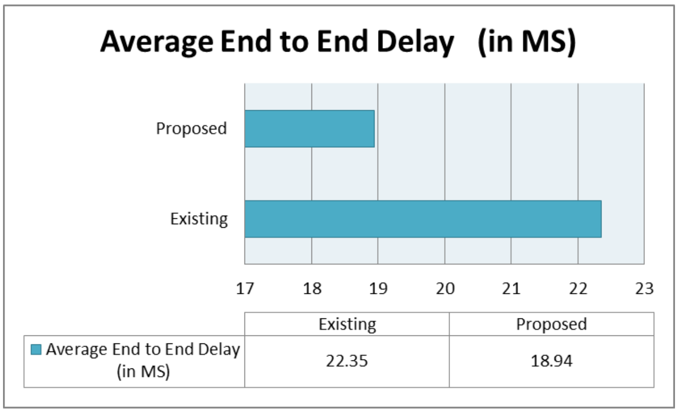


Graph 3: Comparison of ‘Throughput of Network’

Table 5 shows the ‘Average End to End Delay’ of proposed work with respect to existing work.

TABLE 5: Comparison of ‘Average End to End Delay ’

	Existing	Proposed
Average End to End Delay (in MS)	22.35	18.94



Graph 4: Comparison of ‘Average End to End Delay’

VII. CONCLUSION

DTN is delay tolerant network in which there is no end to end path. Hence routing in such network is difficult. We propose a Reliable based algorithm, which could reduce the detection overhead effectively. In this paper we introduced the various performance issues related to the DTN network. In this paper, we have considered transport layer issues, specifically reliability. Table 2,3,4 and 5 along with graph 1,2,3 and 4 clearly show that the performance of the proposed work is much better at various aspects.

REFERENCES

[1] Lo, S. C., Chiang, M. H., Liou, J. H., & Gao, J. S. (2011). Routing and buffering strategies in delay-tolerant networks: Survey and evaluation. In Proceedings IEEE ICPP Workshop, (pp. 91–100), Sept 2011.

[2] Y. Cao and Z. Sun, “Routing in delay/disruption tolerant networks: A taxonomy”, Survey and Challenges IEEE Communications surveys & tutorials, **(2012)**, pp. 1 -24.

[3] H.Zhu, S.Du, Z.Gao, M.Dong, Z.Cao, “Probabilistic misbehaviour detection scheme toward efficient trust establishment in delay tolerant networks.” *Proc. IEEE INFOCOM ’14*, Jan. 2014.

[4] Kang Chen, Haiying Shen, “SMART: Utilizing Distributed Social Map for Lightweight Routing in Delay-Tolerant Networks”, IEEE/ACM Transactions on networking, 2013.

[5] Q. Li and G. Cao, “Mitigating Routing Misbehavior in Disruption Tolerant Networks,” IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr.2012.

[6] A. Mary Judith, V. Anusha, S. Vinod”An iTrust Based Misbehaviour Detection Technique on Clustered Nodes in Delay Tolerant Network” in IJERDT in 2014.

[7] E. Altman, F. De Pellegrini, and L. Sassatelli. Dynamic control of coding in delay tolerant networks. In Proc. of INFOCOM, 2010.

[8] F. C. Choo, M. C. Chan and E. Chang, *Robustness of DTN against Routing Attacks*, in Proceedings of Second International Conference on ommunication Systems and Networks (COMSNETS), pp. 1-10, 2010.

[9] S. Adali, R. Escriva, M. Hayvanovych, M. Magdon-Ismail, B. Szymanski, W. Wallace and G. Williams, *Measuring Behavioral Trust in Social Networks*, IEEE International Conference on Intelligence and Security Informatics (ISI 2010) pp. 150 - 152, Vancouver, BC, May 23 - 26, 2010.

[10] Villalba Luis Javier García , Matesanz Julián García , Orozco Ana Lucila Sandoval 1,3 and Díaz José Duván Márquez,"Auto-Configuration Protocols in Mobile Ad Hoc Networks",The 11th International Workshop on Knowledge Management and Acquisition for Smart Systems and Services (PKAW 2010)

[11] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," *IEEE Trans. Wireless Comm., vol. 9,* no. 4, pp. 1483-1493, Apr. 2010.