Factual Demonstration of Blockchain Routing in Delay Tolerant Network

Renu Dalal
GGSIP University
Manju Khari (manjukhari@yahoo.co.in)
School of Computer and System Science https://orcid.org/0000-0001-5395-5335

Research Article

Keywords: Opportunistic Network, Blockchain, Routing Protocol, ONE Tool, Security, Trust.

Posted Date: August 2nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-760203/v1

Factual Demonstration of Blockchain Routing in Delay Tolerant Network

Renu Dalal[a], and Manju Khari[b,*]
[a]*Department of Computer Science, AIACT&R, GGSIP University, Delhi, India*
[b] *School of Computer and System Science, JNU, Delhi, India*
Email: dalalrenu1987@gmail.com, and manjukhari@yahoo.co.in

Abstract

Frequent disconnection, high end-to-end latency, dynamic topology, sparse node density, lack of pre-existing infrastructure, and opportunistic message transmission on wireless link, makes routing difficult in Opportunistic network (Oppnet). In present scenario, Oppnet allows the people to interact with contrasting ways like with diverse mobility, groups, and etc. During transmission of messages in such network security and trust performs major role. Delay Tolerant Network (DTN) are much prone of having inherent risk of attack. Malicious node, selfish node, and attacks are major impact on deteriorating network performance. To prevent the network from such deteriorating factors, this paper introduces the new platform to provide reliable and authentic transmission of message in opportunistic network. Blockchain-based Routing in Opportunistic Network (BRON) uses the concept of Blockchain through which each node work as an authentic node and transmit the secure messages in Oppnet. Opportunistic Network Environment (ONE) tool is used to implement BRON. This protocol generates 36% reduced packet drops ratio, 57% enhanced delivery ratio, 55% lesser overhead ratio, 35.2% reduced average latency, and 65% lesser average buffer time as compared to direct delivery ratio with respect to number of nodes

Keywords – Opportunistic Network; Blockchain; Routing Protocol; ONE Tool; Security; Trust.

1. Introduction

Subset of Delay or Disruption Tolerant Network is known as Oppnet. This network captured great attention of researchers due to its working characteristics in highly challenging atmosphere. Message dissemination in different regions of opportunistic network is done with using Store-Carry-Forward mechanism. In this mechanism, whenever an Oppnet node receives the packet from one of its neighbouring nodes, packet is stored and carried in nodes' buffer until it encounters another reliable relay node. Irregular connection and no end-to-end route between sender to receiver makes the Oppnet routing different from traditional routing [1]. Vehicular-ad-hoc network, habitat monitoring, emergency & special operations, and communication in smart atmosphere are few emerging & innovative applications of Oppnet. Only with the mutual-effort with all participating Oppnet nodes in network makes the high successful transmission of messages. This mutual-effort individually rely upon each and every node in the network. Few nodes in the network behaves as malicious or selfish or un-cooperative due to finite buffer capacity, limited energy, and irregular wireless connection.

* Corresponding author

E-mail address: dalalrenu1987@gmail.com (Renu Dalal), manjukhari@yahoo.co.in (Manju Khari)

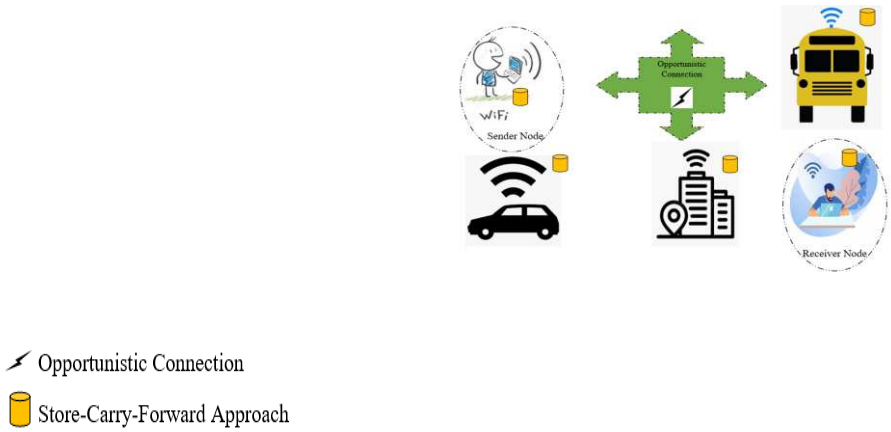


Fig. 1. Working Environment of Opportunistic Network

Message dropping, large amount of un-necessary message transmission, longer time to forward the message, lack of message integrity, and etc are few factors which intensify the network load and decelerate the network performance. Because of open joining property of users in Oppnet makes difficult to prevent this network from selfish or malicious or un-cooperative nodes/users. To maintain the security and trust in Oppnet, it is important to control these un-cooperative nodes. Working environment of Oppnet with Store-Carry-Forward approach is depicts in fig. 1. It includes contrasting small handheld electronic devices with bundle layer. This bundle used for keeps the message in their buffer and passed this message whenever current Oppnet nodes found the best relay node. Mobile Ad-hoc Network (MANET) and DTN network are base of Oppnet.

Opportunistic network includes multifarious properties and also vulnerabilities from DTN and MANET [2]. Many security hazards exist in Oppnet like (a) Lack of message integrity: various heterogenous network transmit the message in Oppnet which enhance the threat of message integrity. (b) Breach of privacy: because relay node keeps the message in their buffer, so it is easy to breach nodes' location, identity, and message content. (c) Exposure of message confidentiality: due to Store-Carry-Forward principle in Oppnet, makes possible to copy the content of message by relay/ intermediate node. (d) Resource consumption attack: finite nodes' energy, buffer space, and calculation power, increases the risk of resource consumption attack. (e) Illegitimate access: limited resources for nodes in network, makes the huge risk of illegitimate access by selfish nodes which becomes the factor of poor efficiency in network performance. (f) Denial of Services (DoS) & Injection attack: protracted delay in message dissemination and intermittent interruption of connectivity in network are the outcome of DoS attack. In injection attack, attacker attempt to inject fictitious data packet in Oppnet, to mislead the normal nodes [3-4].

To implement dynamic trust, security, and to cope with vulnerabilities in opportunistic network, blockchain is the appropriate tool. Decentralization, non-modifiable, and security are the traits of Blockchain Technology (BT). The foundation of BT is consensus algorithm, through which it eliminates the issue of associated trust among nodes in scattered network. Delivery of content, financial environment (banks), non-financial environment (decentralized storage of data), and etc. are few applications of BT. Decentralized characteristics of BT can achieved trust and security between nodes in Oppnet.
The fundamental purpose of this research paper is:

1. Trust mechanism is proposed by using Blockchain Technology. Mobile-Infrastructure based method is used to develop this routing in Opportunistic Network.

2. For dynamic trust updates of Oppnet nodes Proof-of-Work and Proof-of-Stake approach is applied.

3. To implement BRON protocol ONE tool is used.

4. Results of proposed protocols are compared with other existing protocols.

This research paper is structured as follows: literature review on contrasting trust-based routing protocols of opportunistic network is presented in section 2. Preliminaries used in proposed model with BT are described in section 3. Section 4, introduced the novel BRON routing protocol for Oppnet. Implemented results of BRON's performance, and security analysis are discussed in section 5. Finally, paper is concluded with future scope in section 6.

2. Literature Review

In this section, peculiar types of security-based routing protocols of Oppnet are classified and compared in huge domain of Ad-hoc networks. Although lots of work on routing protocols in Oppnet has already done in past years, but very few researchers give attention in aspect of security and trust mechanism in Oppnet routing. Fig. 2 presents, the classification of secure routing schemes in Oppnet. Table 1 presents the different category of secure protocols, and also differentiate these protocols in contrasting terms like their properties, pros, cons, and etc.

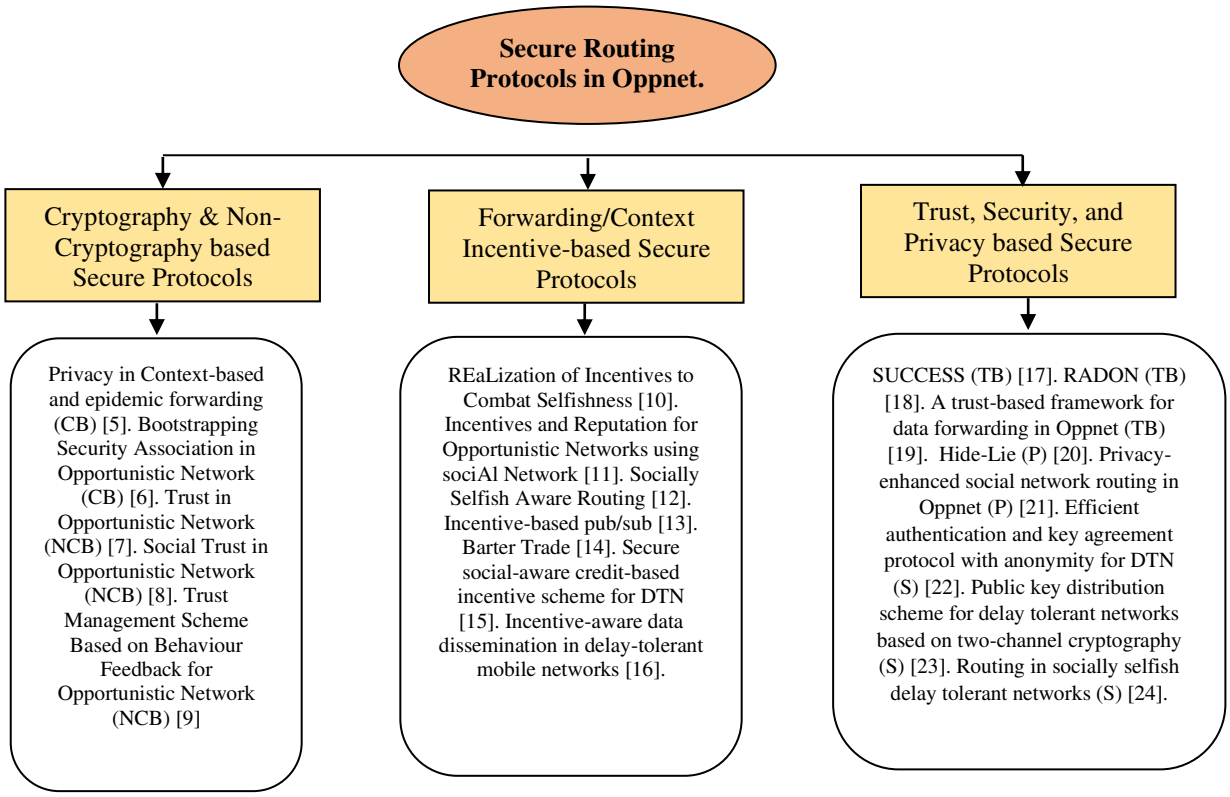


Figure 2. Different Secure Routing Protocols in Opportunistic Network

Table 1. Comparison of Secure Routing Protocols in Opportunistic Network

S. No	Year	Protocol Name	Category	Properties	Pros	Cons	Tool Used	Other Information

1	2009	Privacy in Context-based and epidemic forwarding	Cryptography-Based (CB)	Policy-based & Searchable encryption is used as 2-refinements levels of identity-based encryption. Classical asymmetric technique, ID-based cryptography is used.	Work on privacy issues and security. No need of certificate.	Trusted Third Party (TTP) is used only at offline. Not applicable in extreme environment.	Mathematical key Computation.	Minimum storage space & less computation overhead. Works in 2-phases: set-up phase & run-time phase [5].
2	2010	Bootstrapping Security Association in Opportunistic Network	CB	Key-management with Content-based forwarding concept is used. On the basis of self-organised & local key-management end-to-end confidentiality is achieved.	Prevention from Sybil attack by using individual pseudonyms. Enforcing privacy.	High key computational cost. Identity Manager (IM) is offline. Can't work with practical & extreme scenario.	Mathematical key Computation.	Protect from active attackers & eavesdropping. Asymmetric cryptography & signature is used [6].
3	2009	Trust in Opportunistic Network	Trust based but Non-Cryptography-Based (NCB)	Proposed three trust metrics; Social, Environmental, and Similarity trust. Differentiate the term Trust & Reputation.	More scalable. Not using Central Authority.	Not focused on entity behind the identity.	Simulated in Real world mobility traces like; Haggle Infocom, and MIT.	Complexity during data transfer is O(b) & during communication with familiars is O (b^2) [7].
4	2010	Social Trust in Opportunistic Network	Trust based but NCB	Implicit & Explicit social trust approaches are proposed. Complexity of Implicit trust is *O(b),* and Explicit trust is $O(b^d)$where b is the branching factor, and d is the depth of tree	Work against Sybil Attack. Highly scalable, and robust against manipulation attack.	Not applicable when user is not the part of social network like Facebook, Caveman, protein network, etc.	Uses real world graph and synthetic graph models.	Classical community detection and certificate chain-based approach is not used [8].
5	2015	Trust Management Scheme Based on Behaviour Feedback for Opportunistic Network	Trust based with using certificate	Generation of local certificates by using identity-trust relationship. Interchange and issue of certificates is based on the self-organised key management and with social context information.	Delivery Probability & trust reconstruction ratio is enhanced in large no. of compromised nodes.	Simulated on limited parameters. Not focused on delivery of packets.	ONE Tool	To provide secure routing efficiently explore and filter trust nodes in Oppnet [9].
6	2010	REaLization of Incentives to Combat Selfishness	Incentive-based approach	On the basis of nodes' transit behaviour, explicit rank is given. According to rank	Energy-aware incentive approach for selfish DTN is	Can't work in asymmetrical parameters of network; like	ONE Tool	Evaluate rank and message priority metrics.

		(RELICS)		message priority is decided.	introduced.	intermediate node capacity, physical mobilities of nodes.		Reliable delivery ratio with efficient energy rate [10].
7	2011	Incentives and Reputation for Opportunistic Networks using sociAl Network (IRONMAN)	Incentive-based approach	On the factors of encounter history, message interchange, and interchange history while encounter, node determines the selfishness of another node.	To find the lying about clock timing, clock synchronisation layer is used. Enhance delivery performance.	Compared with basic protocols only and with limited metrices. Works in constrained environment.	3-real world traces are used to simulate; SASSY, MIT reality mining, and HOPE dataset.	Detection time, detection accuracy, and selfishness cost metrics are used to simulate this model [11].
8	2012	Socially Selfish Aware Routing (SSAR)	Incentive-based approach	Nodes' enthusiasm and contact opportunity is used for choosing relay node.	Efficient routing performance with minimum transmission cost.	Only 2 protocols are used for comparison, PROPHET and SimBet.	Uses two traces; Haggle Infocom 05, and MIT Reality for simulation.	Packet delivery ratio, cost, and delay, with selfishness satisfaction metrics are used for simulation [12].
9	2013	Incentive-based pub/sub (ConSub)	Incentive-based approach	Tit-For-Tat (TFT) approach is used to find selfish nodes. Interest channel manager, content utility estimator, and content exchange protocol sub-modules are used to build its architecture.	Works better in terms of packet delivery and transmission hop. Novel content exchange protocol is proposed.	Implemented on few parameters like; transmission cost, hop, and packet delivery ratio.	MIT reality, and Infocom 06 is used for model implementation.	Reliable transmission cost. Computation complexity increases w.r.to storage capacity of buffer [13].
10	2013	Secure user-centric and social-aware reputation-based incentive scheme for DTNs (SUCCESS)	Trust-based (TB)	Self-check & Community-check concepts are proposed for calculation of reputation. Uses Demster-Shafer theory.	Evaluate in two aspects; cryptography operation and efficiency & effectiveness.	Compare only with basic protocols like; spray & wait, epidemic, and prophet.	ONE Tool	Identity-based signature technique is used to secure the nodes from malicious nodes [17].
11	2010	Privacy Enhanced Social Network Routing in Oppnet	Privacy-based (P)	Statisticulated Social Calculated Routing (SSNR) & Obfuscated Social Network Routing (OSNR) two routing schemes are introduced.	Bloom filter data structure with one-way hash is used to find hidden social network information. Obfuscated	Only few metrics (delivery ratio, cost, and delay) are used to evaluate OSNR	Used trace-driven simulation with SASSY dataset and ONE	90% delivery ratio when 60% of nodes are eliminated from social network by using obfuscate.

					social network graph concept is used.	protocol.	tool.	[21]
12	2013	Efficient authentication and key agreement protocol with anonymity for DTN	Security -based (S)	Used only offline public information and key generation centre. On-line trusted third party is not required.	Focus on authentication , anonymity, and confidentiality .	High complexity.	Evaluated on mathemati cal computati on.	Highly secure against probabilistic polynomial-time attacker. [22]

3. Preliminaries

3.1 Motivation

Security, trust, and privacy in opportunistic network are ever the complicated and tough work. Selection of intermediate node in Oppnet depends on various factors and among of them trust is primary parameter. While designing routing protocols in Oppnet; dynamic network topology, limited buffer size of nodes, energy, recurrent links among nodes, finite resources, and etc. are many factors through which, routing becomes a crucial task. According to table 1, many researchers introduced various security approach with novel features. Each existing protocol have their own unique features as well as some limitations. Authors used cryptographic approach which uses asymmetric algorithm to provide privacy in Oppnet. [5]. Bootstrapping scheme prevent the Oppnet from sybil attack by using end-to-end encryption with self-organising key management [6]. Incentive based approaches [10-16] and trust, security & privacy-based many approaches are introduced in [17-24]. But some factors like; inconsistent behaviour of nodes, active & passive attack in network, privacy issues, message integrity, trust between nodes, and etc. motivates author to introduce BRON routing protocol. Subsequentially authors discovered that, blockchain technology can be applied in opportunistic network. Now a days blockchain is such a spectacular technology which provides always unbelievable performance in various field.

3.2 Background of BRON

The sequence of techniques applied in diverse applications, having characteristics of decentralization, irrefutable, and immutable is known as Blockchain Technology. Smart contracts, record keeping, securities, fraud reduction, digital currency, and etc are application of BT. Blockchain is the core method, which is used for “Bitcoin”. It is the digital cryptocurrency, a novel concept introduced by Satoshi Nakamoto in 2008 [25]. Public, private, and consortium (semi-private) are three categories of BT. To provide the features of transparency, and security in distributed network; public-BT is applied. It gives open and equal rights to each user in the network. Banks, government colleges, taxation institutes, hospitals, and other applications, where security, privacy, and more access control is required; consortium or private BT is used. Consensus algorithm & decentralization strategy enables BT to provides security. Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPOS), Ripple, and Tendermint are different versions of Consensus algorithm of BT [26].

4. BRON: The Proposed Scheme

4.1 Security Model in Oppnet

In this subsection, Blockchain-based routing model is illustrated. Fig. 3 depicts the architecture; in this, each node in opportunistic network uses the block-id. This model works in two phases; 1. Authentication phase, 2. Trustworthiness-phase. In authentication phase; whenever an oppnet-node wants to communicate in network; node generates the request for the same function. Block is created with user-id, and now this block is disseminated in the network for the authentication. Each oppnet-node in opportunistic network received the block with user-id. Elected-node in network verify the authentication of requested block. If this block is approved by elected-node this block can become the part of the network. This approved block now added to the current blockchain with unique block-id. In trustworthiness-phase; according to blockchain header (fig. 5) node will receive/forward the message to relay node.

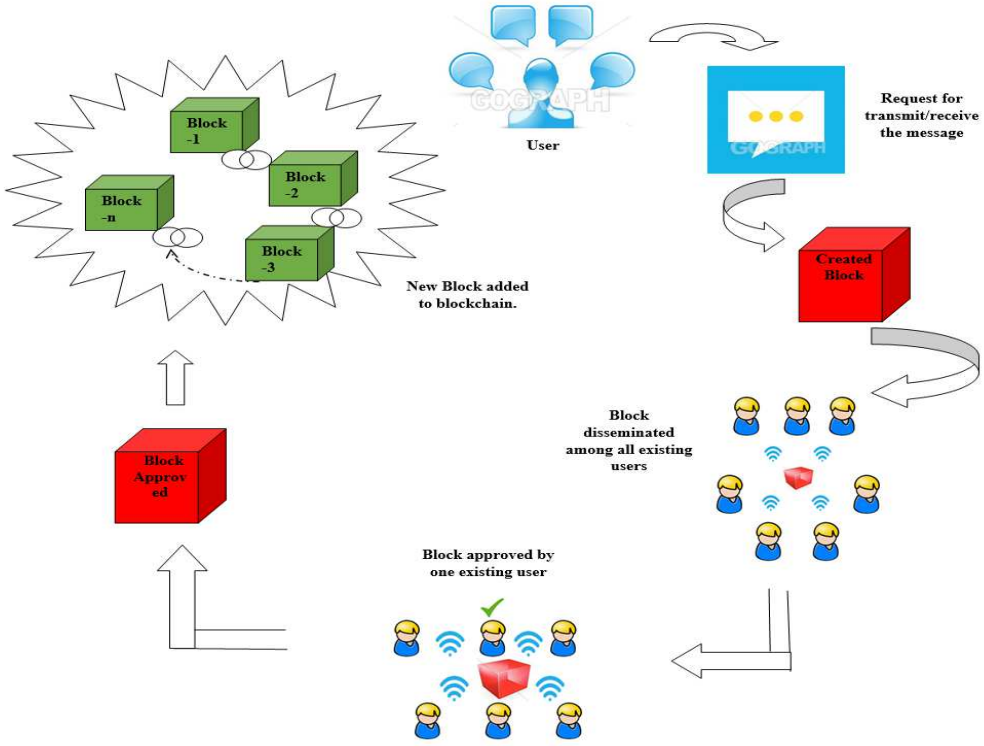


Fig. 3. Blockchain Approach in Oppnet

4.2 Procedure of BRON

Authentication Phase; in this phase, all nodes are established with certified public-key which is provided by Blockchain technology. For authentication process of a new node, Itsuku PoW [27] approach is applied. This approach is improved version of MTP-Argon2 [28]. It prevents from hash composability attack, computation attack and also resolve the problem of parallel search, memory storage, and pseudo-random array. Handling & evaluation of trust with hard-to-forge mathematical computation is sorted by "Itsuku PoW" by using the concept of memory-hardened.

Algorithm – 1: // Authentication Process in BRON.

***Input**: (C, D, S, l)*
Input challenge: C
Difficulty: D
Autonomous Segment: S
Length of Segment: l
***Output**: (N, H, Ǐ, Ł)*
Nonce: N
Markle Hash Tree with selected node & antecedents: T
Index of Selected Node: Ǐ
Selected Node: Ł
***Begin**:*
Construct challenge dependent memory $T_l[1, 2, \ldots\ldots, K]$ as S with length l
Calculation of Root Θ *//*Markle Hash Tree (T)*
** Selection of N*
Computation of $B_0 = H(N \,||\, \Theta \,||\, C)$
for j= 1: L *//* L= length of the one search*
{
$i_{j-1} = B_{j-1} \bmod K$
$B_j = H(B_{j-1} \,||\, T_l[i_{j-1}] \oplus C)$
}
end for j
In reverse order $v = H(B_L \,||\, \ldots \,||\, B_{1-L \bmod 2} \oplus C)$
If v has D binary leading 0's then
Return (N, H, Ǐ, Ł)
else
*go to **

Stop

Algorithm–1 presents how the new oppnet-node get authenticated & can join the network with blockchain-certificate. In this algorithm four input (C, D, S, I) and four output (N, H, Ǐ, Ł) parameters are used. BLAKE2 [29] algorithm is used to calculate the hash function (H). It uses 128 bytes input and generates 64 bytes output in one processing. While computing of B_0 and adding C with hash function doesn't increase any computation cost.

Trustworthiness procedure of proposed protocol is described in Algorithm-2. Majority voting concept from [30] is used. Here, set of authenticated blocks "B" is used as an input parameter, which comes from algorithm-1. "I" is the set of events or task like; message receive, or transmit, or storage. For each B (as node) with particular task $\boldsymbol{\alpha}_i$, trust value is evaluated by $F\left(e_n^i\right)$. Majority trust for each task is calculated by *fn (i).* Communication in network depends upon the majority trust value of node (B). Value of trust given by each node is either 0 or 1. 0 indicates complete trust and 1 presents complete distrust. Whenever the node trust computed as 0, that node will not be the part of network and automatically removed from the network. Concept of blockchain with trust among nodes in opportunistic network enables to achieves many benefits like; Availability, Consistency, Decentralized network, and Message integrity. Fig. 4, shows the flow diagram of Blockchain based routing in opportunistic network. Eq. (1) is used by new block node, for find the shortest distance from itself to authenticated block node in network.

$$V^2(i, j) = (i_2 - i_1)^2 + (j_2 - j_1)^2 \ldots\ldots \quad (1)$$

Algorithm – 2: // Trustworthiness Process in BRON.

***Input**: Node set B ($B_0, B_1, \ldots, B_n$)*
Set of original events $I = \{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots\ldots, \boldsymbol{\alpha}_i\}$
***Output**: T_i* *//*Calculated trust of node B at event $\boldsymbol{\alpha}_i$*

***Begin**:*

***for** i =1: n all B nodes*

Apply function "fn (i)"

$fn(i) = \frac{1}{N}\sum_{n=1}^{N} F\left(e_n^i\right)$

$F\left(e_n^i\right)$= *f {λ (Bn), α_i}* //* λ shows trust value of node B_n at event α_i

T_i ⟵ *fn (i)*

repeat for i in original events I

***end for** i*

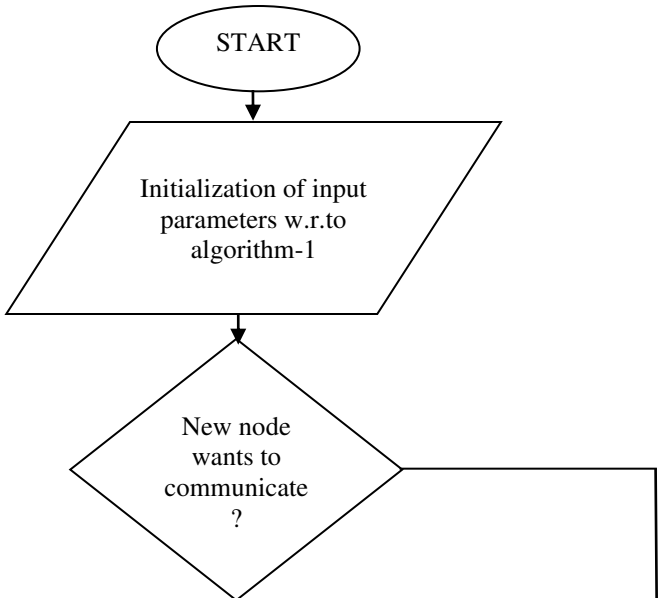
Stop

4.3 Block-Header Format of BRON

Format of blockchain header for proposed routing protocol is shown in fig. 4. Each node in opportunistic network uses this header before performing action. It is structured in eight different fields. The description of each field is as; (1) Prev. B-id: This field contains the previous block-id of oppnet-node. The value of block identification is alphanumeric unique value. (2) Current B-id: Present block ifigdentification unique value is denoted by Current B-id. (3) Message-id: Each message having their unique id, and after forwarding that message; block will remove that message with id from their buffer. (4) λ-value: Trust value of the block is presented by 4th field of the header. On the basis of λ-value communication will be processed in the network. (5) Available Buffer-space: Each block has their buffer capacity to keep the message. This field shows the left buffer space of the block. (6) TTL: This field is used to indicate the Time to Live (TTL) of the block node. (7) DT: It indicate the date and time at which the block is created after the authentication process. (8) Dest. B-id: This is the last field of the header, which presents the block-id of the destination.

Pev. B-id	Current B-id	Message-id	λ-value	Available Buffer-space	TTL	DT	Dest. B-id

Fig. 4. Block-Header of BRON



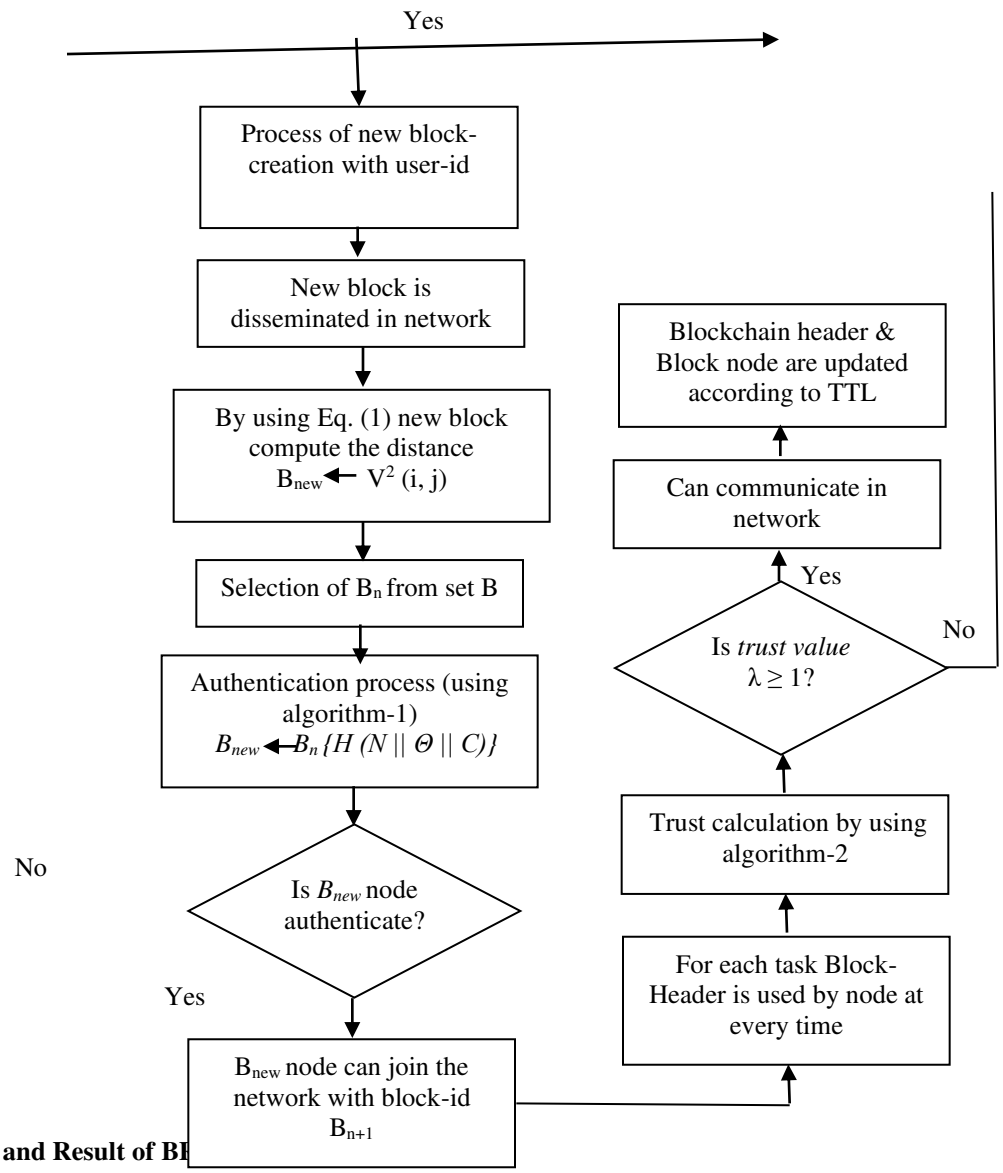


Fig. 4. Flow Diagram of BRON

5. Simulation Set-up and Result of BI

For measure the performance of proposed protocol BRON; java-based and open-source emulator named ONE [31] tool is used. Intel(R) Core (TM) i5-8265U processor, CPU @ 1.80 GHz speed, 8GB RAM, and 64-bit OS system is used for the simulation of proposed work. Table 3 is presenting the environment for simulation of BRON Protocol. Transmission range for opportunistic nodes, time for simulation, speed of broadcasting the packets, name of group movement model, buffer occupancy for nodes, TTL for messages, size of messages, number of nodes used, and route-based mobility model with the specification details are shown in table 3. For performance comparison various variation in the fields have been considered, the explanations of these fields are as follows:

1. Variations in number of nodes in Opportunistic network: The number of nodes in the Opportunistic networks are varied for examine the performance of BRON protocol. No. of nodes are varied from 20 to 100 with the gap of 20 nodes. Therefore, the sequence of nodes is 20, 40, 60, 80, and 100.

2. Variations in Time to Live (TTL) in Opportunistic network: TTL of messages defines the working time or life of messages in the network. In simulation settings TTL fields is varied from 100 min. to 500 min. with the gap of 100 min. in each TTL interval. Thus, the order of TTL is 100, 200, 300, 400, and 500 minutes.

3. Variations in Speed of nodes in Opportunistic network: Opportunistic nodes operates in specific range in Opportunistic network. Speed of nodes defined as the link time among nodes and it directly influence the working performance of protocol. The node's speeds are varied from 0.2 km/h to 1 km/h with interval of 0.2 km/h. The sequence of variation in node's speed are 0.2, 0.4, 0.6, 0.8, and 1 km/h.

Table 3. Environment for Simulation of BRON Protocol

Parameter	Value
Time for Simulation	43200 s
Transmit Speed	259 K
Transmit Range	10 m
Group movement Model	Shortest Path Map Based Movement
Buffer Size	5 Mb
Message Generation Interval	0.5-1.5 sec.
Mgs TTL	300 min.
Movement Model	Map Route Movement
Message sizes	500 KB
Number of Nodes	20 to 100

4. Variations in size of messages in Opportunistic network: To evaluate the performance of BRON routing protocol, size of message are varied from 100 to 500 KB with the interval of 100 KB. So, the sequence of variation in message size is 100, 200, 300, 400, and 500 KB. Message size parameter directly impacts on the performance of proposed protocol. Diverse number of parameters are compared during variation in the fields that discussed in previous section. In simulation time of model other settings are set to default, which are discussed in table 3. The explanation of diverse factors is as given below:

1. Packet Drop Ratio: It is defined as the ratio of number of packets losses to the number of packets created. Whenever the buffer occupancy of node is adequate, opportunistic node will drop the packets. This parameter should be always lesser.

2. Delivery Ratio of Packets: This parameter must be high as possible during packets disseminating in the network. Ratio of successful transmission of packets to the total number of packets produced in the network is known as delivery ratio of the packets.

3. Overhead Ratio: For any routing protocol overhead ratio should be minimum as possible in the network. Overhead ratio is known as the number of message duplicate copy produced per original message during message broadcasting to the relay node in the network.

4. Average Buffer Time: This parameter should be minimum for efficient and reliable routing protocol. Before successful delivery of packet at the receiver node average time spent by packet in the node's buffer is known as average buffer time.

5. Average Latency: It is defined as the average travel time spent by the packet, from message packet created by source node to packet received by receiver node in the network. Average latency parameter is always as minimum for enhancing the performance of any routing protocol.

5.2 Performance Results and Comparison of Proposed Protocol

1. Results during varying the No. of nodes: When the field number of nodes are varying during simulation, all other factors mentioned in table 3 are kept default. And other parameters are evaluated like; packet drop ratio, delivery ratio, overhead ratio, average buffer time, and average latency. Figures 6-10 presents the performance metrics of all parameters. BRON routing protocol performs efficiently in terms of packet drop ratio as compared to other conventional protocol like; prophet, spray & wait, and direct delivery as shown in figure 6. As far as number of nodes increases packet drop factor also increases in every routing protocol. Proposed protocol performs 36% more efficiently as compared to direct delivery protocol, and 23% more efficiently as compared to spray and wait protocol, in terms of packet delivery ratio.

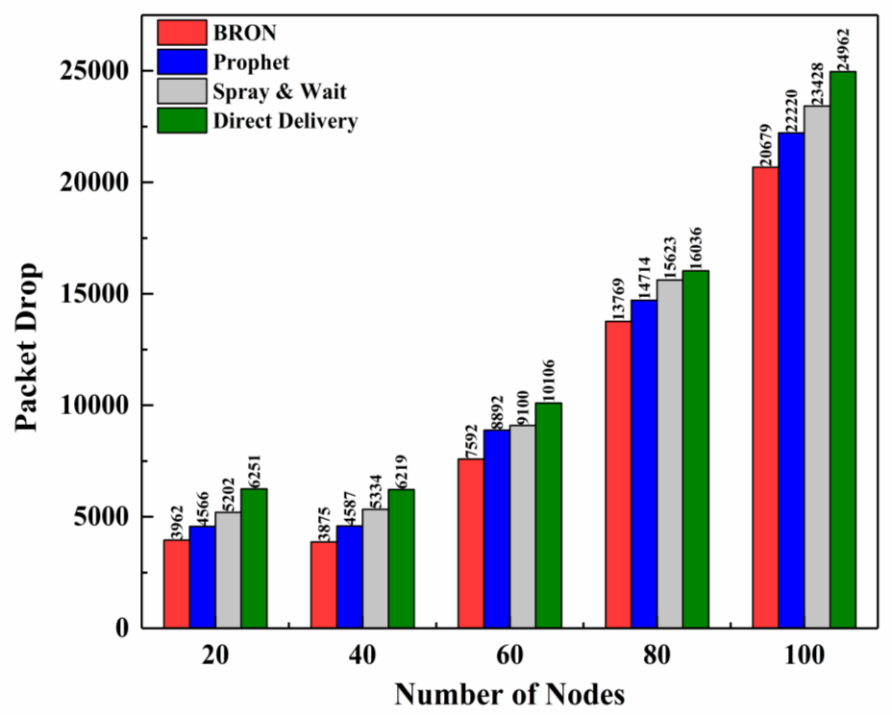


Fig. 6. Packet Drop vs. Number of Nodes

From figure 7, this is clearly present that BRON protocol performs very well in terms of delivery ratio whenever the nodes increase. Proposed protocol gives 57% higher delivery ratio in comparison with direct delivery ratio. At initial time of simulation almost all discussed protocol like direct delivery, prophet, spray & wait, and BRON performs same in terms of delivery ratio. But when the nodes increase BRON protocol works more adequately as compared to other protocols as shown in figure 7.

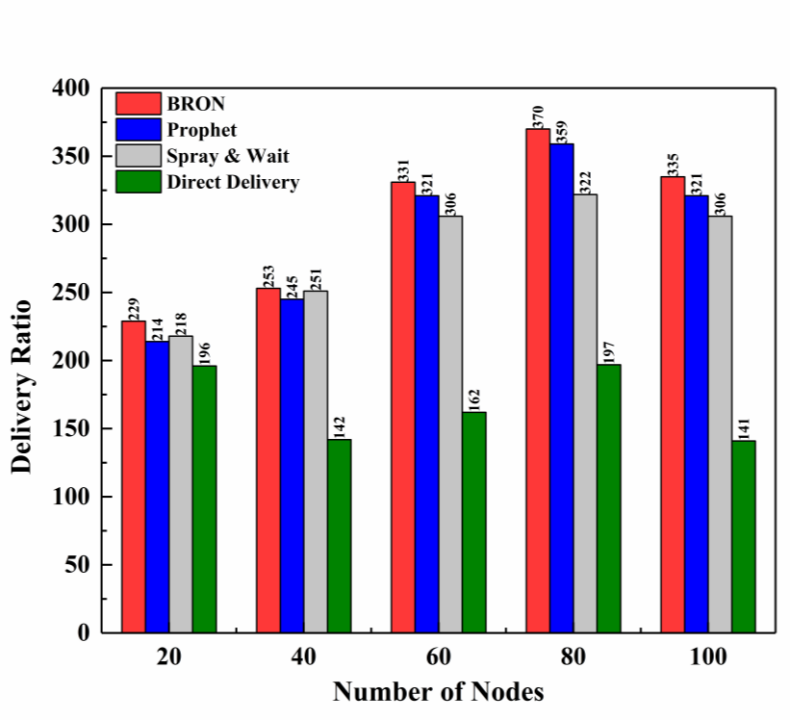


Fig. 7. Delivery ratio Vs. Number of Nodes

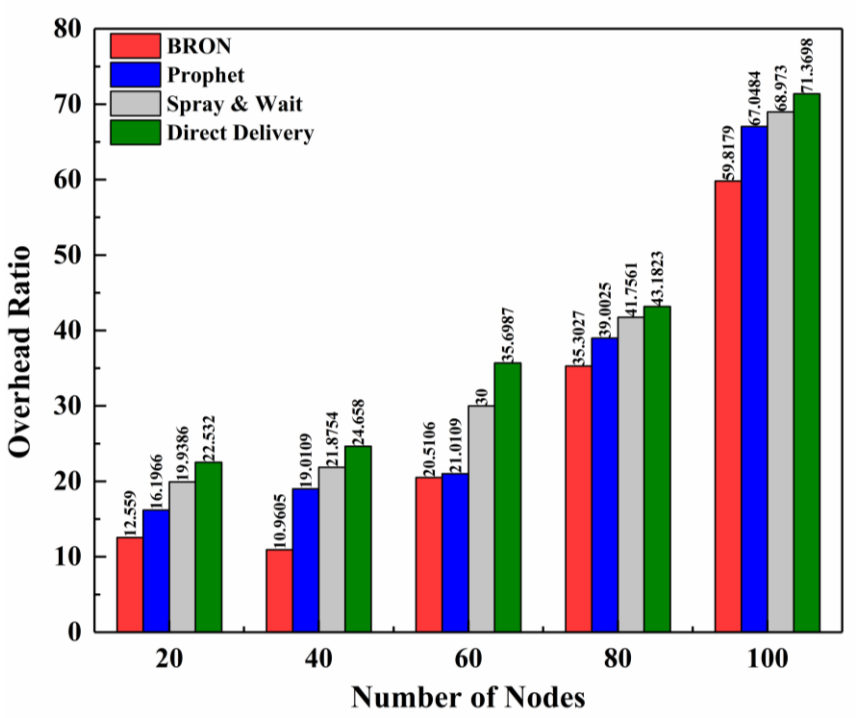


Fig. 8. Overhead ratio Vs. Number of Nodes

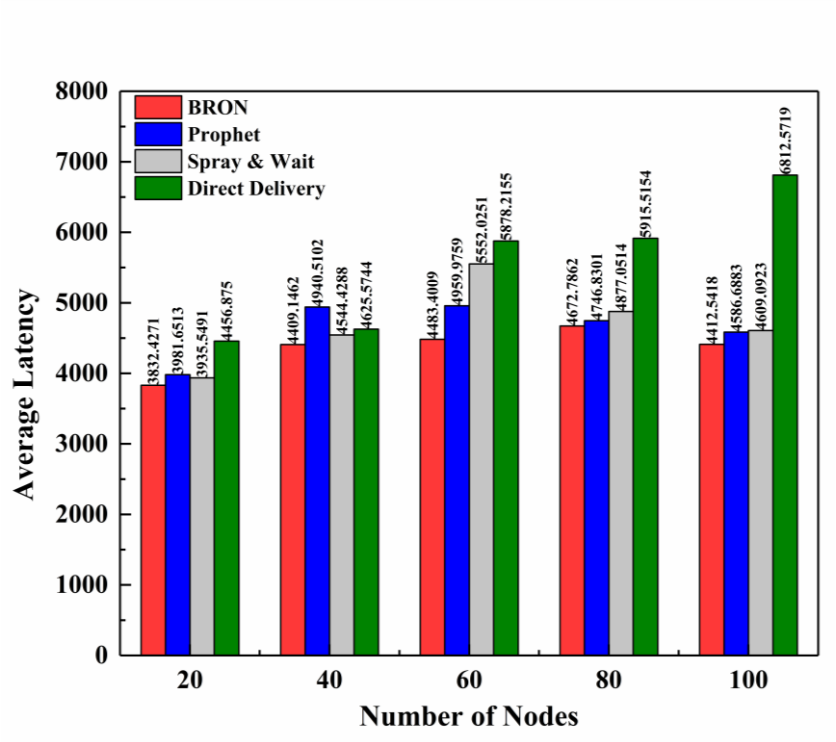


Fig. 9. Latency Vs. Number of Nodes

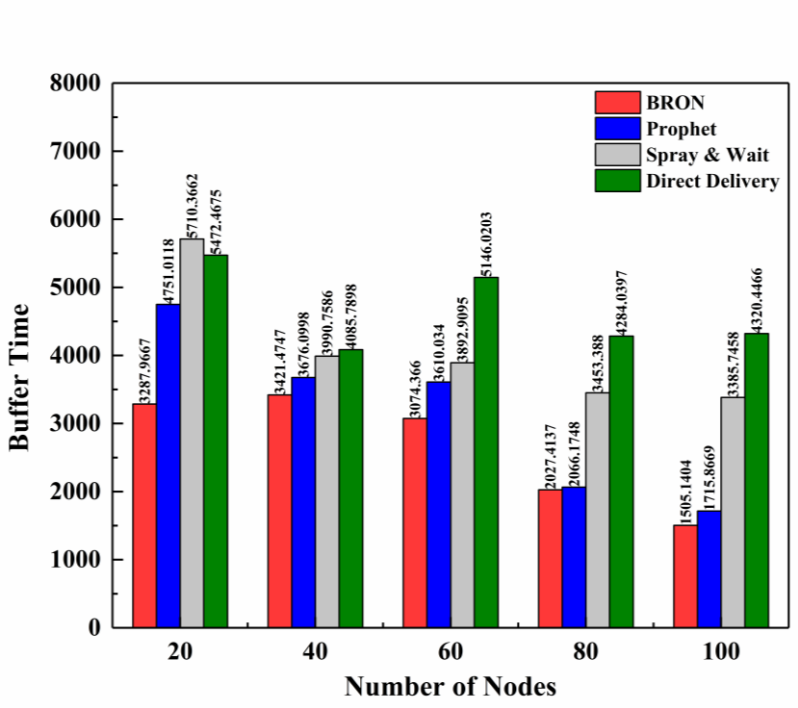


Fig. 10. Buffer Time Vs. Number of Nodes

Simulation results of the parameter overhead ratio with respect to no. of nodes are shown in figure 8. As compared to direct delivery protocol, BRON produces 55% lesser overhead ratio. In the beginning simulation time, when nodes are 20 to 40, BRON gives lesser and almost constant overhead ratio. As soon as no. of nodes are goes higher i.e., 60 to 100; overhead ratio is also increases. Proposed routing protocol works 50% more effiently as compared to spray & wait in terms of overhead ratio.

Implemented results of the factor average latency time and buffer time with respect to the no. of nodes are shown in figure 9 and figure 10 respectively. BRON works more adequately in terms of average latency and buffer time as compared to other protocols like prophet, spray & wait, and direct delivery. Proposed protocol produces 35.2% lesser average latency time as compared to direct delivery protocol. In respect of average buffer time, BRON performs 65% more efficiently. From beginning to end duration of BRON implementation, there is no major changes in terms of average latency parameters when no. of nodes are increases as depicts in figure 9. Average buffer time is decreases as far as number of nodes are increases, when the number of nodes is increases as presents in figure 10.

2. Performance results during varying TTL: Transmission speed, range, buffer size, and all other factors described in table 3 are set as default, when the field time to live (TTL) are varying during simulation. Packet drop ratio, delivery ratio, overhead ratio, average buffer time, and average latency parameters are captured. Simulation results of BRON protocol and other protocols with respect to TTL are presented in figures 11-15. Figure 11. shows the performance metrics of packet drop ratio with respect to TTL parameters. BRON works 24% more

efficient as compared to direct delivery protocol in terms of packet drop ratio with respect to TTL. At beginning simulation time of packet drop ratio vs. TTL, BRON and prophet performs almost in same way. But as far as TTL varies from 300 to 500 minutes, BRON works more adequately as compared to prophet.

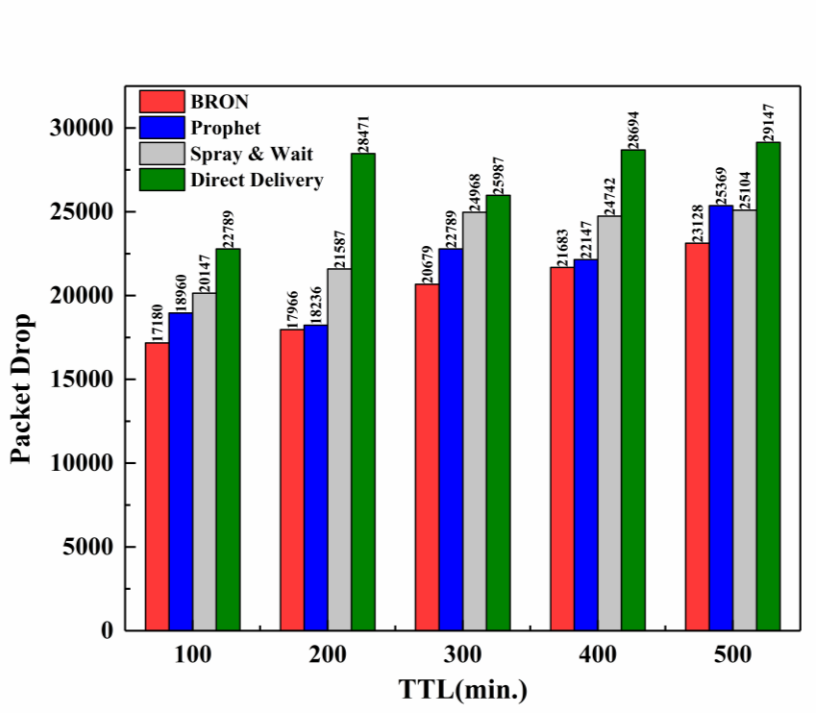


Fig. 11. Packet Drop Vs. TTL

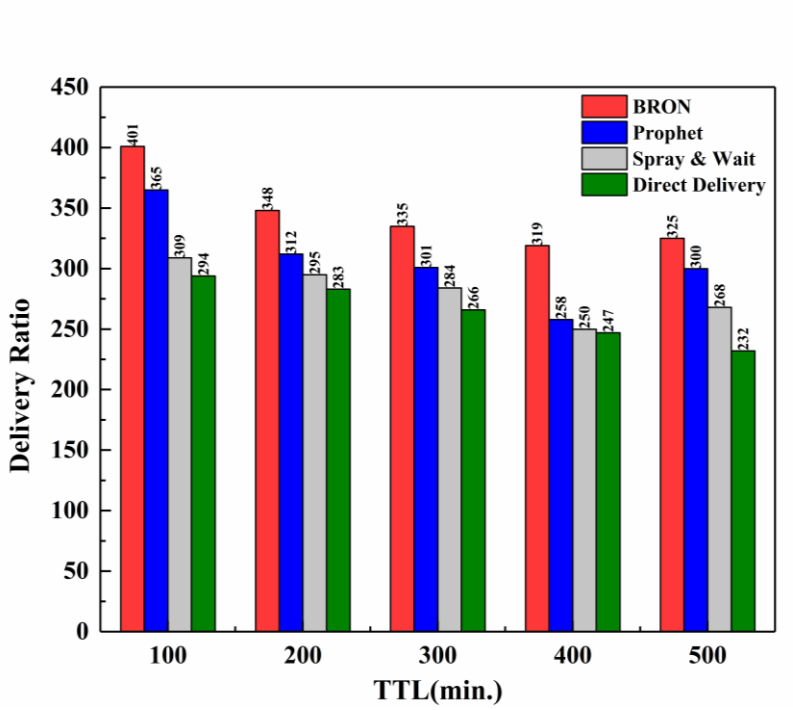


Fig. 12. Delivery Ratio Vs. TTL

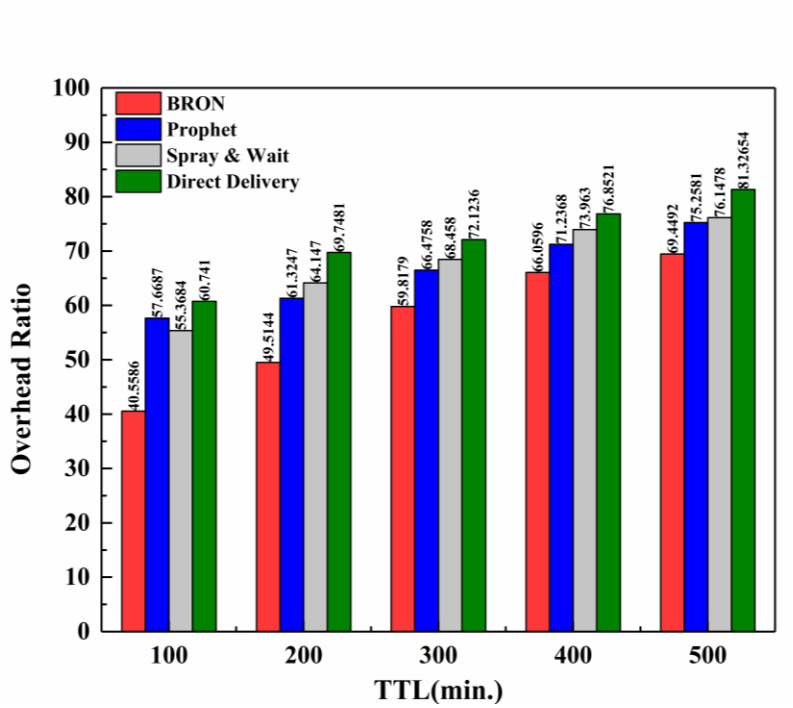


Fig. 13. Overhead Ratio vs. TTL

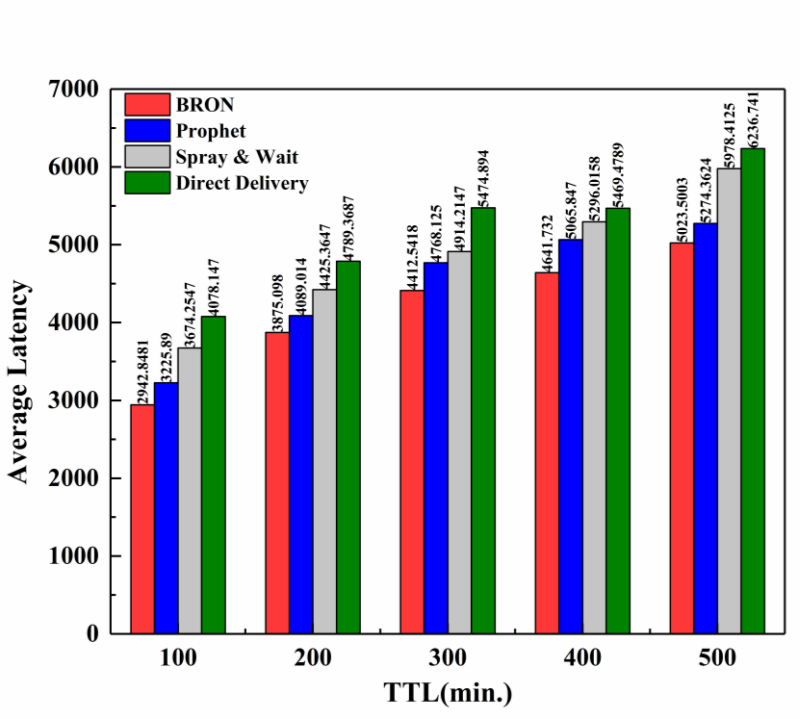


Fig. 14. Average Latency vs. TTL

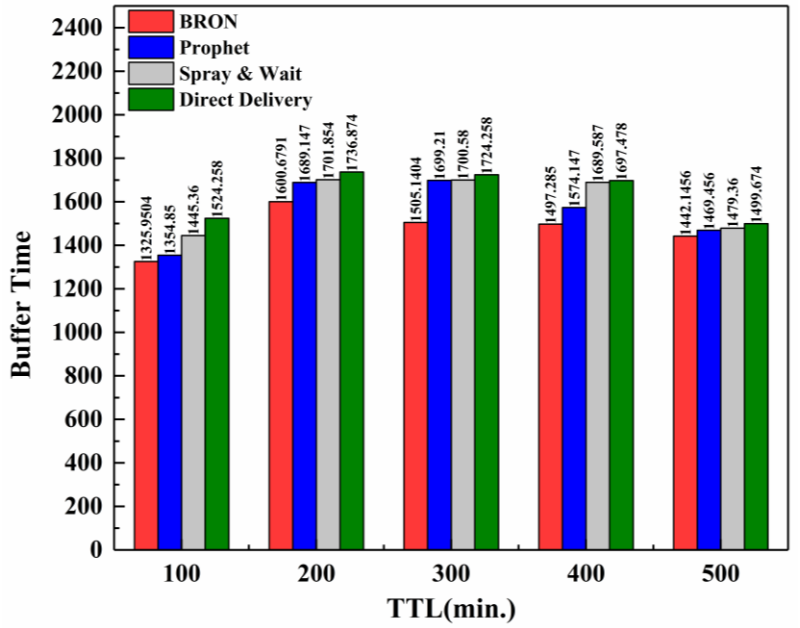


Fig. 15. Buffer Time vs. TTL

Implementation results of the factor delivery ratio with respect to TTL is presents in figure 12. As compared to direct delivery protocol, BRON performs 26% more efficiently in terms of delivery ratio when TTL varies. Whenever the TTL value goes to higher, delivery ratio is also decreasing negligibly in case of all protocols. But BRON still performs adequately as compared to other protocols. Overhead ratio vs. TTL result is shown in figure 13. Proposed protocol generates 33% lesser overhead ratio as compared to direct delivery protocol when TTL varies. As far as when TTL value increases, overhead ratio is also increasing slightly. BRON works more efficiently as compared to prophet, spray & wait, and direct delivery in terms of overhead ratio with respect to variation in TTL value.

Figure 14 and figure 15 depicts the performance of BRON and other routing protocols, for the parameter average latency and average buffer time when TTL value varies from 100 to 500 minutes. Proposed routing protocol performs 27% more efficiently as compared to direct delivery protocol in terms of average latency when TTL varies. Average latency parameter is slightly decreasing, when TTL value increases for all the considered protocol as shown in figure 14. However, BRON works efficiently as compared to other protocols in terms of average latency when TTL varies. BRON takes 13% lesser buffer time as compared to direct delivery protocol with respect to TTL value as shown in figure 15. Whenever the TTL value increases, buffer average time also increases slightly for all protocol shown in figure 15, but BRON takes lesser buffer time as compared to all other protocols.

3. Performance results while varying the field speed of the nodes: All the parameters mentioned in table 3 are remains default, when the field speed of nodes is varies from 0.2 to 1 km/h. Figure 16-20 presents the simulation results for the parameter packet drop ratio, delivery ratio, overhead ratio, average latency, and buffer time when the speed of the nodes in the network varies. BRON performs 43% more efficient in terms of packet drop ratio as compared to direct delivery protocol, when speed of nodes varies. There are no major changes has been considered while simulating the BRON protocol when speed of node varies from 0.2 to 1 km/h. But packet drop ratio is slightly increases when the node's speed increases. However, BRON performs much efficient in terms of packet drop ratio with respect to node's speed, as compared to other protocols which described in figure 16.

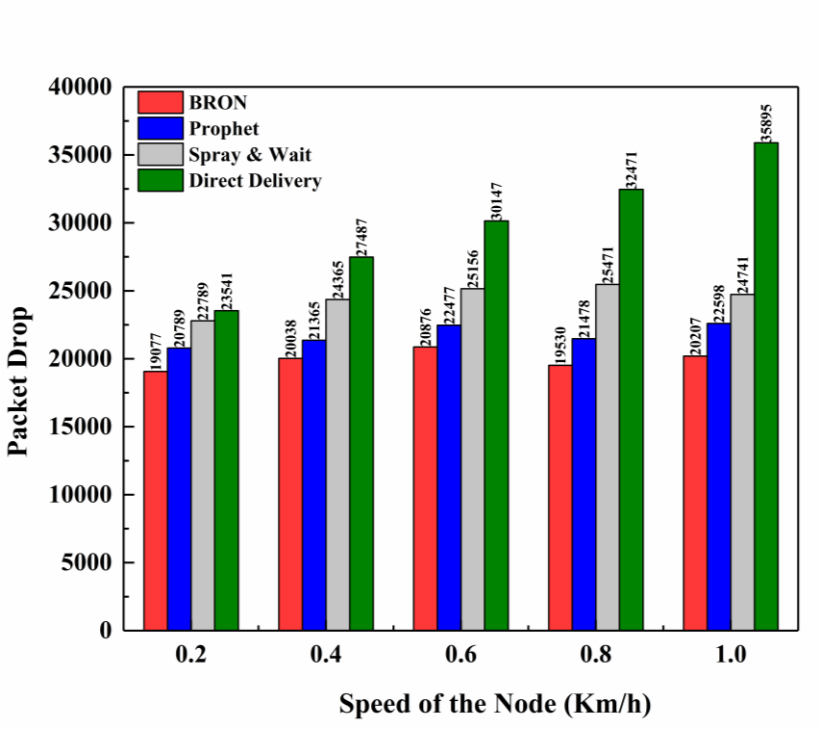


Fig. 16. Packet Drop vs. Speed of the Node

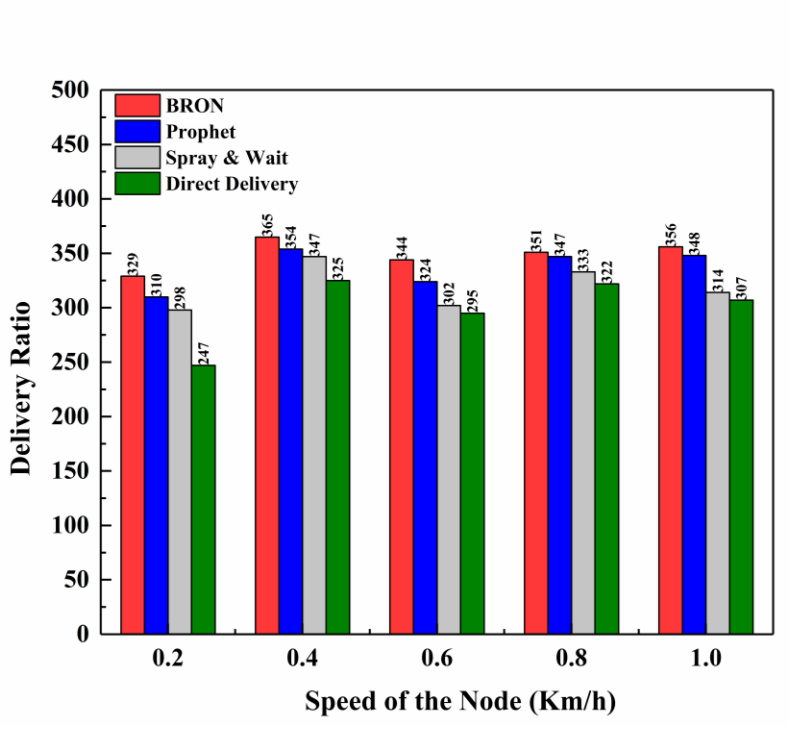


Fig. 17. Delivery Ratio vs. Speed of the Node

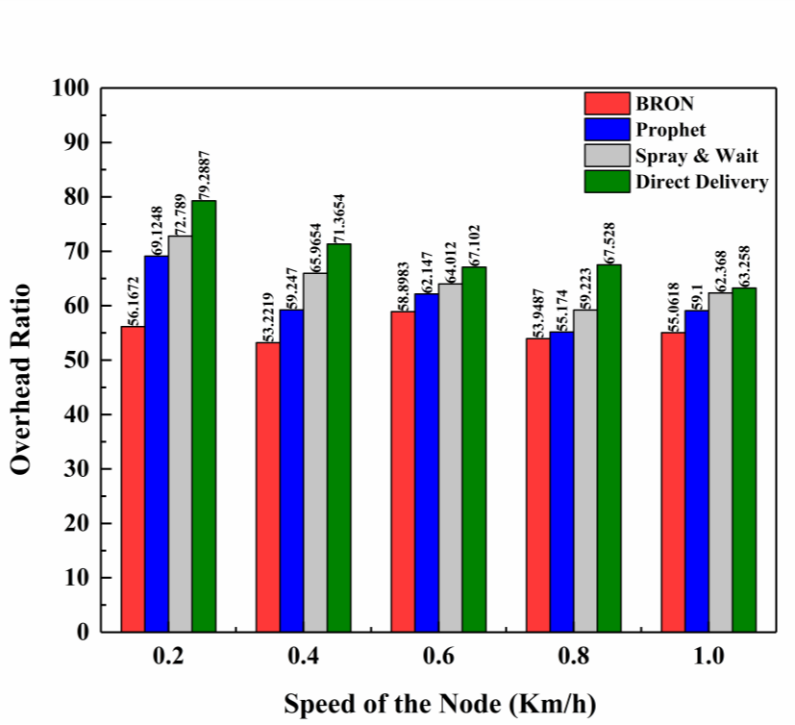


Fig. 18. Overhead Ratio vs. Speed of the Node

Figure 17 presents the results for the parameter delivery ratio when speed of the node varies. BRON performs efficiently as compared to other protocols in terms of delivery ratio with respect to speed of the node varies. BRON produced 24% enhanced delivery ratio in comparison with direct delivery protocol. As far as speed of the nodes increases, delivery ratio of the proposed protocol is also enhanced, this is the positive aspect of the proposed work.

Implementation results for the parameter overhead ratio with respect to speed of node is shown in figure 18. Proposed protocol generates 29% reduced overhead ratio as compared to direct delivery protocol when node's speed varies. Overhead ratio is also decreasing when speed of the nodes increases in case of BRON. As compared to other protocol, BRON performs much efficiently in terms of overhead ratio vs. speed of nodes.

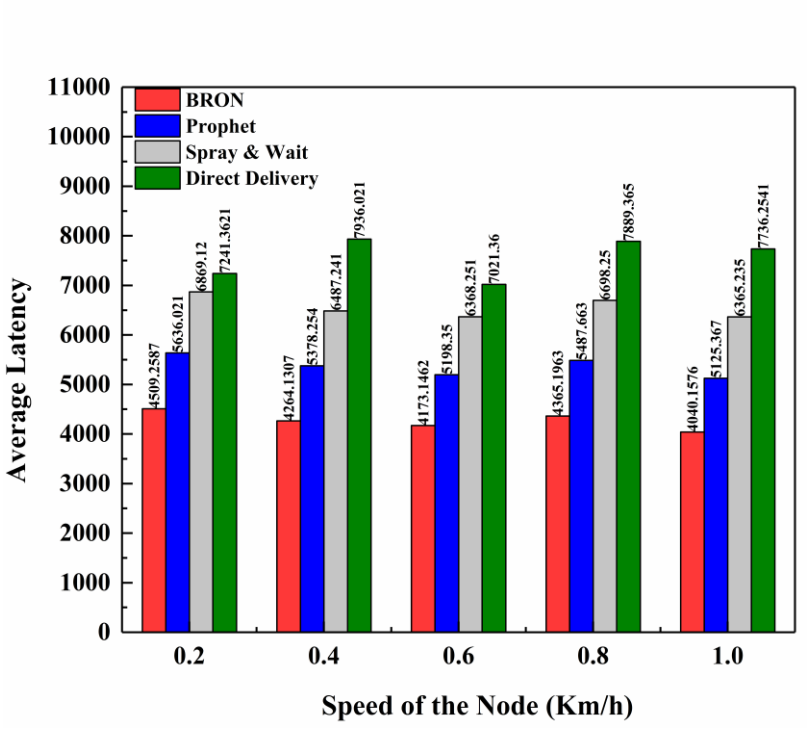


Fig. 19. Average Latency vs. Speed of the Node

The simulated results for the parameter average latency and average buffer time with respect to speed of the node are shown in figure 19 and figure 20 respectively. With the comparison of direct delivery protocol, BRON gives 47% reduced average latency when node's speed varies. As depicts in figure 19, it is very clear that proposed protocol works adequately in terms of average latency factor whenever the speed of the nodes varies. Figure 20 shows the performance result for the parameter buffer time vs. speed of the node. Here, BRON takes 21% lesser buffer time as compared to direct delivery protocol when the speed of the node varies. BRON also performs more efficiently as compared to other protocol which presented in figure 20.

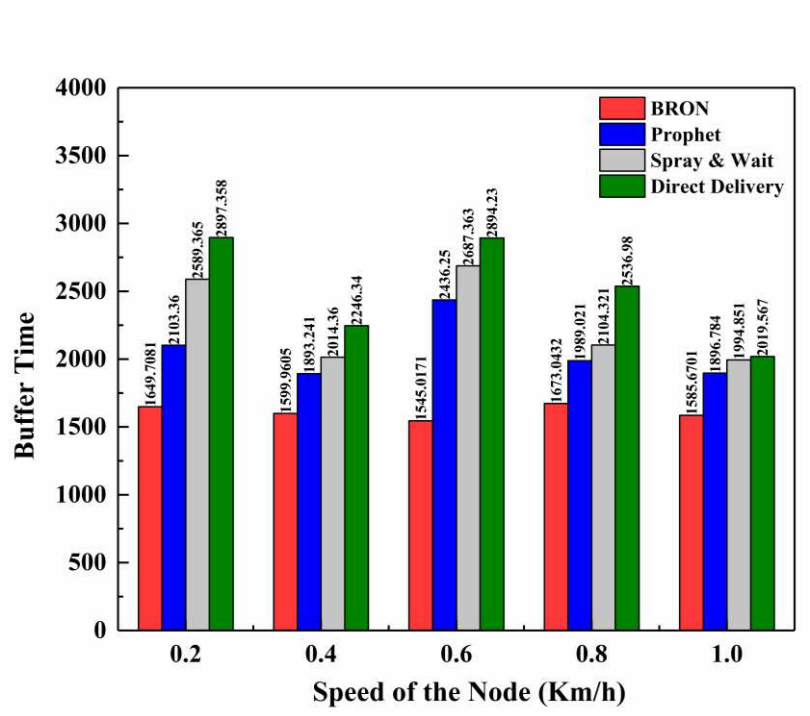


Fig. 20. Buffer Time vs. Speed of the Node

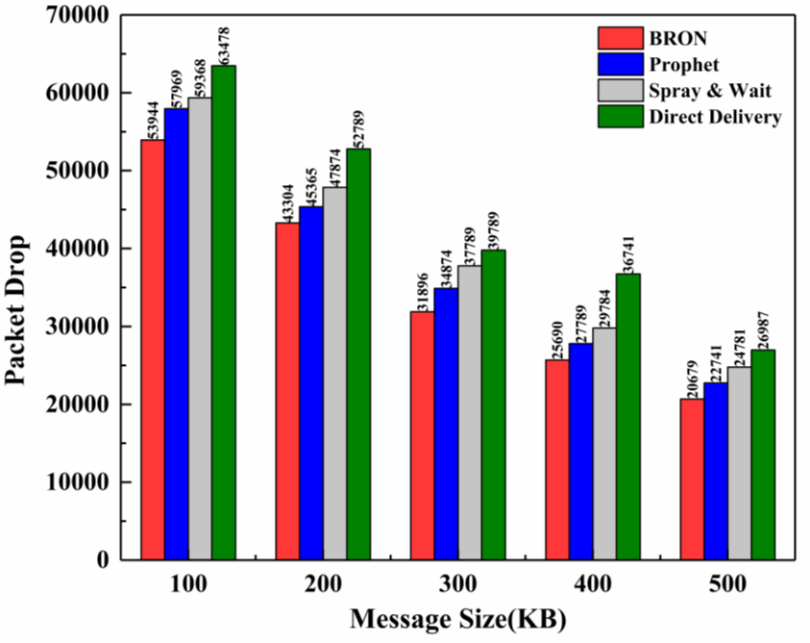


Fig. 21. Packet Drop vs. Message Size

Evaluated result during variation the message size: Parameters described in table 3 are kept default, when the field message size is varies from 100 KB to 500 KB. Simulation results for the parameter packet drop ratio, delivery ratio, overhead ratio, average latency, and buffer time when the message size in the network varies are presents in the figure 21-25. The simulated result for the proposed protocol BRON for the factor packet drops ratio when the message size is varies is presents in figure 21. As far as message size is increasing, there is also some increment in average packet drops in case of all protocols. However, BRON generates 23% lesser packet drops ratio as compared to direct delivery protocol whenever, message size varies in the network.

The results for the parameter average delivery ratio when the message size varies is presents in figure 22. BRON performs better as compared to other protocol in terms of delivery ratio vs. message size varies. Proposed protocol generates 25% more delivery ratio as compared to direct delivery protocol when message size varies. Delivery ratio parameter is decreases negligibly, as far as message size in increases, in case of all protocol as described in figure 22.

Figure 23 describes the results for the factor overhead ratio with respect to the message size varies. BRON generates 44% lesser overhead ratio as compared to direct delivery protocol with respect to message size varies. Overhead ratio is decreases, as far as message is increases. Here, BRON works adequately as compared to all other protocols as described in figure 23.

Average latency factor with respect to the message size varies is shown in figure 24. BRON works much more efficiently as compared to other protocols in terms of average latency parameter when message size varies. BRON, performs 34% more adequately as compared to direct delivery protocol in terms of average latency with respect to variation in message size.

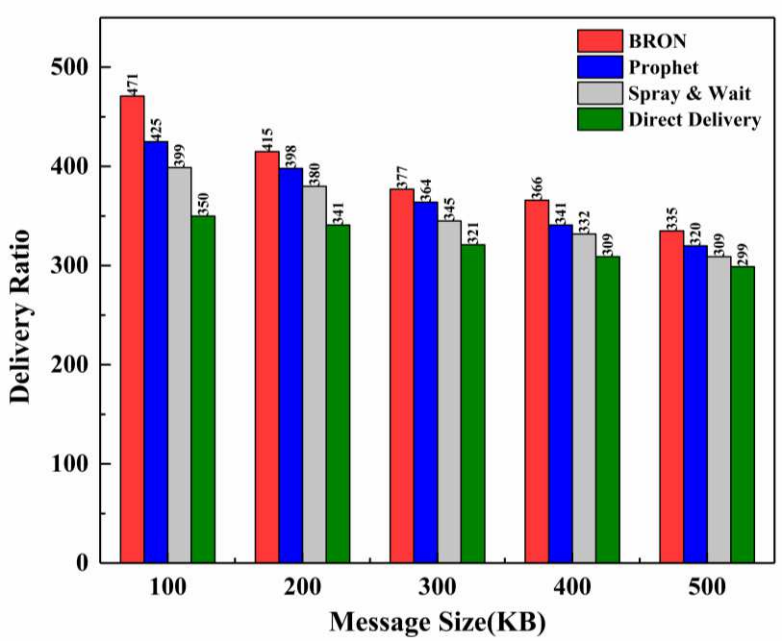


Fig. 22. Delivery Ratio vs. Message Size

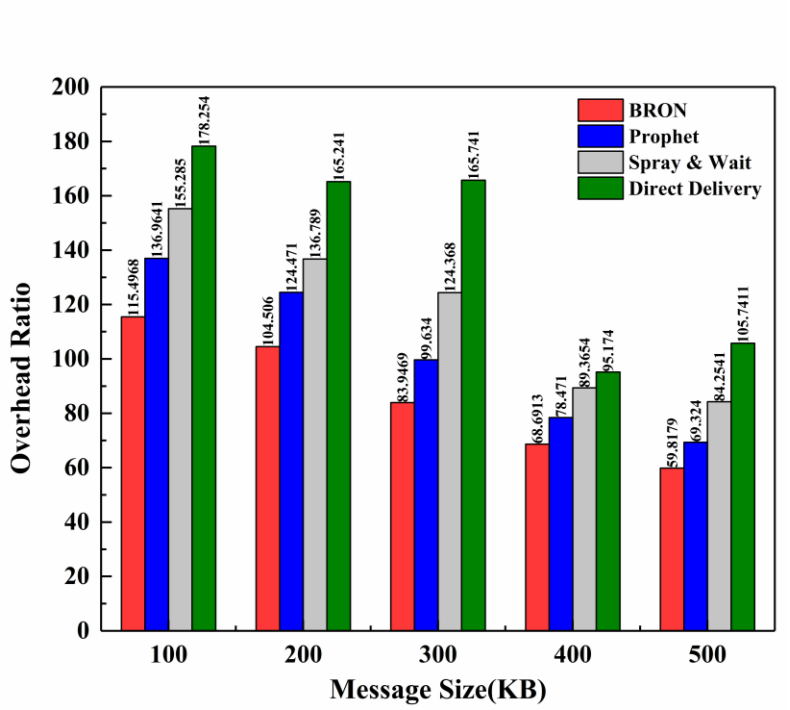


Fig. 23. Overhead Ratio vs. Message Size

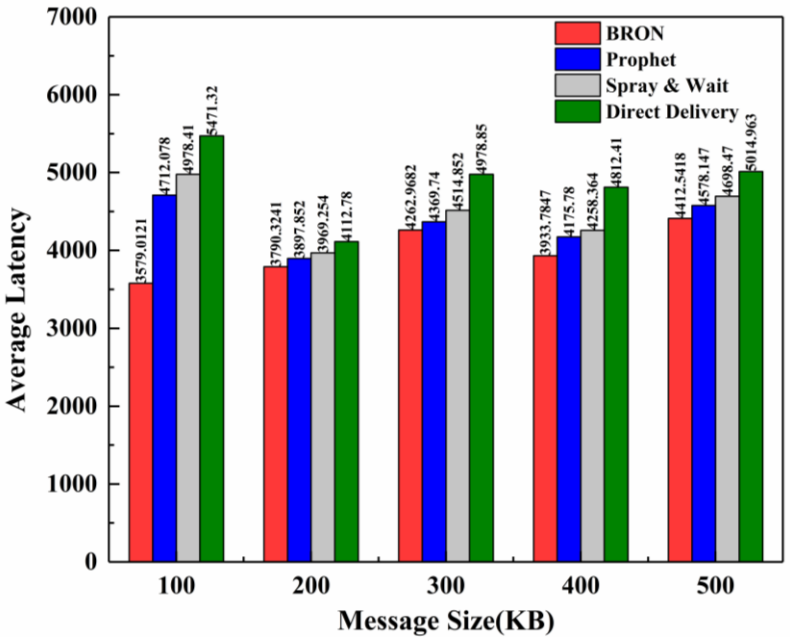


Figure 24. Average Latency vs. Message Size

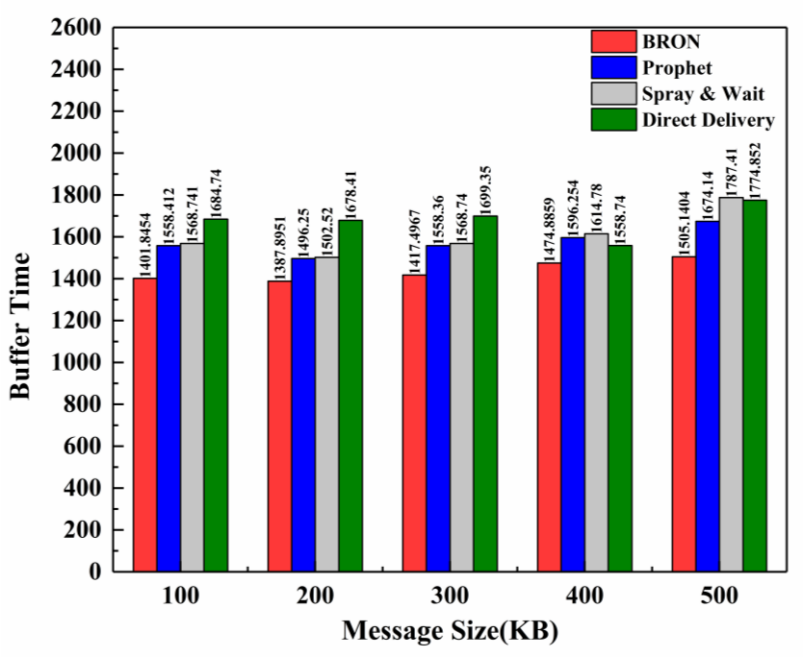


Figure 25. Buffer Time vs. Message Size

Result for the factor average buffer time with respect to variation in message size is presents in figure 25. BRON takes 15% reduced buffer time as compared to direct delivery protocol, when size of messages is varies. Buffer time of all the considered protocols are increases slightly, when the message size is increases. At beginning of the simulation time BRON takes 1401.845 sec. buffer time at 100 KB message size but afterwards, when message size is 500 KB, it takes 1505.14 sec. buffer time.

6. Conclusion and Future Work

The primary object of Opportunistic network is to provide secure and reliable communication in discontinuous linked devices. With the consideration of major challenges of this network, here the author proposed the safe and reliable trustworthy routing protocol named BRON. It utilised the idea of blockchain, to provide the reliable source to destination link for disseminating the packet in the network. Idea of Proof-of Work and Proof-of-Stake is used for the selection of trusted node in the Opportunistic network. By adoption of blockchain technology, trusted platform for Opportunistic network is provided. BRON is implemented on ONE tool and its result are evaluated. The performance of proposed routing is also compared with other protocols. BRON generates 36% reduced packet drops ratio, 57% enhanced delivery ratio, 55% lesser overhead ratio, 35.2% reduced average latency, and 65% lesser average buffer time as compared to direct delivery ratio with respect to number of nodes. In each and every aspect of proposed protocol, simulation result indicates that BRON is better routing protocol for Opportunistic network.

In future work, real-life application-based routing for opportunistic network will be considered. To enhanced the performance of BRON, few modifications can be included in algorithm of BLAKE2 [29]. Detection of malicious node can also be included as a new feature in BRON.

Declaration
Funding: Not Applicable
Conflict of interest: The authors declare that they do not have any conflict of interests. This research does not involve any human or animal participation. All authors have checked and agreed the submission.
Availability of data and material: Not applicable

Code Availability: Not Applicable, we have not used any dataset.

References

[1] C.-M. Huang, K.-C. Lan, and C.-Z. Tsai, "A survey of opportunistic networks," in Proc. 22nd IEEE Int. Conf. Adv. Inf. Netw. Appl. Workshops, 2008, pp. 1672–1677.

[2] Dalal, R., Khari, M., & Singh, Y. (2012, January). Survey of trust schemes on ad-hoc network. In International Conference on Computer Science and Information Technology (pp. 170-180). Springer, Berlin, Heidelberg.

[3] Farrell S, Cahill V. Security considerations in space and delay tolerant networks, Space Mission Challenges for Information Technology 2006 on Second IEEE International Conference, Pasadena, CA, USA, 2006; 8–38.

[4] Farrell S, Symington S, Weiss H, Lovell P. Delay tolerant networking security overview, Draft, IETF, 2009; 1–29.

[5] Shikfa A, Onen M, Molva R. Privacy in context-based and epidemic forwarding. Proceedings of the IEEE International Symposium on World of Wireless Mobile and Multimedia Networks & Workshops. Piscataway NJ: IEEE Press, 2009:1-7.

[6] Shikfa A, Onen M, Molva R. Bootstrapping security associations in opportunistic networks. Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). Piscataway NJ: IEEE Press, 2010:147-152

[7] Trifunovic, S. and Legendre, F., 2009. Trust in opportunistic networks. Computer Engineering and Networks Laboratory, pp.1-12

[8] Trifunovic, S., Legendre, F. and Anastasiades, C., 2010, March. Social trust in opportunistic networks. In 2010 INFOCOM IEEE Conference on Computer Communications Workshops (pp. 1-6). IEEE.

[9] Xi, C., Liang, S., JianFeng, M.A. and Zhuo, M.A., 2015. A trust management scheme based on behavior feedback for opportunistic networks. China Communications, 12(4), pp.117-129.

[10] M. Y. S. Uddin, B. Godfrey, and T. Abdelzaher, "RELICS: In-network realization of incentives to combat selfishness in DTNs," in Proc. 18th IEEE Int. Conf. Netw. Protocols, 2010, pp. 203–212.

[11] G. Bigwood and T. Henderson, "IRONMAN: Using social networks to add incentives and reputation to opportunistic networks," in Proc. 3rd Int. Conf. Privacy Security Risk Trust, 2011, pp. 65–72.

[12] Q. Li, W. Gao, S. Zhu, and G. Cao, "A routing protocol for socially selfish delay tolerant networks," Ad Hoc Netw., vol. 10, no. 8, pp. 1619–1632, 2012.

[13] H. Zhou, J. Chen, J. Fan, Y. Du, and S. K. Das, "ConSub: Incentive-based content subscribing in selfish opportunistic mobile networks," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 669–679, Sep. 2013.

[14] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," Ad Hoc Netw., vol. 8, no. 1, pp. 1–14, 2010.

[15] G. Wu, J. Wang, L. Yao, and C. Lin, "A secure social-aware incentive scheme for delay tolerant networks," in Proc. 12th IEEE Int. Conf. Trust Security Privacy Comput. Commun., 2013, pp. 813–820.

[16] T. Ning, Z. Yang, and X. Xie, "Incentive-aware data dissemination in delay-tolerant mobile networks," in Proc. 8th Annu. IEEE Commun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw., 2011, pp. 539–547.

[17] L. Wei, H. Zhu, Z. Cao, and X. Shen, "SUCCESS: A secure user-centric and social-aware reputation based incentive scheme for DTNs," Ad Hoc Wireless Sensor Netw., vol. 19, no. 1/2, pp. 95–118, 2013.

[18] N. Li and S. K. Das, "RADON: Reputation-assisted data forwarding in opportunistic networks," in Proc. 2nd Int. Workshop Mobile Opportunistic Netw., 2010, pp. 8–14.

[19] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," Ad Hoc Netw., vol. 11, no. 4, pp. 1497–1509, Jun. 2013.

[20] L. Dora and T. Holczer, "Hide-and-lie: Enhancing application-level pri- ´ vacy in opportunistic networks," in Proc. 2nd Int. Workshop Mobile Opportunistic Netw., 2010, pp. 135–142.

[21] I. Parris, G. Bigwood, and T. Henderson, "Privacy-enhanced social network routing in opportunistic networks," in Proc. 8th IEEE Int. Conf. Pervasive Comput. Commun. Workshops, 2010, pp. 624–629.

[22] Y. Ding, X.-W. Zhou, Z.-M. Cheng, and W.-L. Zeng, “Efficient authentication and key agreement protocol with anonymity for delay tolerant networks,” Wireless Pers. Commun., vol. 70, no. 4, pp. 1473–1485, Jun. 2013.

[23] Z. Jia, X. Lin, S.-H. Tan, L. Li, and Y. Yang, “Public key distribution scheme for delay tolerant networks based on two-channel cryptography,” J. Netw. Comput. Appl., vol. 35, no. 3, pp. 905–913, May 2012.

[24] L. Qinghua, Z. Sencun, and C. Guohong, “Routing in socially selfish delay tolerant networks,” in Proc. IEEE INFOCOM, pp. 1–9, 2010.

[25] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys & Tutorials, Thirdquarter vol. 18, no. 3, pp. 2084-2123, 2016.

[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in IEEE international congress on big data (BigData congress), pp. 557-564. June 2017.

[27] F. Coelho, A. Larroche, and B. Colin, Itsuku: a Memory-Hardened Proof-of-Work Scheme. Doctoral dissertation, MINES ParisTech-PSL Research University (2017)

[28] A. Biryukov, and D. Khovratovich, Egalitarian Computing. In *USENIX Security Symposium* (2016) 315-326.

[29] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. BLAKE2: simpler, smaller, fast as MD5, January 2013. Version 2013.01.29.

[30] B. Ostermaier, F. Dotzer, and M. Strassberger. Enhancing the security of local danger warnings in VANETs - a simulative analysis of voting schemes. In *Proceedings of ARES’07*, 2007.

[31] A. Keranen. ― Opportunistic Network Environment Simulator‖. Special Assignment Report, Helsinki University of Technology, Dept. of Communications and Networking, May 2008.