Intelligence-based Routing for Smarter and Enhanced Opportunistic Network Operations

Bassem Mokhtar
Department of Electrical Engineering
Faculty of Engineering, Alexandria University
Alexandria, Egypt
bmokhtar@alexu.edu.eg

Mostafa Mokhtar
Department of Computer Science Engineering
Faculty of Engineering, Alexandria University
Alexandria, Egypt
mustafa.moukhtar@gmail.com

***Abstract*— Opportunistic networking architecture supports mobile cloud computing technology for provisioning huge dynamic resource demands by the ever-growing and continually-evolved Internet. Opportunistic networks are highly dynamic networking environments where there are no static routes and known infrastructure for having consistent end-to-end communication. Additionally, great challenges exist in establishing efficient routes due to mobility features of communicating nodes. Many routing schemes have been proposed in order to optimize quality of service (QoS) of such networks. In this paper, we present intelligence-based routing approach for opportunistic networks via developing application-level reasoning models for learning patterns of data traffic and extracting data semantics. Those semantics, continuously updated, are multi-operation-domain-related highly-abstracted information which aid routing nodes in knowing/expecting locations of more reliable and possible next hop nodes. Hidden Markov models and Fuzzy logic are adopted for designing semantics reasoning models and they are implemented over a set of routing nodes in a simulation scenario. Evaluation results show that integrating our proposed intelligence approach with two existing routing protocols leads to higher data delivery and minimized communication overhead ratio with good level of latency compared with protocols operation without intelligence.**

Keywords- Opportunistic Networks; Semantic-driven Operation; Routing Protocol; Context Awareness; Network Semantic, Information Management.

I. INTRODUCTION

Opportunistic networks enable networking and communication infrastructure for supporting the mobile cloud computing technology, which is emerged due to the proliferation and diversity of mobile smart Internet-enabled entities (e.g., smartphones) [1]. This evolving computation technology allows mobile Internet users to allocate, share and exploit available resources provisioning dynamic QoS requirements of various running Internet applications and services. Since opportunistic networks are highly dynamic challenged mobile ad hoc networks with intermittent connectivity [2], mobile communicating nodes meet great challenges in finding next hop nods and routing data with constant link performance in order to accomplish interesting applications and services. In addition, opportunistic networks are considered as sub-class of delay tolerant networks where end-to-end delay varies [2] [3]. Consequently, delay sensitive services and applications with specific QoS requirements encounter difficulties in running them at such opportunistic networking environments.

Communicating nodes in opportunistic networks can play different roles (e.g., end system host and router). Such networks are a type of packet switching network architecture with store-and-forward technology for transferring data packets amongst nodes. For enhancing network scalability, data routing and delivery ratio, opportunistic network infrastructure is divided into areas where each area comprises group of nodes where some of them can play routing roles. Routing nodes might have powerful resources compared with other nodes located at the same group in order to be able to direct efficiently and successfully data to their interesting destinations.

Routing and data forwarding issues occupy a prominent position in the interesting research issues related to opportunistic networks [3]. Developing efficient routing protocols for such networks can aid, to a large extent, in enhancing QoS and allowing wide scope of applications to be run over these networks. In literature, there are various routing scheme classes that have been proposed for opportunistic networks [4]. Routing in such networks depends on finding suitable paths and/or potential next hop nodes for forwarding data packets since there are no dedicated paths. Some presented routing protocols (flooding-based routing) rely on generating many data packet copies and sending them over the network to increase the probability of data delivery [5]. This scheme leads to high data overhead and latency in networks. Other trials aimed at developing routing schemes (prediction-based routing) with minimum overhead via estimating behavior of surrounding nodes in order to forward data packets to certain set of nodes with high existence probability [6].

In this paper, we provide intelligence-based routing approach for opportunistic networks. The proposed approach depends on developing semantics reasoning models using monolithic intelligence techniques. Those models are implemented on and distributed over powerful network nodes with routing roles for learning patterns of data traffic and reasoning about highly abstracted

 ISBN: 978-1-61208-439-8

information, or semantics. Those semantics are related to various operation domains such as application- and resource-directed issues. For instance, extracted semantics might give information about locations in a network that are interesting in a specific application. Also, learned information can direct routers to forward data to certain set of nodes because they are reliable with good levels of resources. Extracted semantics are maintained and updated continuously in a shared accessible database server allowing authorized communicating nodes to retrieve and learn semantics in order to optimize QoS of their interesting applications. The proposed routing approach can aid in enhancing operation of various existing routing classes applied to opportunistic networks. For example, flooding-based (e.g., epidemic) and prediction-based (e.g., prophet) routing protocols can be integrated with intelligence techniques for aiding in enhancing QoS of related running applications. Enhancing the operation of such protocols will help maximize data packets delivery ratio and minimize resource consumption and network latency. Overall, we aim at enhancing performance of opportunistic networks enabling such environments to accept various applications and services with dynamic QoS requirements.

The remaining of this paper is organized as follows. Related work is presented in Section II. Section III presents our proposed intelligence-based routing approach for enhancing QoS of running applications within opportunistic networks. More technical depth for the adopted intelligence technique is discussed in Section IV. Preliminary results of the proposed routing approach are presented in Section V. Section VI concludes the paper and highlights our future work.

II. Related Work

In literature, lots of research work has investigated and proposed routing protocols for opportunistic networks. In addition, other works have surveyed and classified routing schemes within such networks [4]. Routing schemes in opportunistic networks can be mainly classified as direct transmission, flooding-based schemes [5], prediction-based schemes [6], coding-based schemes, and context-based schemes. The main target of any proposed routing scheme is to ensure successful data delivery to destinations nodes relying on next available hop node-based rule. Unlike routing in case of direct transmission-based schemes, data sources have to wait until finding destination nodes in order to deliver data successfully [7]. Other routing schemes provide routing methodology based on data dissemination to ensure finding next hop nodes with high probability [5]. For minimizing communication overhead, probabilistic techniques-based routing schemes were presented for estimating available next hop nodes relied on calculated statistics and data captured from surrounding context [6][8].

An integrated routing protocol was proposed for enhancing operations of epidemic and prophet routing protocols [8]. The developed protocol utilizes context-based information to decide whether using forward data based prediction technique or via apply data dissemination. But, the proposed protocol did not provide a way for forming dynamic information model that can be used by routing nodes on demand and at runtime to estimate locations of next hop nodes. It assumed that information might not exist. So, it might be directed to flooding-based routing.

Some trials target proposing hybrid routing protocols where a combination of more than routing schemes according to presented classes in [4] can be formed to provide more reliable routing roles. For instance, a context aware routing methodology was provided based on using destination-sequence distance-vector algorithm and probabilistic routing scheme [9]. Such routing scheme exhibits large control overhead affecting data delivery rate. Another trial was presented to mitigate challenges of proposing hybrid routing protocol with low control overhead using optimized link-state routing version 2 [10]. However, there were no capabilities for estimating information from surrounding context that enables efficient changes in routing tables. In the next section, we will describe our intelligence-based routing approach highlighting differences with other trials for developing integrated and hybrid routing protocol for opportunistic networks.

III. Intelligence-based Routing Approach for Opportunistic Networks

Figure 1 presents briefly the proposed intelligence-based routing approach. Our presented routing approach can be considered as an integrated or hybrid routing

Algorithm 1: Intelligence-based Routing Scheme

Input: raw network data, D_{Raw} (including attributes such as node identifiers and data packet size); current routing configuration parameters, R_p (e.g., next-hop node ID in routing tables); initial reasoning model parameters, M_p; training data set, $D_{training}$; reasoning window size, T_R.

Operations:

1. **for** every T_R **do**
2. Learning set of data attributes A using machine learning algorithm $\mathbf{f}_{ML}$: $A = \mathbf{f}_{ML}(D_{Raw})$
3. Classifying A using data classification techniques $\mathbf{f}_{class}$ & based on each attribute's value to get A_c: $A_c = \mathbf{f}_{class}(A)$
4. Training adopted reasoning model adopting supervised/unsupervised learning algorithms $\mathbf{f}_{learn}$ to get its adjusted parameters $M_{p,new}$: $M_{p,new} = \mathbf{f}_{learn}(D_{training}, M_p)$
5. Extracting high-level features F based on the trained reasoning model and classified attributes. $F = f_{\text{reason}}(A_c, M_{p,new})$
6. Representing F as correlated semantic topics or information S, according to common learned classified attributes and using semantics representation model $\mathbf{f}_{rep}$: $S = \mathbf{f}_{rep}(F)$
7. Modifying R_p according to learned S: $R_{p,new} = \mathbf{f}_{alter}(R_p, S)$
8. **end for**

Output: $R_{p,new}$, S

Figure 1. The proposed intelligence-based routing scheme

scheme that combines operation features of more than one routing scheme class. In other words, the operation of the presented routing approach relies on integrating artificial intelligence techniques with work methodology of any routing scheme class in order to optimize scheme's overall operation. This is done via attaching routing schemes with efficient decision making abilities for routing data based on embedded enhanced semantics reasoning and situational awareness capabilities and accessible continually-updated information. This information is maintained at database servers helps distributed routing nodes to find, with high probability, location-specific next hop nodes and know more reliable nodes with sufficient resources in order to get consistent end-to-end communication. For provisioning privacy, communicating nodes register their identifiers (ID) at database servers to get information access authorization. Also, authorized communicating nodes will be able to learn knowledge on demand and at runtime that helps those nodes direct data packets to certain areas with high data delivery probability. For retrieving and learning helpful knowledge, authorized communicating nodes will communicate with available localized database servers based on the proximity base. In next subsection, we provide an example which clarifies the routing strategy via the proposed intelligence-based approach.

A. *Routing Strategy*

We discuss the operation of our proposed intelligence-based routing approach for opportunistic networks via a simple network scenario as depicted in Figure 2. The scenario comprises two network levels. The first level concerns the running applications where its shows various interesting applications and services implemented on communicating nodes. That level shows that some mobility-enabled nodes, e.g., routing nodes, employ reasoning models to reason about semantics. The other level describes the communication and routing level where data traffic among communicating mobile nodes and also information (or semantics) traffic transferred between nodes and shared database servers. Distributed routing nodes capture raw data from passed traffic and they learn

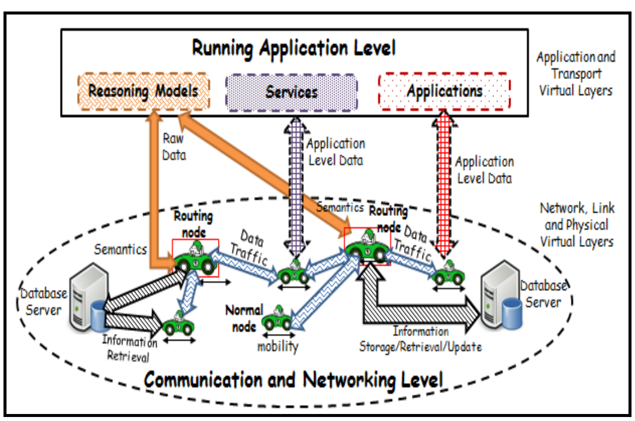

Figure 2. Opportunistic Network Architecture with Intelligence-based Routing

data patterns via adopting artificial intelligence technique-based reasoning models to reason about semantics related to behavior of normal nodes within specific opportunistic network region. Extracted semantics will give information about the amount of data sent from each available connected node with specific ID within certain time slot and located in certain areas. Routing nodes might adopt hidden Markov models (HMM) [11] for semantics reasoning as will be discussed in the next section. Routing nodes store/update semantics as accessible information at shared always-on distributed database servers. This information can be accessed by normal nodes, with host roles, at runtime to learn where and to which reliable next hop node they will foreword data packets.

IV. HMM-BASED REASONING MODEL

This section discusses the operation and technical details of a semantics reasonign model employing HMM. Reasoning processes will be implemented and executed over set of network routers, which possess powerful resource and communication capabilities. Figure 3 depicts the overall process of extracting high level information based on learning patterns of raw data and utilizing HMM-based reasoning models. Other monolithic or hybrid intelligence techniques can be used. However, we apply HMM as a case study where HMM-based reasoning models can suit characteristics of network data and some models were developed and tested for enhancing networking-based services [12].

For targeting processes shown in Figure 3, we develop Java-based software agents that run artificial intelligence techniques for learning data patterns and extracting semantics. Agents are implemented over powerful network nodes with routing roles and integrated with their operating systems. Those agents, called intelligence agents, learn patterns of data traffic generated within opportunistic environments and related to various running hosts, which are located at various areas and supporting heterogeneous applications and services. Captured raw data are represented by intelligence agents as data profiles of attribute-value pairs Intelligence agents will adopt machine learning, such as association rule learning, and Fuzzy logic for knowing data patterns and related set of data attributes. Also, HMM-based semantic reasoning algorithms are adopted for extracting high-level data

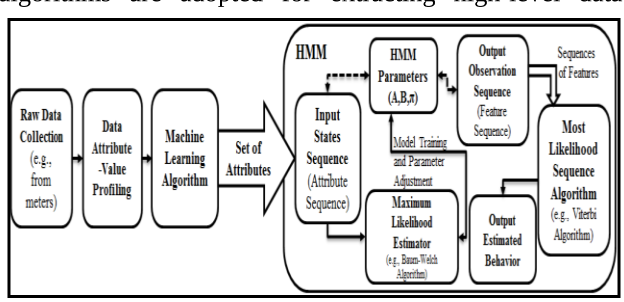

Figure 3. HMM-based Semantics Reasoning Model

features and reasoning about data semantics based on groups and sequences of known features.

For example, intelligence agents on routers can extract semantics, using HMM-based reasoning models that help router have enhanced context awareness via estimating the most reliable next hop nodes with good resource level and high probability of existence. Additionally, those agents will be able to support routers with information about behavior of surrounding hosts within a specific region during the day and predicting which hosts are speedy ones with low probability of existence. Different HMM-based reasoning models can be built and implemented over routers' agents where each model will be directed to focus on studying and estimating information related to certain operation domain (e.g., node location, speed, resource, application type, etc.). The output from those models will integrate multi-operation-domain-based features that provide highly abstracted information, which leads to having efficient decisions taken by routers. For instance, two potential next hop nodes, with common features, can be chosen by a router, however, one of them is preferred due to the total calculated weight of the combined features. In other words, set of joint interesting features might exist in two network next-hop nodes. But, one of the two nodes might have required features with maximum likelihood existence probability higher than the one of the other node.

A. HMM Overview

HMM comprises categorical sequence labeling supervised/unsupervised algorithms for estimating outputs based on sequence of hidden input words or states [11]. The estimation process for outputs relies on continuous input sequence with different Gaussian distributions. Then, HMM performs distribution mixture for obtaining the most likelihood output sequence. The input states to HMM are described as sequences. Each input state represents one learned and classified data-attribute through using machine learning mechanisms. HMM exhibits structured architectures that are able to predicting sequences of semantics based on input sequences of extracted network attributes or features. Depending on input sequences or pattern of high discriminative network-data features, HMM with forward and backward algorithms can learn semantics efficiently. HMM's statistical foundations are computationally efficient and well-suited to handle new data [13]. A single HMM can be built by combining a verity of knowledge sources [14] with the consideration of their properties. This enables an efficient design of an HMM to reason about semantics related to various network-related issues (e.g., applications and resources)

B. Example

HMM-based reasoning model might be used by the routers' intelligence agents to detect locations of high reliable nodes with powerful resources. For instance, we assume that routers within specific opportunistic networking environments are able to extract and learn identifiers of running hosts. Captured raw data by routers enable them to learn semantics that can reveal rate of data exchanged amongst set of hosts and also the time slots when those hosts exist with high probability. Reasoning processes in agents depend on learning patterns of transferred data packets that are stored as profiles of attribute-value pairs. As an example, "*average_packet_size*", "*node_ID*" and "*time_delta*" is a combined learned and classified attribute based on fields found in a stored data profile and time synchronization in all communicating nodes (i.e., it can help in measuring latency). The HMM-based model looks at the group and the sequence of data attributes within data profiles. Extracted and classified attributes form states sequence and convey to HMM parameters (A, B, π), discussed later, to generate semantics. The order of states in an input sequence might change the output observations. In other words, the existence of the same data-attributes, however, with different order might result in different outputs adopting the same HMM model. Figure 2 illustrates HMM-based model for reasoning about semantics.

According to the above discussed example for learning the more reliable next hop nodes, we assume that there are four input states to the HMM model. Those input states represent the extracted and classified data attributes according to transferred data through routers. For example, routers might know that a communicating node with a certain ID has transferred a number of large-size packets to a set of nodes located in an area within during a specific time slot. Accordingly, the input sequence to HMM-based reasoning model might have the following states: "*large_average_packet_size*", "*near_host*", "*small_scale_ network*" and "*non_speedy_hosts*". Those states are with equal initial state probability π (i.e., π =1/4) and state transition probabilities A (i.e., A_{ij} = 1/3 for i≠j and A_{ij} = 0 for i=j where A_{ij} is the transition probability form state *i* to state *j*). The estimated behavior for neighboring hosts based on the previous states sequence is "*related hosts are reliable*". To get the previous output, the observation probability B matrix, which relates each input state with that specific output, will be high. For instance, B might consist of four rows ***r*** and two columns ***c***; and it might equal ((0.2, 0.8), (0.25, 0.75), (0.15, 0.85), (0.3, 0.7)) where ***r*** represents the number of input states while ***c*** represents the number of outputs. We have two outputs in this case which are *related hosts are (i) unreliable (ii) reliable*. According to the example, all input states have high observation probability with the second output "*related hosts are reliable*". Then, this information will be maintained/updated by routers at shared accessible database. Hence, authorized communicating hosts can learn this information (e.g., IDs of reliable hosts) and they begin to forward data packets to reliable hosts. For sure, this information will be changed over time and communicating hosts have to update continuously their awareness with new available information (i.e., data routes might change over time).

V. EVALUATION

We conducted a simulation scenario, using opportunistic network environment (ONE) simulator [15], for building an opportunistic network similar to the one depicted in Figure 2. We hypothesize that our proposed intelligence-based routing approach can be applied to many routing classes working for opportunistic networks. So, we compare the QoS of running data transfer applications via four cases: i) the first two cases when adopting two routing protocols related to two difference routing scheme classes, which are flooding-based routing (epidemic protocol [5]) and prediction-based routing (prophet protocol [6]); and ii) the second cases when integrating the intelligence approach with the pervious routing schemes. We developed Java classes for building software intelligence agents over some routing nodes in the scenario. Those agents employ HMM-based models for semantics reasoning and Fuzzy membership functions (FMF) for classifying some captured attributes/features based on their values whether numeric or string values. We integrated such agent-related classes with Java classes of ONE simulator providing add-on intelligence services for semantics reasoning processes. Such services are attached to set of scenario nodes with routing roles.

The simulation scenario is as follows. Data traffic is generated among group of communicating nodes where certain routing scheme is applied. Routing nodes capture raw data from passed traffic and they learn patterns of such traffic via extracting set of data attributes, which are classified using FMF. Extracted attributes comprise node ID, packet time stamp, packet size, etc. Such set of attributes are fed to HMM-based reasoning models to generate information that are kept in a shared database that can be accessed by communicating nodes. Such information can reveal powerful nodes that are located with high probability in a certain area and they have sufficient resources. According to this information, nodes can forward data packets to those nodes. For evaluation, we target the performance metrics described in Table I where they will be measured and compared among the different adopted routing protocols. Table II shows the simulation parameters.

TABLE I. PERFROMANCE METRICS

Metric	Description
Data delivery probability	number of delivered packets to number of created packets
Communication overhead ratio	This is a measure of the number of packets that have been introduced into the network to deliver a packet from the source to its destination] it is calculated as [(number of relayed packets - number of delivered packets)/(# of delivered packets)] it refers to the number of used resources
Average network latency (sec)	the average amount of time that elapses between packet creation and its delivery to its destination
Average buffering time (sec)	the time that packets spend in the buffers of intermediate nodes
Average hop count (hop)	Average number of intermediate nodes through which data are transferred

TABLE II. SIMULATION PARAMETERS

Parameter	Value
Number of hosts (fixed)	126 hosts
Number of routers (fixed)	6 routers
Number of host clusters (fixed)	6 clusters
Number of router per cluster (fixed)	One router
Min/Max host speed	0.5/14 meter/second
Min/Max host waiting time	0/120 seconds
Transmission range	10 meters
Data transmission rate (fixed)	2 Mbps
Host buffer size (fixed)	5×10^6 bytes
Router buffer size (fixed)	50×10^6 bytes
Data message size (fixed)	500 KB and 1 MB
Data message time to live (fixed)	18000 seconds
HMM approach/number of training sequences	Unsupervised using Baum-Welch algorithm/1000 seq.
Reasoning process rate (fixed)	4 times/simulation time
Scenario area (fixed)	4500×3400 m^2
Simulation time (variable)	2500 – 7500 seconds

Figure 4 shows that data delivery probability is enhanced at using our intelligence-based approach compared with the case of no intelligence. The obtained result clarifies that more data packets are relayed and delivered to destination nodes according to the attached effective situational awareness capability to operating nodes (i.e., hosts and routers) and efficient routing decision taken by routing nodes. As appeared in Figure 5, the communication overhead is decreased when integrating intelligence with routing protocols where communicating nodes learn from shared databased the reliable next hop nodes. So, the number of data packet replica, that will be sent and relayed to reach destination hosts successfully, decreases compared with the case of operation without intelligence. Figure 6 portrays that applying intelligence over existing routing protocols does

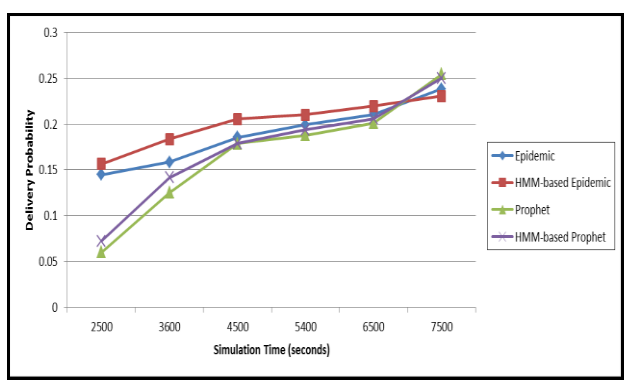

Figure 4. Data delivery probability

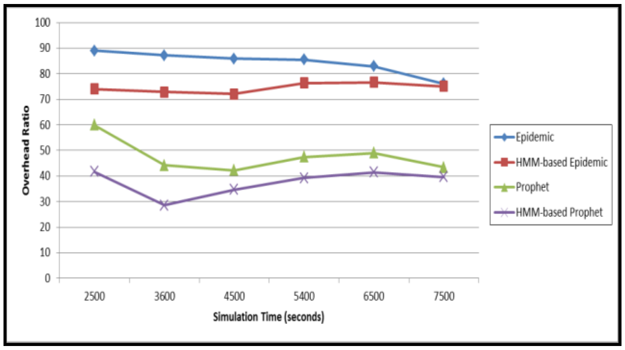

Figure 5. Communication overhead ratio

not cause much network latency compared with the operation without intelligence. There is some increase in the average buffer time of intermediate nodes in case of using intelligence as shown in Figure 7. This is because nodes which have packets to forward have chosen the most reliable nodes in the network to pass packets to them. Hence, more data packets can be sent and received successfully to intermediate and destination nodes. Figure 8 depicts the average hop count number faced at running with different routing protocols. We almost have same average hop count. This means that the implemented intelligence techniques were able to learn the most reliable locations which can support enhanced services with approximately same hop count. In other words, good level of propagation delay can be obtained.

From results, we can conclude that our intelligence-based routing approach succeeded in improving the QoS of running application compared with the case of using only epidemic and prophet routing schemes. According to these results, we have the following enhanced performance metrics:

- High data delivery ratio
- Low communication overhead ratio
- Low network latency

VI. Conclusion and Future Work

We have presented intelligence-based routing approach for the highly dynamic opportunistic networks in order to optimize QoS of running related applications. Our approach depended on developing and implementing light-weight application-level reasoning models on powerful

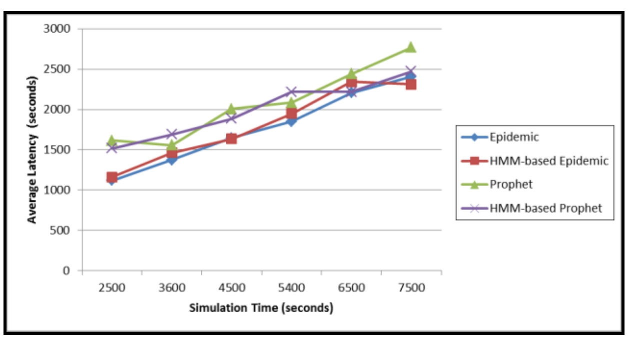

Figure 6. Average network latency

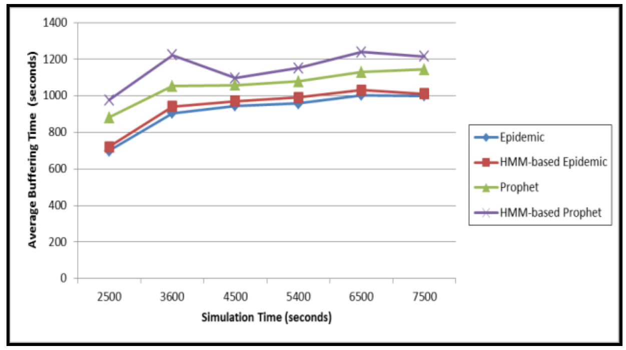

Figure 7. Average buffering time

routing nodes for learning traffic patterns and reasoning about semantics. Learned semantics are updated continuously and are maintained at accessible shared databased providing useful information for communicating nodes in sending data to the most reliable next hop nodes in specific regions. For evaluation, we integrated the proposed intelligence approach with two known flooding-based and prediction-based routing protocols, which are epidemic and prophet, respectively. Simulation results demonstrated the efficiency of adopting the proposed intelligence-based routing approach over two known routing protocols. There were enhancements in data delivery and communication overhead ratios compared with the case of operation with the two routing protocols without intelligence.

Our future work includes a) developing mathematical model for the proposed approach and its operation and complexity within opportunistic networking; b) making analytical study and validation; and c) investigating security vulnerabilities that might affect QoS of the intelligence-based routing approach. Additionally, we aim at designing hybrid intelligence techniques which suit communication and routing requirements within opportunistic networks. Also, we target more complex scenarios for validating the proposed routing approach.

Acknowledgment

This research work has been sponsored in part by the SmartCI center of research excellence, Faculty of Engineering, University of Alexandria, Egypt.

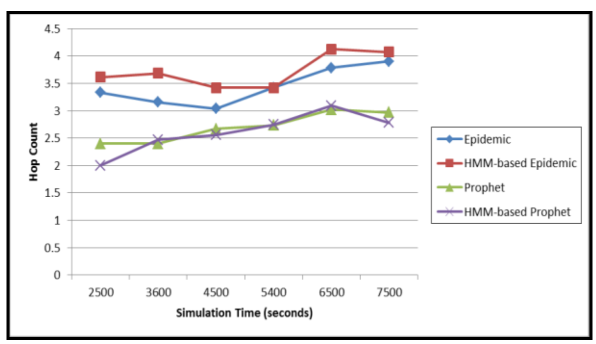

Figure 8. Average Hop Count

 ISBN: 978-1-61208-439-8

REFERENCES

[1] M. Conti, S. Giordano, M. May and A. Passarella , "From opportunistic networks to opportunistic computing," Communications Magazine, IEEE, vol. 48, 2010, pp. 126-139.

[2] C.-M. Huang, K.-C. Lan and C.-Z. Tsai, "A survey of opportunistic networks," in Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on, 2008, pp. 1672-1677.

[3] L. Pelusi, A. Passarella and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," Communications Magazine, IEEE, vol. 44, 2006, pp. 134-141.

[4] B. Poonguzharselvi and V. Vetriselvi, "Survey on routing algorithms in opportunistic networks," in *Computer Communication and Informatics (ICCCI), 2013 International Conference on*, 2013, pp. 1-5.

[5] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Technical Report CS-200006, Duke University, 2000.

[6] A. Lindgren, *et al.*, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE mobile computing and communications review,* vol. 7, 2003, pp. 19-20.

[7] T. Spyropoulos, *et al.*, "Single-copy routing in intermittently connected mobile networks," in *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, 2004, pp. 235-244.

[8] A. Verma and A. Srivastava, "Integrated routing protocol for opportunistic networks," *International Journal of Advanced Computer Science and Applications,* vol. 2, 2011, pp. 85-92.

[9] M. Musolesi and C. Mascolo, "CAR: Context-Aware Adaptive Routing for Delay-Tolerant Mobile Networks," *Mobile Computing, IEEE Transactions on,* vol. 8, 2009, pp. 246-260.

[10] R. Zhi, *et al.*, "An effective hybrid routing algorithm for opportunistic networks," in *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*, 2012, pp. 543-547.

[11] L. Rabiner and B. Juang, "An introduction to hidden Markov models," *ASSP Magazine, IEEE,* vol. 3, 1986, pp. 4-16.

[12] B. Mokhtar and M. Eltoweissy, "Hybrid Intelligence for Semantics-Enhanced Networking Operations," in *The Twenty-Seventh International Flairs Conference*, 2014, pp. 449-454.

[13] K. Seymore, *et al.*, "Learning hidden Markov model structure for information extraction," in *AAAI-99 Workshop on Machine Learning for Information Extraction*, 1999, pp. 37-42.

[14] J. Yang and Y. Xu, "Hidden markov model for gesture recognition," *Tech. Report CMU-RI-TR-94-10*,1994.

[15] A. Keränen, *et al.*, "The ONE simulator for DTN protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*, 2009, pp. 55:1 - 55:10.