Artificial Intelligence based rule base fire engine testing model for congestion handling in opportunistic networks

Ahthasham Sajid¹, Nighat Usman², Imranullah Khan³, Saeeda Usman⁴, Aamir Mirza Mehmood¹, Muhammad Sheraz Arshad Malik⁵ and Javed Masood Rana⁶

Abstract
Opportunistic network is emerging as a research domain nowadays with the introduction of Internet of things phenomena. In recent years, storage level congestion issue due to handheld devices is considered as a key challenge to be handled in the opportunistic networks. The prime objective of conducting this research is to develop artificial intelligence rule-based fire engine model to be tested using artificial intelligence latest classification algorithms further implemented using ONE simulator tool over MaxProp protocol. The achieved results show 98% accuracy in terms of classification using k-fold validation technique over six algorithms. The achieved results have been compared with MaxProp protocol over evaluation parameters such as delivery ratio, throughput, routing load, and overhead; whereas delivery ratio increase about 20% for node level and 5% for buffer level and throughput tends to increase 500 and 150 kbps for network and buffer levels, respectively.

Keywords
Internet of things, less congested node, average congested node, high congested node, buffer occupancy, delay tolerant network

Date received: 30 April 2020; accepted: 17 June 2020

Background
An emerging research area that encompasses communication challenges in opportunistic networks is due to its intermittent connectivity and lengthy postpone in the network; for this reason, the Internet congestion control mechanisms are not suitable for opportunistic networks. Packet delivery ratio and transmission delay are the key challenges faced in such types of network.¹ Short range wireless communications such as Wi-Fi, Zigbee and Bluetooth, has introduced a new concept of communication known as opportunistic networks (OppNets) or pocket switch network (PSN).² In such networks, nodes exchange data using store carry and forward mechanics whenever they came in range of another device that is why it is called opportunistic networks.³ Due to limited storage capacity of handheld devices in 4G or 5G networks by the end user, only limited amount of data can be transferred. Nodes in 5G networks are, therefore, difficult to implement peer-to-peer communication for data exchange, so a new emerging type of communication via identifying suitable relay node as custodian node using store and forward mechanism is identified for bundle exchange between peers when a best opportunity is found in terms of storage and connectivity.⁴

Introduction
Communication scenario in recent years has changes dramatically due to billions of devices connected over
the Internet of things (IOT) by the users. Mobility aspect of device as well as user has given birth to emerging type of networks such as opportunistic networks. Communication in opportunistic networks relies totally on the opportunity of two user or nodes to contact each other. Congestion at both link and node level can affect communication, in general.5

In the case of opportunistic networks, due to irregular connectivity, heterogeneous network architecture and limited storage of the mobile node, it always suffers with storage (node) level congestion majorly. Intermediate nodes between source and destination tend to be more critical to cope with storage level congestion, as it cannot store bundle in its buffer space for longer time until next suitable opportunistic node is identified. Social connections among the users in the case of social networks may therefore help in identifying suitable forwarding intermediate node to transmit bundle in the network.6

Delivery ratio in opportunistic network would be increased by keeping an eye on key parameters that affect node level congestion directly such as time to live (TTL), number of copies, number of hop count and contact history between the peers in the opportunistic networks.7 One of the good policies to vacant buffer space is by deleting message for which no suitable contacting node is intact even after crossing it defined as threshold value. In opportunistic networks, flooding-based routing as its promise’s higher throughput with short delay could not always be a good solution due to handling limited storage capacity of the node.8 Due to the unstructured and unpredictable contact opportunity of communication or contacts, in opportunistic environment, node is not sure about contact opportunity as well as time period for which contact would be established, thus high diversity in node contact pairs leads to many available paths, as illustrated in Figure 1.

**Challenges of opportunistic network**

Following are the key challenges that opportunistic networks must deal with.

**Buffer space.** As discussed earlier, due to intermittent connectivity in opportunistic network, all intermediate nodes have to take custody of a message and these nodes have to store these messages in their buffer until an optimal next custodian node is found. Therefore, an intermediate node should have enough buffer space to incorporate the incoming messages.9

**Energy.** Due to high mobility and irregular connectivity among the nodes in opportunistic networks, an efficient routing scheme should be designed in such a way that is capable enough to overcome energy level issue to store and transmit the packets.9

**Reliability.** In opportunistic networks, it is viable to have reliable communication in the form of some acknowledgment received by a receiver to a sender, when a packet/message is received successfully.9

**Processing power.** One of the key objectives of opportunistic networks is to adopt such routing protocol, which requires limited processing power in terms of CPU and memory consumption. Contrary to the traditional network, nowadays, devices which are mostly being used are mobile devices.9

**Security.** Security is the most important objective in opportunistic or in any other network communication to achieve secure transmission between sender and receiver. It depends on the application to provide secure guaranteed mechanism and transmission using cryptographic techniques to achieve the authenticity.9

The major contribution of this research work is as follow:

- Development of an artificial intelligence (AI)–based validation and testing model.
- Artificial intelligence–based rule-based fire engine (AIbRBFE) to cope storage level congestion in opportunistic networks with high delivery ratio and less packet drop rate.

**Related work**

Opportunistic network does not follow a traditional feedback loop mechanism as adopted by other environment and routing schemes like wireless, mobile ad hoc network (MANET), etc. In opportunistic network, node can only use local information available to them at specific time to avoid node level congestion that can be done by removing data items in advance from the buffer of that node. Following methods is used to evict data item from the buffer of the node:10

1. Buffer eviction using acknowledgment.
2. Buffer size advertisements.
3. Data-centric node congestion avoidance.
4. Duplication avoidance.

The authors in this study have introduced a dynamic scheme where a routing decision could be taken adaptably according to situation by routing agent over bundle protocol for both ad hoc on-demand distance vector (AODV) and delay tolerant network (DTN) using transmission control protocol (TCP). Simulation shows that the high delivery ratio and shorter end-to-end delay are achieved in case of adopting DTN routing with bundle protocol in comparison with AODV with TCP. Collisions and retransmission issue at the MAC layer in case of using DTN and epidemic routing have been addressing using either AODV or DTN based on local information, message size and node density. Through simulation results, it is achieved that in case of dense network AODV and in case of sparse network DTN, routing protocol performs best with less delay and high delivery ratio. Epidemic routing suffers in case of too dense networks like node can run out of bandwidth. Decision of selecting TCP and DTN depends on node velocity, message size and node density, and these metrics could be used in a best manner if measured locally per node. Node density can be calculated upon aggregating measurement of the node encounters, whereas each node knows its speed and message size it carries normally. It has also been achieved by the simulation results that broadcast performs best in case of too dense network rather than multi-copy scheme in applying epidemic routing. 8

In this research work, the issue addressed is that a situation where a network frequently splits down in form for connected groups, so at that time DTN and MANET routing protocols do not perform well. In this research study, therefore, to cope with such situation, a hybrid protocol scheme, hybrid DTN-MANET (HYMAD), was introduced. HYMAD uses MANET for communication within the group, while it uses DTN for disjoint group to be communicated. HYMAD uses topological information exchange between the nodes to work in fully decentralized manner. Simulation done to evaluate results of HYMAD was using both artificial and real-life mobility traces, in terms of delivery ratio and delay HYMAD outperform multi-copy spray-and-wait DTN routing protocols. HYMAD uses distance vector for intra group and spray-and-wait for inter group routing. 11

It has been analyzed that, during this research work, few schemes have been introduced by combining both MANET and DTN routing aspects together. One of the techniques proposed by Whitbeck named as HYMAD. HYMAD uses MANET as a routing within the group and when intra group communication is required, so it uses DTN routing between disjoint groups. HYMAD has outperformed multi-copy spray-and-wait DTN routing protocols on the parameters of delivery ratio and delay by the achieved results. Assumption made in HYMAD to work on is that DTN nodes will form group in forming networks. In this approach, end-to-end semantic was trying to be maintained when end-to-end semantic does not exist, so the DTN-based communication will be used as another option. Internet protocol (IP) networking has been also introduced to cope long delay in environments but it found suitable to forward only moderate data units not a large/big files. 12

**Problem formulation and proposed scheme**

Communication under opportunistic networks is done using hop-by-hop manner. Packet forwarding totally depends on opportunity of contact between nodes; therefore, such type of networks must bear longer delay and high message drop rate and node level congestion due to limited buffer capacity of nodes as one of the key challenges. In opportunistic environment, in the case of multiple copies protocol, a message with various copies exists in the network; therefore, if a message must be stored for longer time in buffer would, therefore, cause overhead for the node specifically and for network in general. Therefore, an efficient buffering strategy should therefore store message in buffer for minimum time as a best custodian node is found so message should be evicted from the buffer. If the buffering time is too long, buffers will fill up and more messages can be neither received nor forwarded or messages may be dropped. An intelligent technique is thus required which should reduce the challenges of limited buffer space as addressed. In this research work, such intelligent rule-based fire engine is implemented by categorizing node, (low), (average) and (high) congested node, based on node current buffer availability to cope node level congestion efficiently. Efficiency in the technique has also been enhanced based on contact history to be used as logic to decide best relaying nodes such as (Custodian) node in opportunistic networks.

**AIbRBFE**

This research work consists of two phases: in phase one, an artificial intelligence–based validation and testing model is presented in Figure 2. Random forest and Gradient boosting algorithms are used for testing to check accuracy of the proposed AIbRBFE model. In phase two of this paper, simulation performed using ONE simulator with MaxProp protocol has been tested, and the achieved results is compared on these key evaluation parameters such as delivery ratio, network load, routing load, drop rate and throughput at network, node and buffer level.

**Model of AIbRBFE**

The below model, as illustrated in Figure 2, has been developed to check the accuracy of the proposed rule-
based expert system in the figure previously. This AI model consists of two sub models: Model 1 is for predicting TTL class either less, average or high based on set threshold. Model 2 has been designed and validate for checking accuracy of the proposed rules such as (X) and (Y).

**Working of AlRBFE**

The implemented artificial intelligence rule-based fire engine calculated buffer occupancy (BO) using equation (1), less congested node (LCN) using equation (2), average congested node (ACN) using equation (3) and high congested node (HCN) using equation (4)

\[
\text{Buffer occupancy (BO)} = \frac{\text{Accrued Buffer Size}}{\text{Total Buffer Size}} \times 100
\] (1)

\[
\text{LCN} = BO \geq 0\% \text{ & & } BO \leq 30\% 
\] (2)

\[
\text{ACN} = BO \geq 31\% \text{ & & } BO \leq 75\% 
\] (3)

\[
\text{HCN} = BO \geq 76\% \text{ & & } BO \leq 100\% 
\] (4)

TTL of packet in queue are categorized either low, average and high TTL using equations (8)–(10), respectively, using TTL_TH_1 (TTL_Threshold_1), TTL_TH_2 (TTL_Threshold_2) and TTL_TH_3 (TTL_Threshold_3) and calculated using equations (5)–(7), respectively, further

\[
TTL_{TH_1} = (LB) \geq 0\% \text{ & & (UB) } \leq 30\% 
\] (5)

\[
TTL_{TH_2} = (LB) \geq 31\% \text{ & & (UB) } \leq 70\% 
\] (6)

\[
TTL_{TH_3} = (LB) \geq 71\% \text{ & & (UB) } \leq 100\% 
\] (7)

\[
LOW_{TTL} = \frac{TTL_{TH_1}}{100} \times \text{Total TTL Size} 
\] (8)

\[
AVG_{TTL} = \frac{TTL_{TH_2}}{100} \times \text{Total TTL Size} 
\] (9)

\[
HIGH_{TTL} = \frac{TTL_{TH_3}}{100} \times \text{Total TTL Size} 
\] (10)

**Algorithm for AlRBFE**

**Input:** Buffer Occupancy, TTL
**Processing:** Calculate Buffer Occupancy, Calculate TTL Threshold, Categorized TTL Packets, Call (AlRBFE)
**Output:** Match and Fire rule from (AlRBFE)
**Procedure:** Node Contacting Module ()

1. **START**
2. **Assign Labels** to each node; (LCN, ACN and HCN) using equations (2), (3) and (4)
   - For Each node n in (Ni)Categorized Node (LCN, ACN and HCN)
     - LCN = (BO > = 0 % & & BO < = 30 %)
     - ACN = (BO > = 31 % & & BO < = 75 %)
     - HCN = (BO > = 76 % & & BO < = 100 %)
3. **Calculate TTL Threshold using equations (5), (6) and (7)**
   - TTL_TH_1 = ((LB) 0% & & (UB) 30%)
   - TTL_TH_2 = ((LB) 31% & & (UB) 70%)
   - TTL_TH_3 = ((LB) 71% & & (UB) 100%)
4. **Categorized TTL packet’s** (Low_TTL, Average_TTL and High_TTL) using equations (8), (9) and (10)
   - For Each bundle in Contacting node Queue
     - Low_TTL = (TTL_TH_1/100) * Total_TTL_Size
     - Average_TTL = (TTL_TH_2/100) * Total_TTL_Size
     - High_TTL = (TTL_TH_3/100) * Total_TTL_Size
5. **Call (AlRBFE)**
6. **Match and Fire Rule from (AlRBFE)**
   - IF (Rule 1 to Rule 6)
     - Call Rule Base (A)

**Figure 2.** Artificial intelligence–based model of rule-based fire engine.
Else (Call Rule Base (B))
{
    IF (Rule 7, 8 and 9) && Rule (10)
    {
        Fire Decision 2
    }
    IF (Rule 7, 8 and 9) && Rule (11)
    {
        Fire Decision 3
    }
    FINISH
}

Fire Decision 1

Rule bases
The implemented AlbRBFE consists of two rule bases such as rule base A is presented in subsection “Rule base (A)” and rule base B in subsection “Rule base (B).” Rule base A consists of total six rules from rule 1 to rule 6 and one decision to be fired against match, whereas rule base B consists of three rules such as rule 7 to rule 9 which work further with rule 10 and rule 11 to fire decision 2 and decision 3 upon match criteria.

Rule base A. Rule base A consists of total six rules such as rule (1) to rule (6) and one decision upon match to be fired from database.

Rule 1: LCN Encounter with LCN
Rule 2: ACN Encounter with LCN
Rule 3: HCN Encounter with LCN
Rule 4: LCN Encounter with HCN
Rule 5: HCN Encounter with ACN
Rule 6: HCN Encounter with HCN

Decision 1: Either nodes have met before or not so evict messages from the queue in less, average and high TTL priority.

Rule base B. Rule base B consists of total five rules such as rule (7) to rule (11) and two decisions upon match to be fired from database, as illustrated in Figure 3.

Rule 7: LCN Encounter with ACN
Rule 8: ACN Encounter with ACN
Rule 9: ACN Encounter with HCN
Rule 10: Previously Contacted
Rule 11: Previously Not Contacted

Decision 2: Evict messages from the contacting node buffer in less, average and high TTL order.

Decision 3: Evict message from the contacting node buffer in order of high, average and less TTL.

Testing of AlbRBFE
Figure 4 illustrates comprehensive test accuracy achievement for all the seven classification techniques used for testing and validating proposed AlbRBFE in this research paper. 10k-fold validation techniques are performed (A stacking generative, Support Vector Machine (SVM), Naïve Bayes, decision tree, x-gradient boosting, random forest and gradient boosting). On the basis of average accuracy achieved, proposed AlbRBFE ending Random Forest (0.91048486) and Gradient boosting (0.90992168) are finally selected due to high accuracy and tested further for classifying node category either as LCN, ACN and HCN as well as TTL category as low, average and high TTL packets in the queue of transmitting node.
Under first phase, initially 150 and 300 nodes over 15,000 and 25,000 simulation times has been tested with both Random Forest and Gradient Boosting techniques.

Figure 5(a) illustrates that 150 nodes over random forest technique were tested over 15,000 s simulation time and 300 nodes over 15,000 s simulation time, as shown in Figure 5(b). 150 and 300 nodes over 15,000 s simulation time predicted two output classes of TTL, such as high TTL and average TTL, no data from less TTL over this time frame could be extracted. Accuracy was 94% for both classes and 97% over 300 nodes, as shown in Figure 5(b).

Figure 5(c) illustrates random forest using 300 nodes with classes of TTL. Accuracy for high TTL and average TTL was 92% and for third class (less TTL), accuracy achieved was 99%.

Figure 6(a) illustrates gradient boosting techniques as tested over 25,000 s simulation time with 150 nodes and Figure 6(b) illustrates test performed using gradient boosting over 300 nodes with 15,000 s simulation time. In 25,000 s simulation time, all three classes of TTL were predicted, such as less TTL with 79%, average TTL with 71% and high TTL with 83% accuracy was achieved. Figure 6(b) shows the accuracy achieved with 300 nodes over 15,000 s simulation time as 94% for high TTL and 95% for average TTL.

Figure 6(c) illustrates gradient boosting technique test analysis performed over 25,000 s simulation time with 300 nodes to predict classes of TTL and it provided 95% accuracy for classifying TTL packets based on threshold.

Simulation environment and result discussion

Simulation work for this study has been conducted using ONE simulator tool specifically designed to support opportunistic environment using MaxProp key protocol. Simulation parameters used under this research study is presented in Table 1. Results based on key evaluation parameters, such as delivery ratio, throughput, packet drop rate, routing load and overhead, have been analyzed and presented further in this section.

Results discussion

Figure 7 illustrates routing load comparison of proposed AlrbRBFE with MaxProp key protocol against maximum number of nodes 500 used in the simulation test. Routing load for proposed AlrbRBFE due to efficient forwarding of packets from the queue of contacting node using rule-based fire engine has outperform existing routing protocol MaxProp.

Figure 8 further illustrates relationship between number of nodes comparison of proposed AlrbRBFE with MaxProp key protocol with respect to throughput. 100–500 nodes have been tested in the simulation to measure throughput of the AlrbRBFE; throughput for both MaxProp and AlrbRBFE initially over 100 nodes were 35 kbps but at the end, over 500 nodes, it ended up with 5000 kbps for AlrbRBFE and 4500 kbps for MaxProp, so overall increase in 500 kbps has been achieved in the proposed technique due to its efficient packet forwarding logic to vacant buffer. So, Figure 5 clearly illustrates that rule-based fire engine has outperform existing routing protocol MaxProp in terms of throughput.

Figure 9 further illustrates relationship between throughput parameter over different buffer sizes used in simulation work. In the beginning, throughput for MaxProp protocol was 1620 kbps and for AlrbRBFE, it was 1900 kbps, but when the buffer size increased from 3 MB to 12 MB, throughput for AlrbRBFE has
Figure 5. Random forest for (a) 150 nodes with 15,000 times; (b) 300 nodes with 15,000 times; and (c) 300 nodes with 25,000 times.

Figure 6. Gradient boosting for (a) 150 nodes with 25,000 times; (b) 300 nodes with 15,000 times; and (c) 350 nodes with 25,000 times.
increased as well and ended up with 2200 kbps, whereas MaxProp ended at 2050 kbps.

Figure 10 illustrates relationship of overhead and buffer size of the different nodes in the simulation. Minimum buffer size of 3 MB buffer and maximum buffer size of 12 MB buffer have been set for the nodes under simulation test. Overhead for proposed AlbRBFE was at higher side up to 8 MB buffer size in comparison with MaxProp protocol, whereas after 9 MB buffer size, proposed AlbRBFE system has improved in terms of overhead too. In the beginning with 3 MB buffer, overhead was 535 for AlbRBFE and 510 for MaxProp protocol and at the end, with over 12 MB buffer, overhead was over 300 intended for both.

Figure 11 describes how various number of nodes in the network with respect to different simulation times behaved in terms of overhead. As the number of nodes in the networks tends to increase from 100 to 500 nodes gradually, similarly overhead has also increased as it was near 90 for 10,000, 20,000 and 30,000 s simulation time for 100 nodes, whereas over 500 overhead ended at 800, 760 and 730 for 10,000, 20,000 and 30,000 s simulation time, respectively.

Figure 12 shows relationship in terms of delivery ratio for all three types of nodes classified in this research work such as LCN, ACN and HCN.
number of nodes in the networks tends to increase in the network, delivery ratio also increased dramatically for all types of nodes with more opportunities of bundle to be transmitted. For 500 nodes in the simulation test nodes, LCN, CAN and HCN ended with 455, 450 and 442 packets’ delivery, respectively.

Figure 13 illustrates relationship between various buffer sizes used in the simulation with respect to delivery ratio achieved. Initially, over 3 MB buffer size delivery ratios were at low side; 16% for both MaxProp and AlbRBFE but as the buffer size increases from 3 MB to 12 MB gradually for the nodes, delivery ratio also increased. Over 12 MB buffer size, delivery ratios ended at 54% and 51% for AlbRBFE and MaxProp, respectively.

Conclusion
In this research study, artificial intelligence–based classification algorithm have been tested and validated over proposed rule-based fire engine to cope node level congestion in opportunistic networks. Training of data has been done using 20% and testing has been performed over 80% of the total data sets used in both model of the proposed AlbRBFE. Results have been compared using two random forest and gradient boosting algorithm for predicting all three classes of TTL such as less, average and high. Accuracy check testing of AlbRBFE has been done using 150 and 300 nodes. Random forest with 150 nodes and 10,000 s simulation time has achieved accuracy of 94% as shown in Figure 3(a), 97% as shown in Figure 3(b) and 92% as shown in Figure 3(c). Gradient boosting with 150 nodes and 10,000 s simulation time has achieved accuracy of 83% as shown in Figure 4(a), 95% as shown in Figure 4(b) and 98% as shown in Figure 4(c). Delivery ratio for all LCN, ACN and HCN types of nodes increased dramatically and overall throughput for entire network is also enhanced for AlbRBFE in comparison with MaxProp protocol.

Future works
Overhead and routing load yet need to be improved for the proposed AlbRBFE, so in future, we will address these issues so that efficiency of the proposed fire engine system could be improved further. Reducing the number of packet drop rate could be another interesting parameter for the researchers.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs
Imranullah Khan https://orcid.org/0000-0002-3268-4844
References

1. Trifunovic S, Kouyoumdjieva S, Distl B, et al. A decade of research in opportunistic networks: challenges, relevance, and future directions. *IEEE Commun Mag* 2017; 55: 168–173.

2. Kuppusamy V, Thanthrive U, Udugama A, et al. Evaluating forwarding protocols in opportunistic networks: trends, advances, challenges and best practices. *Future Int* 2019; 11(5): 113.

3. Chancay-Garcı´a L, Herna´ndez-Orallo E, Manzoni P, et al. Optimising message broadcasting in opportunistic networks. *Comput Commun* 2020; 157: 162–178.

4. Zhu Y, Zhang L, Shi H, et al. An adaptive routing-forwarding control scheme based on an intelligent fuzzy decision-making system for opportunistic social networks. *Symmetry* 2019; 11(9): 1095.

5. Pan D, Ruan Z, Zhou N, et al. A comprehensive-integrated buffer management strategy for opportunistic networks. *EURASIP J Wirel Commun Netw* 2013; 2013(1): 103.

6. Keränen A. The ONE simulator for DTN protocol evaluation. In: *Proceedings of the 2nd international ICST conference on simulation tools and techniques*, Rome, 2–6 March 2009, pp. 55. Portland, OR: ICST.

7. Lakkakorpi J, Pitkänen M and Ott J. Adaptive routing in mobile opportunistic networks. In: *Proceedings of the 13th ACM international conference on modeling, analysis, and simulation of wireless and mobile systems*, Bodrum, Turkey, 17–21 October 2010, pp. 101–109. New York: ACM.

8. Yahaya B. Congestion control strategies on integrated routing protocol for the opportunistic network: a comparative study and performance analysis 2015; 117(4): 5–10.

9. Soelistijanto B and Howarth MP. Transfer reliability and congestion control strategies in opportunistic networks: a survey. *IEEE Commun Surv Tutorials* 2013; 16: 538–555.

10. Radenkovic M and Grundy A. Congestion aware forwarding in delay tolerant and social opportunistic networks. *2011 Eighth International Conference on Wireless On-Demand Network Systems and Services*, Bardonecchia, 2011; 60–67. DOI: 10.1109/WONS.2011.5720201

11. Zhang D, Yang M and Cui L. Congestion control strategy for opportunistic network based on message values. *J Networks* 2014; 9(5): 1132–1138.

12. Whitbeck J and Conan V. HYMAD: hybrid DTN-MANET routing for dense and highly dynamic wireless networks. *Comput Commun* 2010; 33(13): 1483–1492.