ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse45842019.pdf
https://doi.org/10.30534/ijatcse/2019/45842019

Relay Selection Trust Management (RSTM) model for Delay Tolerant Networks

Kiran Babu T S[1], Dr. Sanjay Chitnis[2]
[1] Dept of CSE, CMR Institute of Technology, Bangalore India , kiran.ts@cmrit.ac.in
[2]Dept of CSE, Dayananda Sagar University, Bangalore India, sanjay.chitnis@gmail.com

ABSTRACT

Increased demand for wireless communication required efficient quality of communication. Nowadays, wireless communication ns where end-to-end connectivity from source to destination is a crucial task such as interplanetary networks, vehicular networks, underwater networks, etc…In order to address these issues, DTN (Delay Tolerant Networks) have been introduced which helps to enable the end-to-end connectivity between source and destination by using a store-and-forward mechanism. However, the connectivity and performance of conventional DTNs suffer from the issue of unreliable environments, high dynamics of nodes and power consumption. Moreover, security is also considered a challenging task in these networks. Thus, in this work we focus of these issues of DTN and introduce a novel hybrid approach which provides an efficient solution for relay selection, buffer and, trust management scheme, this scheme is called as Relay Selection Trust Management (RSTM) model for Delay Tolerant Networks. The performance of the proposed approach is compared with the existing techniques such as Epidemic routing, Game theory, and spray & waits approaches. The experimental results show that the performance of the proposed approach RSTM achieves better performance in terms of packet delivery, delay, communication.

Key words: DTN, QOS, RSTM,. Trust management protocol**.**

1. INTRODUCTION

Recently, the demand for wireless communication has increased drastically and it is widely adopted in various types of real-time communications. In the current era, numerous devices are connected through wired and wireless networks over vast distances. For example, cellular networks where cell phones are connected to the different types of servers around the world. These type of communication standards widely adopted due to their significant performance but these networks face some challenges such as end-to-end connectivity from source to destination with the help of intermediate connectors. However, these assumptions can be violated easily due to several aspects of the network such as node mobility, excessive power consumption, and unreliable networks. In order to deal with these issues, a new networking scheme is developed which is called as Delay Tolerant Networking (DTN) which helps to improvise the network coverage. This is considered as a promising technique for enabling communication in challenged networks such as deep space networks, sensor networks, and mobile ad-hoc networks, etc. The main aim of this approach is to mitigate network disconnections [1].

Delay Tolerant Networks (DTN) [2] is a new communication prototype which performs as the decentralized and distributed manner for communicating devices which are connected dynamically. This type of networks addresses several challenges related to network connectivity such as high latency, sparse connectivity, delay, asymmetric data rate, and end-to-end connectivity. According to DTNs, a store-and-forward scheme is applied for packet transmission and a bundle layer is used to provide the interoperability in heterogeneous networks. In DTNs, the source node generates a packet which is forwarded to the intermediate nodes which are closer to the destination node. In some cases, when no connectivity is available, then the intermediate node stores the data packet and the complete process of data transmission is repeated hop by hop until the message/packet is transmitted to the destination node [3]. Based on these significant advantages of DTN, these networks are widely adopted in several scenarios such as ZebraNet [4] for wildlife tracking, vehicular networks [5], underwater networks [6], and interplanetary networking [7], etc.

Despite several applications of these networks suffer from various challenging issues which can degrade the overall performance of the network. The main open challenges are key management in DTN, Replay handling, data traffic analysis, routing security, multicast security, and performance issues. However, several schemes have been introduced during the last decade to overcome these issues. These approaches include several aspects to improve the DTN performance. According to the concept of DTN, the store-and-forward mechanism is used which shows that

packets are transmitted in an opportunistic manner however, this mechanism can be violated due to some security attacks or malicious nodes. Hence, Zhu et al. [8] presented a security provisioning approach for DTNs called as SMART which is implemented in a distributed process and helps to prevent different types of attacks. This study shows that security is one the key component of in DTNs. The conventional approaches assume that link between communicating nodes is stable and do not fail frequently but due to high dynamics in real-time scenario these assumptions can be violated hence Singh et al. [9] focused on the security issue and presented a novel trust based secure routing using Artificial Neural network for DTNs. Similarly, Guo et al. [10] discussed several issues on different communication layers in DTN and also presented an evolutionary game theory approach for security in DTNs.

On the other hand, various studies are presented to address performance-based challenges. Generally, the complete performance of the system depends on the routing. Jain et al. [11] presented an improved version of store-and-forward based packet forwarding and buffer management scheme using Fuzzy logic approach. This approach works as a spray and wait for a routing protocol to incorporate the buffer management approach. For efficient packet delivery, shortest path routing is considered as a contemporary promising approach to improve the network performance. Stewart et al. presented CASPaR approach to address the congestion avoidance shortest path algorithm for DTNs. The main aims of this approach are identifying the direct routes from source to destination, congestion avoidance, topology correction, and latency minimization to improve the overall network performance [12]. These networks are applied for satellite communication where authors in [13] addressed QoS performance issues and developed a storage-Time-aggregated approach for QoS enhancement in satellite communication. However, the complete performance of these techniques depends on the network characteristics. Some of the network characteristics we discuss in the following subsection.

1.1 DTN Characteristics

Generally, DTN is a group of several computing systems which are participating in the network formulation, are called as nodes. These nodes are connected via one-way links. As discussed before, due to the mobility of nodes or other issues, the network connectivity may get affected which can lead to the downgrading of the link. Sometimes when the link connectivity is high, then the node has the maximum probability to transmit the data packet. This opportunity of transmitting the packets is called as contact [1]. In the network, contact set is formulated which represents the availability of the total number of contact times during. Generally, this is expressed with the help of graph theory where it can be represented as time-varying multi-graph. In conventional DTNs, the data packet is transmitted through each hop where each packet has to wait until the next hop is available or free. This can cause long waiting time at the nodes. This process of transmitting the data packet from one node to another node is divided into four stages such as time to wait, queuing time, delay in transmission and propagation delay [14]. Waiting time is the total amount of time for a data packet to wait between its arrival and contact to the next hop when it is available. Queuing time represents the total time to drain the high priority messages in the buffer. Transmission delay represents the time taken for transmitting all bits in the message and propagation delay represents the time taken to transmit a data bit through the connection.

1.2 Contribution of work

Several techniques have been introduced to improve the performance of Delay Tolerant networks, but due to an increasing demand for efficient communication, the complexities in the implementation also have increased. Moreover, the mobility and connectivity issues also become a challenging task hence, in this work we present a novel approach to address the performance issue of DTN. The main contribution of the proposed approach is as follows:

(a) Development of relay selection scheme for DTNs
(b) Development of buffer management scheme for reducing the delay
(c) Development of trust based model for security
(d) A comparative study to show the robust performance of the proposed approach.

1.3 Article organization

The complete article is organized as follows: section II presents a brief discussion about recent techniques in this field of DTN. Section IV presents the proposed QoS and security enabled model for DTNs. Performance analysis and comparative study are presented n section V and finally, section V presents concluding remarks.

2. LITERATURE REVIEW

In this section, we present a brief discussion about recent approaches in the field of DTN routing which are used for improving the communication performance in terms of QoS and security.

Dias et al. [15] studied vehicular networks and focused on the security aspects in VANETs. In this work, vehicular networks are considered as delay tolerant networks where an end-to-end path is not always available which can cause frequent packet drop and delay. In order to overcome this issue, cooperative relay based approach is developed where all nodes follow the same routing process, however, due to

malicious nodes, this protocol can be violated hence, and authors presented watchdog system to detect the node misbehavior. In [18] also vehicular networks are considered and DTN based communication approach is implemented to improve the overall communication delay tolerant networks. In this work, authors considered a huge scenario of deployed road-side units (RSUs) and identified that the contact time duration between vehicle and RSU follows an exponential distribution whereas contact rate follows a Poisson distribution. Based on these assumptions, data replication for RSU based problem is analyzed where an opportunistic data dissemination approach is considered for transmitting the data. In other words, a contact-aware RSU aided vehicular mobile data transmission NP-hard optimization problem is formulated and a heuristic solution is provided to this considered problem.

Mobility is also considered as a challenging issue in DTN communication which can cause frequent disconnection between links. In order to address this issue, Zhang et al. [16] studied mobility and its impact on networks. These works present a mobility prediction based routing scheme for DTNs where node mobility and spatial information are considered for performance consideration. In order to describe the mobility, a semi-Markov model is implemented. Yu et al. [17] developed a hybrid approach for message delivery probability and message redundancy for DTN to reduce the communication overhead and improve the high message delivery rate. In these networks, contact duration and frequency plays an important role which are used for computing the message delivery probability in the considered network. Later, message copies are assigned to the source node and later these copies are used for the relay node to generate the binary tree of the data transmission. For these type of problems, several optimization solutions are present which can be helpful to achieve the efficient solution. Based on this assumption, Johari et al. [18] developed a novel approach to address the issues of delay in DTN communication, this approach is called as Licklider transmission protocol convergence layer (LTPCL) which is developed with the help of several meta-heuristic approaches such as genetic algorithm and ant colony optimization along with the shortest path routing scheme. Liu et al. [20] focused on the delay and congestion problems in the delay tolerant networking. In order to focus on this issue, an improved Socially Aware Congestion Control algorithm (SACC) approach is developed where a social congestion metric is formulated based on the social features and congestion level. In this approach, if the congestion state occurs then the link cost is computed and the packet is dropped with the minimum link cost. In [21] Veas-Castillo studied about message delivery issues in DTNs for disaster scenarios. In order to overcome this issue, a novel approach called *MinVisited*is developed which helps to find the optimal path from source to destination by selecting the best path to identify the next node based on these two features, the distant Neighbor and largest number of encounters with the destination node. This helps to achieve the most suitable minimum path. Prabha et al. [22] used delay tolerant network routing in wireless sensor network scenario. Generally, WSNs suffer from network lifetime and energy efficiency issues. In these networks, energy holes problem occurs which causes a massive degradation in network energy, hence, Energy Efficient Energy Hole Repelling routing algorithm is presented in this work. According to this process, large cluster is formed away from the sink whereas smaller clusters are formed near the sink node and cluster head is selected based in the residual energy and less distance.

3. PROPOSED MODEL

The In this section, we present the proposed solution to overcome the issue of DTN such as energy efficiency, network overhead, and security. Here our main aim is to improve the overall performance of the entire network system where total number of heterogeneous mobile nodes is present in the network deployment area. Let us assume that available nodes are equipped with the limited storage and finite bandwidth which is used for communicating with other nodes. Each node can transmit the packets to the other neighboring node when both nodes are in the predefined communication range. Here, we assume that nodes have a copy of information during transmission which can help to improve the reliability of the communication. The messages can be transmitted in short contact duration which does not require multiple attempts to transmit the packets which are of same size and un-fragmented. Each message is associated with its TTL (Time-To-Live) value, if the TTL of any message packet is expired, the message is discarded by the associated nodes.

Based on these assumptions, we present a routing protocol for short contact communication system to address the issues of relay selection, buffer management, and trust evaluation. These three key components are analyzed before transmitting the packet in the deployed network.

3.1 Relay selection scheme for DTN

Let us consider that a mobile node contains message stored into its buffer which needs to be transmitted to the destination . Before transmitting the packet, the node analyses the environment to discover the neighboring node . Hence, each neighboring node identifies the all possible routes based on the minimum delay as from neighboring node to destination . Hence, the minimum delay between to can be given as

$$Dela\,y_{Min}(s,d) = E\left[\min_{i\in\{1,\dots,n\}}(I_{s,i} + Dela\,y_{Min}(v_i,d))\right]$$

Where represent the intercontact between source node and its neighboring node , $\forall_i \in \{1,\dots,n\}: Dela\,y_{Min}(v_i,d) \leq Dela\,y_{old}(s,$ and Del . Let us consider that $\hat{v} = \arg\min_{i\in\{1,\dots,n\}} Delay_M$. Hence, the

message can be replicated to the node by following constraint, which can be expressed as:

$$Dela\,y_{Min}(\hat{v}, d) < Dela\,y_{Min_{new}}(s, d)$$

Let us assume that is a random variable which represents the minimum delay based on the maximum possible routes with the help of its neighboring node. Hence the can be denoted as:

$$\mathbb{D} = \min_{i \in (1,\dots,n)} (I_{s,i} + c_i)$$

Where is the known quantity of Here we assume that random variable interconnects rate is which varies according to the node configuration and the rate of interconnect is independent for any pair of communicating node. With the help of these parameters, the closed-form function can be expressed in the form of the probability density function of as follows:

$$f(x) = \begin{cases} 0 \; if \; 0 < x < c_1 \\ \hat{\lambda}_i . e^{-\hat{\lambda}_i x + \hat{c}_i} \quad if \; c_i < x < c_{i+1} \\ \hat{\lambda}_n . e^{-\hat{\lambda}_n x + \hat{c}_n} \quad if \; c_n < x < \infty \end{cases}$$

Where $\hat{\lambda}_i = \sum_{k=1}^{i} \lambda_k, \hat{c}_i =$, and . With the help of these parameters and probability density function the delay expectation function can be expressed as:

$$E[\mathbb{D}] = \int_0^{\infty} x f(x) dx$$

$$= \sum_{i=1}^{n-1} \int_{c_i}^{c_{i+1}} x . \hat{\lambda}_i . e^{-\hat{\lambda}_i x + \hat{c}_i} + \int_{c_n}^{\infty} x . \hat{\lambda}_n . e^{-\hat{\lambda}_n x + \hat{c}_n}$$

At this stage, each node maintains the expected delay function which is exchanged during the short contact between nodes. Moreover, these nodes maintain the inter-connect time distribution for each node and the contact rate can be expressed as:

$$\lambda_i = \frac{N}{\sum_{k=1}^{N} T_i}$$

Where T denotes the time samples for the short contact. During this short contact, finite buffers are present hence message dropping and transmission prioritization becomes a challenging task which can be resolved using relay selection methods.

Here we study about the impact of the message scheduling and message dropping on the communication delay. Before analyzing the impact, the network information such as a number of copies of the message after the elapsed time from its creation, the number of hops through which the message has been transmitted, the encounter rate between nodes which contain the replicas of the message and the encounter rate of nodes which have seen the message. In the deployed network, each communicating nodes maintains a communication table which is obtained through the direct connection or contact exchange between other nodes. The node maintains the communication table which contains the following information about node k: a node id, list of messages which have been seen by the nodes, and last updated time information. On the other hand, message data also maintains the metadata which is message ID, message delivery status as the message is in buffer or message is dropped, elapsed time, remaining time, and encounter rate between k node and a destination node for message m. During this process of node contact, the required information such as node ID, and message list is exchanged, moreover, network state information such as total number of available message copies in the elapsed time T_i since creation of message packet, number of nodes through which message has been transmitted and the nodes have the message information and the node encounter rate. In this stage also, the network related information is exchanged between the communicating nodes and the information related to a node such as a node ID and message list is updated according to the given time duration. In order to identify the suitable path optimal path, we develop a model to compute the delay utility. Let us consider that $\mathbb{D}$ denotes the delay to transmit the data packet, the expected delay delivery can be given as:

$$E[\mathbb{D}_i] = P[no\; dlivery] * E[\mathbb{D}_i | \mathbb{D}_i > T_i] + P[Message\; dlivery] * 0$$

For simplicity, we assume that the message is delivered directly to the destination and the first replica of the message is transmitted towards the destination using exponential distribution as $\hat{\lambda}_{d_i} = \sum_{l \in n_i(T_i)} \lambda_{d_i}$. Hence the expected message delivery can be expressed as:

$$E[\mathbb{D}_i | \mathbb{D}_i > T_i] = T_i + \frac{1}{\sum_{l \in n_i(T_i)} \lambda_{d_i}}$$

$$= T_i + \frac{1}{l \in n_i(T_i).\Lambda_{l,d_i}}$$

Where Λ_{d_i} denotes the average rate of an encounter between nodes which is computed as $\Lambda_{d_i} = \frac{\sum_{l \in n_i(T_i)} \lambda_{d_i}}{n_i(T_i)}$. With the help of Eq. (8) and Eq. (9) we can obtain expected delay parameters as:

$$E[\mathbb{D}_i] = \exp\left(- \sum_{k \in n_i(T_i)} \lambda_{k,d_i} T_i \right) * \left(T_i + \frac{1}{n_i(T_i).\Lambda_{d_i}} \right)$$

Later, we differentiate the expected delay parameters to identify the optimal policies to improve the expected delay optimal policy which can be expressed as:

$$\frac{\partial E[\mathbb{D}_i]}{\partial n_i(T_i)} = - \exp\left(- \sum_{k \in n_i(T_i)} \lambda_{k,d_i} T_i \right) * \frac{1}{n_i(T_i)^2.\Lambda_{d_i}}$$

The above given Eq. (12) can be rewritten in the discretized form as:

$$\Delta E[\mathbb{D}_i] = - \exp\left(- \sum_{k \in n_i(T_i)} \lambda_{k,d_i} T_i \right) * \frac{1}{n_i(T_i)^2.\Lambda_{d_i}} * \Delta n_i(T_i)$$

Here $E\mathbb{D}$ denotes the expected delivery time delay for all messages, it can be summarized as:

$$\Delta E\mathbb{D} = \sum_{i=1}^{U(t)} \Delta E[\mathbb{D}_i]$$

$U(t)$ denotes the total number of unique messages in the entire network at time t. Based on the expected delay parameters, we formulate a strategy to decide three main stages of packet transmission as: (a) transmit the data packet to the next hop, (b) drop the packet and (c) store the packet in the buffer. This can be obtained as:

$$\Delta n_i(T_i) = \begin{cases} -1 \ message\ drop\ from\ buffer \\ 0\ retain\ the\ mesage \\ +1\ new\ message\ arrived\ in\ the\ buffer \end{cases}$$

Once the packet routing is performed successfully using relays, trust management becomes an important task to achieve for reliable communication. The trust management is discussed in the next section.

3.2 Trust management protocol

This section presents a trust management model for delay tolerant networks. According to the proposed approach, two types of trust characteristics are considered which are called as QoS based trust and social trust. QoS trust can be computed by analyzing the capacity of the communication network to deliver the packets successfully to the destination. In this work, we consider energy and connectivity as the important parameters for QoS trust evaluation. Similarly, social trust is considered based on healthiness and unselfishness to measure social trust. According to the proposed approach, we assume the trust level of a node which is in the range of [0,1]. We define that trust value 1 indicates the complete trust, 0.5 values indicates the ignorance and 0 indicates complete distrust. We present a trust evaluation model for node j evaluated by node i at time t which can be denoted as $T_{i,j}(t)$ which is estimated by computing the weighted average of connectivity, energy, unselfishness, and healthiness as:

$$T_{i,j}(t) = \sum_{A}^{all} w^A \times T_{i,j}^A(t)$$

Here, A represents the trust property which depends on the social and QoS trust parameters. In the present work, we develop a trust aggregation protocol where node i and node j are considered for trust evaluation in A at a time interval $[t, t+\Delta t]$ can be given as:

$$T_{i,j}^A(t+\Delta t) = \beta T_{i,j}^{direct,A}(t+\Delta t) + (1-\beta) T_{i,j}^{indirect,A}(t+\Delta t)$$

β denotes the weight parameter for trust management towards the node j in the given time interval . the considered trust evaluations factors A have a specific value of β which is subjective to $T_{i,j}^A(t)$. In (15), the direct trust node can be evaluated as follows:

$$T_{i,j}^{direct,A}(t+\Delta t) = \begin{cases} T_{i,m}^{enconter,A(t+\Delta t)} \ if\ m = j \\ e^{-\lambda_d \Delta t} \times T_{i,j}^A(t) \ if\ m \neq j \end{cases}$$

During this communication phase, if node m (encounter node) is itself j note then trust can be evaluated directly because both nodes are 1-hop neighbors. $T_{i,m}^{enconter,A(t+\Delta t)}$ is used for identifying the trust level towards node j. However, if the node j not encountered to any other new node then further information about node j cannot be accessed. Hence, the node i will continuously pass the trust information towards j over a time t decayed over the interval of Δt. In order to limit the decay, we consider a decay factor as $e^{-\lambda_d \Delta t}$. Once the node i interacts with another node, then $T_{i,m}^{enconter,A(t+\Delta t)}$ is used for assessing the trust values based on the following observations:

- $T_{i,m}^{enconter,connectivity}(t+\Delta t)$ is one of the important parameters for achieving trust and reliability during communication in delay tolerant networks. Connectivity is analyzed from node m to destination node d. If the connectivity of the nodes is high, then the good packet delivery can be obtained resulting in improved performance. The connectivity is measured based on the encounter matrix over a time interval.
- $T_{i,m}^{enconter,energy}(t+\Delta t)$ is obtained based on the energy consumption and requirement to perform the basic routing. this can be measured by computing the signal strength over a time interval of $[t+\Delta t]$ and generalizes the total remaining energy in the node m
- $T_{i,m}^{enconter,healthiness}(t+\Delta t)$: this is a measurement of node condition which provides the node information regarding its health whether a node is affected due to malicious attacks such as bad-mouthing, self-promoting, etc. which can be identified from the encounter history matrix where data is exchanged between nodes. Similarly, the bad mouthing/good-mouthing attacks can be identified by comparing the communication recommendation values from node I to Jand the attacks can be identified based on the threshold.
- $T_{i,m}^{enconter,unhealthiness}(t+\Delta t)$ this is measured by applying to overhear and snooping techniques by the node i. This helps to identify whether a node is following the assigned routing protocol in a given time duration.

With the help of the aforementioned measurements, we can build a trust model when a communicating node encounters other nodes. In this work, we have considered a trust threshold to measure the trust value i.e. if obtained trust value( ) of node i is higher than the threshold then the node is considered as a reliable relay otherwise node is discarded for current communication.

4. RESULTS AND DISCUSSION

In this section we present complete experimental study for delay tolerant networks using proposed relay node selection and trust management scheme. The performance of the proposed approach is compared with existing techniques such as Epidemic [23], prophet [24], spray and wait [25], ARAG [23] and GTMA [26]. The simulation parameters are given in Table 1.

Table 1: Simulation parameter setting

Parameter	Considered value
Network Size	10000mX10000m
Number of nodes	150
Buffer size	5-50Mb
Message Size	500 kb-2 Mb
Simulation time	100 h

Performance of the proposed approach is computed in terms of delivery ratio, average delay, and network overhead. The delivery ratio represents the overall ratio of successful packet delivery to the destination node in a given time duration.
The average delay represents the total average time taken to deliver the packet to the destination node during simulation. Similarly, network overhead is computed based on the ratio of packets which are not delivered successfully and the packets which are delivered successfully.

4.1. Delivery ratio performance

In this subsection, we present the comparative performance in terms of delivery ration where buffer size and time are varied to evaluate the performance of the proposed approach. Figure 1 shows a comparative performance in terms of the delivery ratio for varied buffer size. The complete study shows that the average delivery ratio depends on the buffer size i.e. as the buffer size increases, the overall delivery rate also increases for each scheme. The average delivery rate for each approach is obtained as 0.514, 0.422, 0.278, 0.316, 0.378 and 0.598 by using ARAG [23], GTMEA [26], Prophet [24], Epidemic [23], Spray & Wait [25] and RSTM (Proposed) approach.
The proposed RSTM approach shows significant improvement in packet delivery performance when compared with the existing techniques.

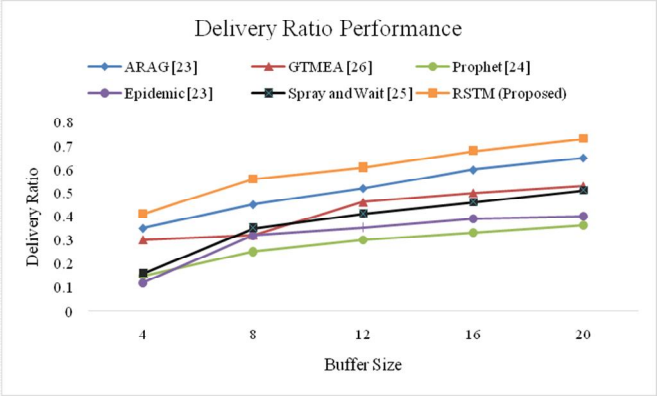

Figure.1: Delivery ratio performance for buffer size variation

Similarly, we have evaluated the performance of the proposed approach in terms of the delivery ratio for varied simulation time. The obtained performance is depicted in Figure 2.

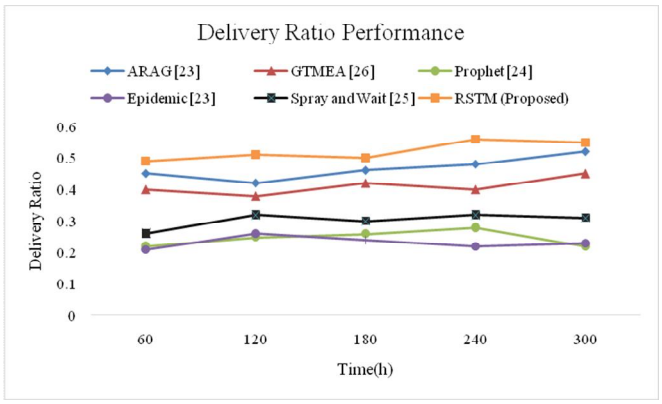

Figure 2: delivery ratio performance for time variation

The above-given figure shows comparative performance in terms of delivery ratio. In this experiment, we have evaluated the performance by varying the time parameter. The average delivery ratio performance is obtained as 0.466, 0.41, 0.246, 0.232, 0.302, and 0.522 using ARAG [23], GTMEA [26], Prophet[24], Epidemic [23], Spray &Wait[25] and RSTM (Proposed).

4.2. Delay Performance

In this sub-section, we present the comparative in terms of end-to-end delay for the varied size of the buffer. Figure 3 presents a comparative performance in terms of end-to-end delay. This study shows that the increased buffer size doesn't have a significant impact on performance. The overall performance remains the same for all variations in buffer size. According to this study, the average delay values are obtained as 3180s, 3780s, 4780s, 5220s, 4324s and 2310s using ARAG [23], GTMEA [26], Prophet [24], Epidemic [23], Spray & Wait [25] and RSTM (Proposed).

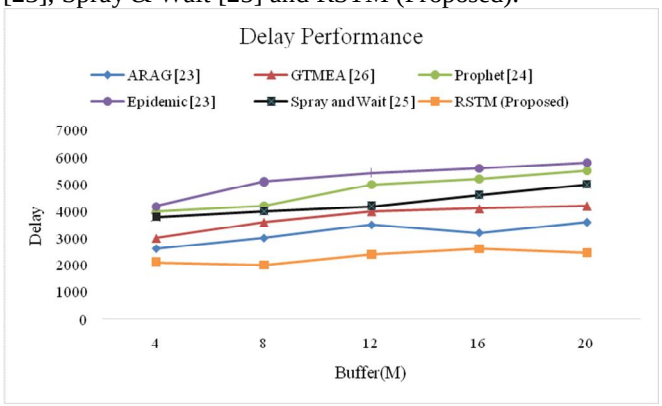

Figure.3: End-to-end delay performance for buffer variation

On the other hand, we evaluate the performance of the proposed system in terms of delay by varying the time and compared the performance of with the existing techniques. The comparative analysis is depicted in Figure 4.

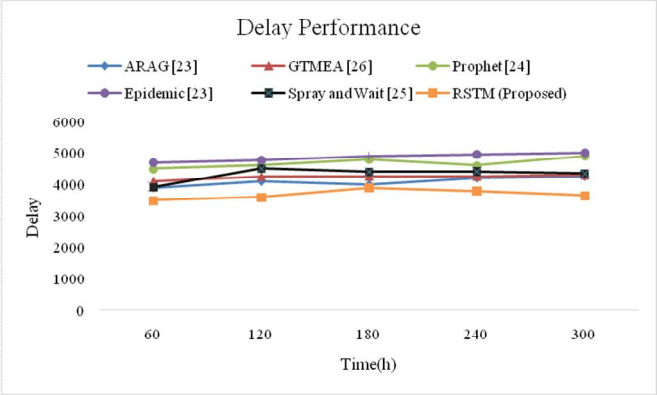

Figure.4: End-to-end delay for time variation

The above-given Figure 4 shows comparative performance in terms of end-to-end delay for time variation. However, the performance of all schemes is comparatively equal for different parameters of time but the proposed approach further reduces the end-to-end delay. According to the current experiment, the average delay performance values are obtained as 4090s, 4230s, 4680s, 4866s, 4314s, and 3690s with the help of ARAG [23], GTMEA [26], Prophet [24], Epidemic [23], Spray &Wait [25] and RSTM (Proposed)approaches.

4.3. Communication overhead performance

Here we present a comparative study in terms of network overhead by varying the buffer size and time parameters. The outcome of the proposed approach is compared with the existing techniques as discussed before. Figure 5 shows a comparative performance in terms of network overhead.

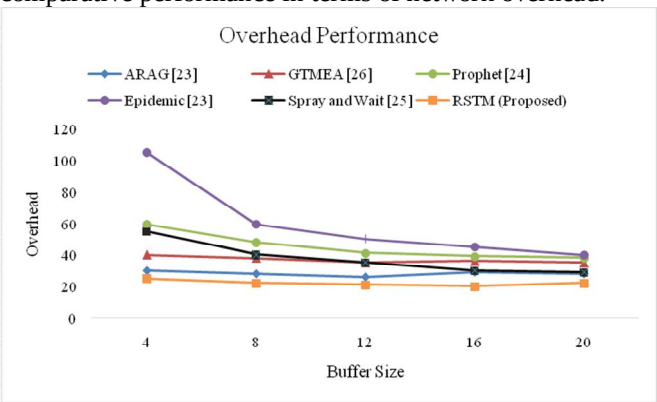

Figure.5: Network overhead performance for varied buffer size

This experiment shows that the proposed approach achieves better performance in terms of communication overhead because it has less delay and packet delivery rate. The obtained performance using ARAG [23], GTMEA [26], Prophet [24], Epidemic [23], Spray and Wait [25] and RSTM (Proposed) is 28.2, 36.8, 45.2, 60, 37.8 and 22, respectively.

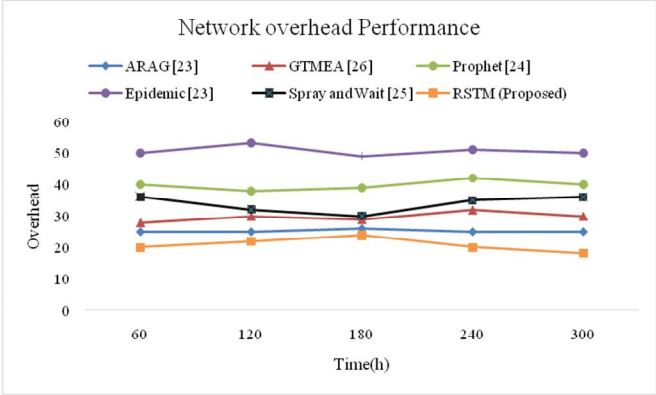

Figure. 6: Network overhead performance for time variation

Finally, Figure 6 shows a comparative performance for network overhead where the average overhead is obtained as 25.2, 29.8, 39.8, 50.6, 33.8 and 20.8 for ARAG [23]GTMEA [26], Prophet [24], Epidemic [23], Spray and Wait [25], and RSTM (Proposed).

5. CONCLUSION

In this work, we have considered the wireless networks field for our research. The demand for communication is increasing day by day which requires efficient approaches to meet the user requirements in the complex environments. Generally, end-to-end connectivity is a crucial parameter which affects the communication performance hence Delay tolerant networks based communication strategy is presented recently which helps to provide the end-to-end connectivity. However, high dynamics and unreliable networks can degrade the performance of DTN, similarly, security is also considered as a challenging task. Thus, we focus on these issues and presented a novel combined approach which presents relay selection, buffer management to improve the packet delivery performance and a trust management model is developed to incorporate the security in the deployed network. The proposed approach is called as Relay selection and trust management (RSTM) model for DTNs. In order to show the robust performance of the proposed approach, we compare the performance of RSTM with state-of-art techniques. The comparative study shows that the proposed approach achieves better performance.

REFERENCES

1. K. Fall, "A delay-tolerant network architecture for challenged internets," in Proceedings of ACM SIGCOMM, pp. 27–34, August 2003.
2. Crowcroft, J., Yoneki, E., Hui, P., & Henderson, T. (2008). **Promoting tolerance for delay tolerant network research.** *ACM SIGCOMM Computer Communication Review***,** 38(5), 63-68. https://doi.org/10.1145/1452335.1452345
3. Soares, V. N., Farahmand, F., & Rodrigues, J. J. (2009,July). **Improving vehicular delay-tolerant**

network performance with relay nodes. *In Next Generation Internet Networks*, 2009. NGI'09 (pp. 1-5). *IEEE*.
https://doi.org/10.1109/NGI.2009.5175762

4. Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L. S., & Rubenstein, D. (2002). **Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet.** *ACM SIGARCH Computer Architecture News*, 30(5), 96-1
https://doi.org/10.1145/635506.605408
5. Dias, J. A., Rodrigues, J. J., Kumar, N., & Saleem, K. (2015). **Cooperation strategies for vehicular delay-tolerant networks**. *IEEE Communications Magazine*, 53(12), 88-94.
https://doi.org/10.1109/MCOM.2015.7355571
6. Bouk, S. H., Ahmed, S. H., & Kim, D. (2016). **Delay Tolerance in Underwater Wireless Communications: A Routing Perspective**. *Mobile Information Systems*,2016.
https://doi.org/10.1155/2016/6574697
7. El Alaoui, S., & Ramamurthy, B. (2017). **EAODR: A novel routing algorithm based on the Modified Temporal Graph network model for DTN-based Interplanetary Networks.** ***Computer Networks***, *Trans* 129, 129-141.
https://doi.org/10.1016/j.comnet.2017.09.012
8. Zhu, H., Lin, X., Lu, R., Fan, Y., &Shen, X. (2009). **SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks**. *IEEE Trans. Vehicular Technology*, 58(8), 4628-4639.
https://doi.org/10.1109/TVT.2009.2020105
9. Singh, A. V., Juyal, V., &Saggar, R. (2017). **Trust-based Intelligent Routing Algorithm for Delay Tolerant Network using Artificial Neural Network.** ***Wireless Networks Trans*** , 23(3), 693-702.
https://doi.org/10.1007/s11276-015-1166-y
10. Guo, H., Wang, X., Cheng, H., & Huang, M. (2016). **A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks**. *Applied Soft Computing*, 38, 469-476.
https://doi.org/10.1016/j.asoc.2015.10.019
11. Jain, S., Chawla, M., Soares, V. N., & Rodrigues, J. J. (2016). **Enhanced fuzzy logic-based spray and wait routing protocol for delay tolerant networks**. *International Journal of Communication Systems*, 29(12), 1820-1843.
https://doi.org/10.1002/dac.2796
12. Stewart, M., Kannan, R., Dvir, A., &Krishnamachari, B. (2017). **CASPaR: Congestion avoidance shortest path routing for delay tolerant networks**. *International Journal of Distributed Sensor Networks*, *13*(11), 1550147717741264.
https://doi.org/10.1177/1550147717741264
13. Zhang, T., Li, H., Zhang, S., & Li, J. (2017, December**). A Storage-Time-Aggregated Graph-Based QoS Support Routing Strategy for Satellite Networks.** *In GLOBECOM 2017-2017 IEEE Global Communications* Conference (pp. 1-6*). IEEE*.
https://doi.org/10.1109/GLOCOM.2017.8255093
14. S. Jain, K. Fall, and R. Patra, "**Routing in a delay tolerant network,**" in Proceedings of *ACM SIGCOMM*, vol. 34, pp. 145–158, ACM Press, October 2004
https://doi.org/10.1145/1030194.1015484
15. Dias, J. A., Rodrigues, J. J., Xia, F., &Mavromoustakis, C. X. (2015). **A cooperative watchdog misbehavior nodes in vehicular delay-tolerant networks**. *IEEE Transactions on Industrial Electronics*, 62(12), 7929-7937.
https://doi.org/10.1109/TIE.2015.2425357
16. Zhang, L., Cai, Z., Lu, J., & Wang, X. (2015). **Mobility-aware routing in delay tolerant networks. Personal ,** *Ubiquitous Computing*, 19(7), 1111-1123.
https://doi.org/10.1007/s00779-015-0880-x
17. Yu, C., Tu, Z., Yao, D., Lu, F., & Jin, H. (2016). **Probabilistic routing algorithm based on contact duration and message redundancy in delay tolerant network**. *International Journal of Communication Systems*, 29(16), 2416-2426.
https://doi.org/10.1002/dac.3030
18. Li, Y., Jin, D., Hui, P., & Chen, S. (2016). **Contact-aware data replication in the roadside unit aided vehicular delay tolerant networks**. *IEEE Transactions on Mobile Computing*, (2), 306-321.
19. Johari, R., &Mahmood, D. A. (2016). **GA-LORD: and LTPCL-Oriented Routing Protocol in Delay Tolerant Network**. *In Wireless Communications, Networking and Applications* (pp. 141-154). Springer, New Delhi
20. Liu, Y., Wang, K., Guo, H., Lu, Q., & Sun, Y. (2017). **Social-aware computing based congestion control in delay tolerant networks**. *Mobile Networks and Applications*, *22*(2), 174-185.
21. Veas-Castillo, L., Ovando-Leon, G., Gil-Costa, V., & Marin, M. (2018, March). MinVisited: **A Message Routing Protocol for Delay Tolerant Network. In** ***Parallel, Distributed and Network-based Processing (PDP)****, 2018 26th Euromicro International Conference on* (pp. 325-328). IEEE.
22. Prabha, K. L., &Selvan, S. (2018). **Energy Efficient Energy Hole Repelling (EEEHR) Algorithm for Delay-Tolerant Wireless Sensor Network**. *Wireless Personal Communications*, 101(3), 1395-1409.
https://doi.org/10.1007/s11277-018-5768-4