ISSN 2347-4289

Efficient Routing In Delay Tolerant Network Based On Secure Fuzzy Spray Decision Algorithm

Kumar Kombaiya.A, S.Gnanasoundari

Kumar Kombaiya.A, Asst. Prof. in Computer Science, Chikkanna Govt. Arts College, Tirupur-2.
S.Gnanasoundari, Research Scholar, Dept. Of Computer Science, Chikkanna Govt. Arts College, Tirupur-2.

ABSTRACT: Delay Tolerant Networks (DTN) where the nodes in this network come into contact with each other opportunistically and communicate wirelessly and, an end-to-end path between source and destination may have never existed, and disconnection and reconnection is common in the network. In such a network, because of the nature of opportunistic network, perhaps there is no a complete path from source to destination for most of the time and even if there is a path; the path can be very unstable and may change or break quickly. Therefore, routing is one of the main challenges in this environment and, in order to make communication possible in an opportunistic network, the intermediate nodes have to play important role in the opportunistic routing protocols. In this paper we proposed an Secure Fuzzy Spray Routing Protocol in delay tolerant network (SFSR-DTN). This protocol is using the simple parameters as input parameters to find the best path to the destination node. It dynamically adjusts the delivery probability for messages according to a new metric. Meanwhile, SFRDTN arranges the forwarding sequence and the dropping priority based on their assigned weight. The weight is determined by the Replication Density (RD), the Message Length (ML), and Message Remaining Life Time (MRLT). An extensive simulation of SFRDTN was carried out and its performance was compared to well known DTN routing protocols: PRoPHET, and epidemic routing protocols. Simulation results show that the proposed routing protocol outperforms them in terms of packet delivery ratio, delivery delay and message overhead.

Keywords: Wireless sensor network, Ant colony optimization, Pheromone updating.

1 INTRODUCTION

Opportunistic network is a type of Delay Tolerant Networks (DTN) "[1, 3]" where network communication opportunities appear opportunistic, an end-to-end path between source and destination may have never existed, and disconnection and reconnection is common in the network. In the other words an opportunistic network as a subset of Delay-Tolerant Network where communication opportunities (contacts) are intermittent, so an end-to-end path between the source and the destination may never exist. The link performance in an opportunistic network is typically highly variable. Therefore, in the absence of reliable end to end connection between the source and destination node, TCP/IP protocol will not work. Opportunistic networking tries to simplify this aspect by providing several kinds of opportunistic routings. In opportunistic networks, communication devices can be carried by people, vehicles or animals, etc. Some devices can form a small mobile ad hoc network when the nodes move close to each other. But a node may frequently be isolated from other nodes. Therefore, a node is just intermittently connected to other nodes, and this partitioning is dynamically changing with time. Thus, an end-to-end connection between the source and the destination can be absent at the time the source wants to transmit, and even later. Many researchers have proposed new routing protocols such as Epidemic "[5]", Prophet "[6]", Spray-and-Wait "[7]", Spray-and-wait "[8]", Max Prop "[9]" , ORWAR "[10]", ERS "[11]", APRP "[12]", and PFBR "[13]" to handle this specific problem for DTN Recently, a new mechanism has been offered for WSNs security improvement. This mechanism relies on constructing trust systems through analysis of nodes observation about other nodes in the network. This article shows the last enhancement for WSNs by trust and reputation mechanisms found in literature. Research on the trust and reputation model is proposed for optimization in terms of security and scalability. This model is evaluated through applying security threats such as collusion and oscillating of malicious nodes in WSNs. Traditional routing protocols are not suitable for this scenario, because in those routing protocols, end-to-end connection between the source and the destination node is basic assumption. Devices in opportunistic network are enabled to interconnect by operating message in a store-carry-forward style and, each node can act as host, intermediate node, thus, it can store, carry and forward the message between for other nodes. The big challenge in opportunistic networks is how to route messages from their source to their destination, with the absence of end-to-end path. When there is no path existing between the source and the destination, nodes need to communicate with each other via opportunistic contacts through store-carry-forward operation.In this paper, a Secure Fuzzy Spray Routing Protocol (*SFSR-DTN*) for DTNs was proposed. *SFSR-DTN* cryptography enables DTN nodes to exchange their public keys or revocation status information, with authentication assurance and smartly integrates the forwarding and buffer management policies into an adaptive protocol that includes a local network parameters estimation mechanism It arranges the forwarding sequence and the dropping priority based on their assigned weight. The weight is determined by the three local parameters, namely, Replication Density (RD), Message Length (ML), and Message Remaining Life Time (MRLT). The rest of the paper is organized as follows. Section 2, gives an overview of related work. Section 3 presents proposed approach. In Section 4, deal with some topologies to validate proposed approach. Conclusion is presented in Section 5.

2 RELATED WORK

In the past few years, many routing algorithms are proposed in DTN network, such as Epidemic routing, Spray and wait, PROPHET, and so on. The basic idea of them is to increase identical copies of data into network and rely on node mobility to transmit the copies toward the destination. Obviously if there are more copies in network, the better delay performance tends to achieved in opportunistic network. But its drawback is that the traffic overhead is tremendous. If network resources are limited, replication based schemes will degrade the network performance. The

reader can find a comprehensive survey on routing protocol for DTN network. The routing in opportunistic network as mentioned before does not need to end–to-end path between the source and destination node and this fact is simplified the touting protocols in opportunistic networks; however, challenges remain that are distinct from those of conventional network routing methods. According to the classifications of routing protocols (i.e. context-oblivious, Partially Context-Aware and Fully Context-Aware) "[2]" there are some routing protocols have been proposed. In the context-oblivious, routing protocols are based on the flooding. To increase network capacity, the maximum number of repeated messages and the total number of copies of a message are limited. When nothing else is allowed to duplicate, the node should deliver the message directly to the final node. These protocols reduce the delay in getting the message, but many resources are consumed.

2.1 Epidemic Routing

Epidemic Routing is classified as replication-based routing. In Epidemic Routing, each node distributes replicated messages with no restrictions. In simple word, every node forwards their stored messages to each meeting node. Epidemic routing each node send a duplicate message with no limit so it is generate more traffic on network Epidemic Routing is the most avoidable in all DTN routings.

2.2 Spray and wait

Spray and Wait protocol work on controlled copy/Replication Schemes. There are different scheme for its protocol like Spray and wait (Snw) its advantage fewer transmission than epidemic, low contention under high traffic, scalable, Requires little knowledge about network and Disadvantage is only source node is allowed to spray copies. Thus, it incurs considerable Delay & needs to investigate the performance in realistic situation. "[4]","[14]", Binary Spray and Wait (BSW) its Advantage: Fewer transmissions than epidemic, low contention under high traffic, scalable, Requires little knowledge about network and It does blind fold forwarding (random) of message copies. It needs to investigate the performance in realistic situation." [4]","[14]" Spray and Focus has advantage are Improves the performance by twenty times than spray & wait, Disadvantage Finding optimal distribution strategy, Spray and Wait with average delivery probability, Fuzzy Spray and Wait its has own.

2.3 PROPHET

Probabilistic Routing Protocol by means of History of Encounters and Transitivity (PROPHET) establishes a summary vector that indicates what messages a node are carrying. Furthermore establishes a probabilistic metric called delivery predictability, P(a, b) (0, 1), at each node a for every known destination b. It is signify how likely it is that this node will be capable to deliver a message to that destination. The computation of the delivery predictabilities has three parts. First, whenever a node is encountered, the metric is updated as Equation. a, where P is an initialization constant.

2.4 Quality of Node

SaW and QoN routing protocols forward messages without taking node mobile patterns into concern, therefore the delivery utility is too near to the ground. To overcome above mentioned problem we consider QoN. Quality of node indicates the action of a node, or the number one node meets other different nodes within a given time interval. In the same period of time, the more nodes that one node meets, the greater the QoN. The variation of QoN can dynamically represent the node activity in a given period of time "[15]". In this paper, we use the ratio of QoNs to dynamically forward the number of message copies.

2.5 MaxProp

MaxProp is forwarding based routing protocol. In MaxProp routing each node initially set a probability of meeting to all the other nodes in network and also exchanges these values to its neighbour nodes. The probability value is used to calculate a destination path cost. Each node forwards messages through the lowest cost path. MaxProp also uses an ordered queue which is divided into two parts according to an adaptive threshold. MaxProp assigns a higher priority to new messages and forward it first with low hop count and drops a message with the highest cost path when buffer is full. MaxProp has poor performance when nodes have small buffer sizes because of the adaptive threshold calculation. Max Prop performance is better with large buffer size.

3 PROPOSED APPROACH

This protocol provides an interesting technique to control the level of flooding. The secure message is mainly delivered in two phases: the Spray phase and the Wait phase. For every message originating at the source node, L copies of the message are spread over the network by the source node and other nodes receive a copy of the message from the source node to L distinct relays. In the Wait phase if the destination was not found during the spray phase, each relay node having a copy of the message performs the direct transmission. The simulation results show that this protocol has less number of transmissions and less delivery delay as compared to the Epidemic Routing.

Spray and Wait routing consists of two phases:

i) Spray phase: In this phase, a limited number of copies (L) of messages are spread over the network by the source and some other nodes which later receives a copy of the message.

ii) Wait phase: After the spreading of all copies of the message is done and the destination is not encountered by a node with a copy of the message in the spraying phase, then each of these nodes carrying a message copy tries to deliver its own copy to destination via direct transmission independently (i.e., will forward the message only to its destination).

3.1. Secure Communication

Secure communication in a DTN requires mutual authentication between two DTN nodes before initiating a data transfer. In this section, we discuss mutual authentication between two DTN nodes and mechanisms for secure end-to-end data transfer.

3.1.1 cipher-text attribute based encryption

In ABE scheme, the encrypted creates an access tree structure T with a set of attributes and threshold gates. The access tree structure describes the access control policies that a user must satisfy to decrypt a particular message. To decrypt the message, the user must own the secret keys associated with the access tree structures over the set of attributes. These secret keys are generated by a trusted authority. In a CPABE system, each user is associated with a set of attributes. When encrypting a message M, the encryption specifies an access tree structure which is expressed in terms of a set of selected attributes for M. The message is then encrypted based on the access structure such that only those whose attributes satisfy this access structure can decrypt the message. Let us consider a sport event scenario where track teams from various schools in the tri-state area meet. CP-ABE scheme consists of four steps: Setup: This is a randomized algorithm that takes a security parameter as input, and outputs the public parameters PK and a master key MK. PK is used for encryption and MK is used to generate user secret keys and is known only to the central authority. Ken Gen: This is a randomized algorithm that takes as input the set of a user (say X)'s attributes SX, the master key MK and outputs a secret key SK that identifies with SX . Encrypt: This is a randomized algorithm that takes as input a message M, an access structure T, and the public parameter PK. It outputs the cipher text CT. Decrypt: This algorithm takes as input the cipher text CT and a secret key SK for an associated attribute set SX. Only if SX satisfies the access structure embedded in CT will it return the message M. In our construction, each leaf node of the access tree T represents either a positive or negative attribute. An example of a positive attribute is "Advisor" and an example of a negative attribute is "Not Rutgers". However, private key components are only assigned to positive attributes, i.e. for any user X, SX does not contain any negative attribute. Each internal node of the access tree T represents a threshold gate, which can be an "AND" gate or an "OR" gate. If num x is the number of children of a node, x, and kx is its threshold value, then x< Kx$\leq$k num . The parent of node x by parent(x). Let G0 be a bilinear group of prime order p, and let g be a generator of G0. In addition, let e :G0 ×G0 $\rightarrow$G1 denote the bilinear map. We further map each attribute to a unique integer in Z_p^*. using a collision hash function F: {0,1}* $\rightarrow Z_p^*$. For example, let say the attribute of a leaf node x is "Advisor", then att(x)=F('Advisor') $\in Z_p^*$. Furthermore, a function H: Zp-> G0 is used to map any attribute, x, to an element in G0 where H(i)=gi where att(x)=i. Our cryptosystem consists of the following algorithms: Setup: This algorithm chooses three random exponents $\alpha, \beta, \gamma \in Z_p$. A parameter d specifies how many attributes this system use. A polynomial v(x) of degree d is chosen at random subject to the constraint that v(0)= β. The public parameters are as follows:

$$PK = [G_0, g, h = g^{\beta}, h^{\gamma}, f = g^{1/\gamma}, e(h,g)^{\alpha}, \{g^{v(0)}..g^{v(d)} \quad (1)$$

The master key MK is $\beta, \gamma, g^{\alpha}$. Note that PK is public information shared with all users. KenGen(MK,S) This algorithm takes as input a set of attributes S and outputs a secret key that identifies with S. The algorithm first chooses a random $r \in Z_p$ and then random $r_j \in Z_p$ for each attribute $j \in Z_p$. Then, it computes the secret key SK as

$$SK = \left[D = g^{(\alpha+r)/\gamma}, D_1 = g^r \forall j \in S, D1_j = h^r.H(j)^{r_j}, D2_j = g^{r_j}, D3_j = (V(j))^r\right] \quad (2)$$

Delegate (SK, $\bar{S}$) The delegation algorithm takes in a secret key SK which is for a set S of attributes, and another set $\bar{S}$, such that $\bar{S} \in S$. The algorithm chooses random $\bar{r}$ and $\bar{r}_k \forall k \in \bar{S}$. Then, it creates a new secret key as

$$\overline{SK} = \left[\bar{D} = D.f^{\bar{r}}, \overline{D1} = g^r.g^{\bar{r}}, \forall k \in S, \overline{D1}_k = \overline{D1}_k.h^{\bar{r}}.H(k)^{\bar{r}_k}, \overline{D2}_k = \overline{D2}_k.g^{r_k}, \overline{D3}_k = \overline{D3}_k\left(V(k)\right)^{\bar{r}}\right] \quad (3)$$

Encryption (PK, M, T) The encryption algorithm encrypts a message M under the tree access structure T. As in the basic scheme, this algorithm first chooses a polynomial qx (with degree dx=kx-1) for each node x (including the leaves) in the tree T. For example, at the root node R of the access tree, the algorithm chooses a random $s \in Z_p$, and sets qR(0)=s. Then, it chooses dR other points of the polynomial qR randomly to define it completely. Let Y1 and Y2 be the set of the leaf nodes in T with positive and negative attributes, respectively. For each node $y \in Y2$, we randomly choose uy from Zp. Recalls that the function F maps each attribute into an element in Z_p^* . A function $v(i): Z_p \rightarrow G_0$ is defined as $V(i) = g^{v(i)}$. Then, the cipher text CT is constructed as follows:

$$CT = [T, c1 = Me(h,g)^{\alpha s}, C2 = (h^{\gamma})^s \quad (4)$$

$$\forall \text{nodes } y \in Y1: C1_y = g^{q_y(0)}, C2_y = H(i)^{q_y(0)} \quad (5)$$

Where $i = F(att(y))$, and

$$\forall\, nodes\ y \in Y2: C3_y = h^{q_y(0)+\mu_y}, C4_y = (V(i))^{\mu_y}, C5_y = g^{\mu_y} \quad (6)$$

Decrypt(CT,SK): First, we define a recursive algorithm Decrypt Node(CT,SK,x) that takes as input a cipher text CT, a secret key SK, which is associated with a set of attributes S, and a node x from the access tree T. If the node x is a leaf node, then we let i=att(x). If x corresponds to a positive attribute, and $i \in S$, then

$$\text{DecryptNode}(CT, SK, x) = \frac{e(D1_i, C1_x}{e(D2_i, C2_x} \quad (7)$$

$$= \frac{e(h^r.H(i)^{r_i}, g^{q_x(0)}}{e(g^{r_i}.H(i)^{g_{x(0)}}} \quad (8)$$

$$\frac{e(h^r, g^{q_x(0)}.e(H(i)^{r_i}.g^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \quad (9)$$

$$= e\left(h^r, g^{q_{x(0)}}\right) = e(h,g)^{rq_x(0)} \quad (10)$$

If x corresponds to a positive attribute, and iÏS , then we define DecryptNode(CT,SK,x)=$\perp$ which means that node x is not satisfied by S. On the other hand, if node x corresponds to a negative attribute and i=att(x) $\notin$ S , then we say that node x is satisfied by S. If x corresponds to a negative attribute, and i$\in$ S , then we define DecryptNode(CT,SK,x)= $\perp$. When a leaf node x is satisfied by S, then DecryptNode(CT,SK,x)= $e(h,g)^{rq_x(0)}$. Next, we can recursively compute DecryptNode(CT,SK,x) when x is a non-leaf node. For all nodes c that are children of x, we compute DecryptNode(CT,SK,c) and store the output in Lc. Let Ux be an arbitrary kx sized set of child nodes such that Lc is not an empty set. If no such set exists, then the node x was not satisfied by S and DecryptNode(CT,SK,x)= $\perp$. Otherwise, we can verify that DecryptNode(CT,SK,x)= (0) (,)rqx e h g . Thus, the decryption algorithm begins by simply calling the function on the root node R of the access tree T. If the tree is satisfied by S, then we set A=DecryptNode(CT,SK,R)= $e(h,g)^{rq_R(0)} = e(h,g)^{rs}$. Then, the decryption algorithm can decrypt the cipher text by computing

$$\frac{C1}{\frac{e(C2,D)}{A}} = \frac{C1}{\frac{e\left(h^{\gamma s}, g^{\frac{\alpha+r}{\gamma}}\right)}{e(h,g)^{\gamma s}}} \quad (11)$$

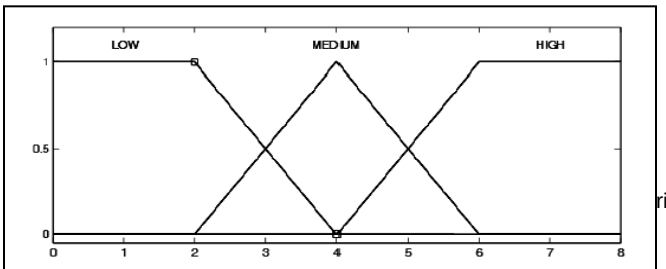
$$= \frac{Me(h,g)^{rs}}{e(h,g)^{rs}} = M \quad (12)$$

Since the CP-ABE solution can be expensive in terms of computations, our security solution combines the symmetric key solution with our enhanced CP-ABE solution. In our security solution, each data publisher encrypts his data items using symmetric keys. The symmetric keys are then encrypted using our enhanced CP-ABE scheme such that only authorized personnel can decrypt these messages to retrieve the symmetric keys, and then use these symmetric keys to decrypt the encrypted data items.

3.2. Fuzzy spray based Routing Protocol

3.2.1 Probability of Delivery

In Fuzzy-Spray protocol, Forward Transmission Count or FTC was proposed in order to prioritize messages in buffer of nodes. In SFSR used the same concept to calculate the copies of message in the network. This parameter is increased when the nodes exchanges their messages so it is approximately show the number of message transmission in the network. The value of MTC is as same as FPD but the membership function had been defined again and it is depicted in Fig.1.



3.2.2 Energy Value

Since that most nodes of the mobile network nodes or devices have limited buffer size and the size of message is very important so we considered it as input parameters as same as Fuzzy Spray Protocol but there is some deference in the member ship function which is defined as Fig.2.

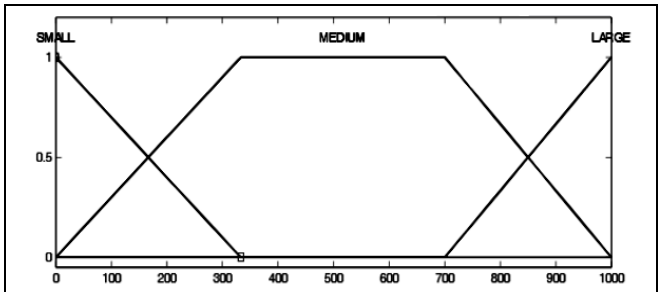


Fig. 2. Memberships function of energy value.

Fig.2: Memberships function of energy value

3.2.3 Time to Live

In fact the TTL time is very important in routing protocol. When messages are not delivered in their TTL, the drop ration of message will be increased and the total performance of proto9cl will be decreased. TTL is considered in our protocol in order to increasing the ratio of message delivery which is not considered in Fuzzy-Spray protocol. The membership functions for TTL is depicted in Fig. 3

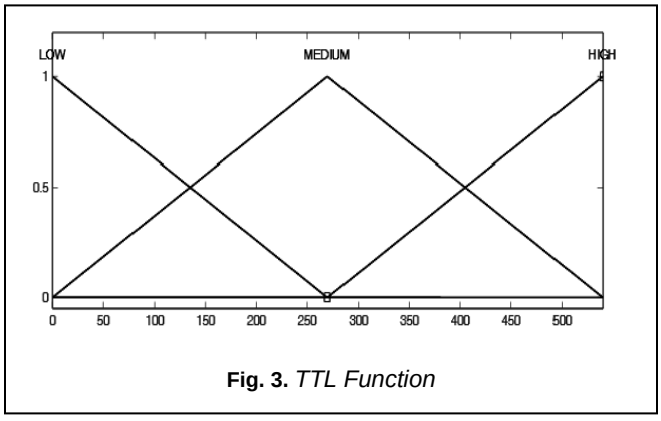


Fig. 3. *TTL Function*

3.3 Buffer Sections

According to the input, SFSR protocol will be divide the buffer of nodes into 19 sections and according to the input the message will be select the appropriate section. This partitioning finally will be used to prioritize the message in order to exchange it in next contact. The priority of

message will be calculated as bellow: Priority_of_Message=1-BS_of_Message.Error! Reference source not found. shoes the membership function of BS

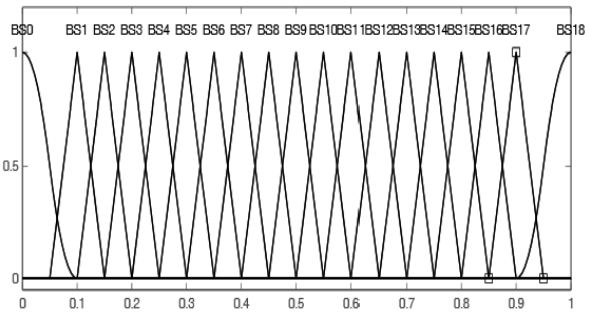


Fig. 4. TTL buffer section

Fig.4 TTL Membership Function

4 Experimental Results

There scenarios are defined in order to compare the message delivery ratio and buffer consumption of *SFSR* protocols with the other same protocols such as Fuzzy-Spray, Spray and Wait and Epidemic. The simulation time was set to one week and the expiry time for the bundles was set to 1430 minutes. The number of nodes was 100, and a total of 17000 bundles were sent. In this set up, the buffer space was limited to 10MB per node and the available bandwidth was 100 kbit/s. limited resources (buffer and band- width) *SFSR* (The proposed routing) performed better performance than PRoPHET and Epidemic Routing in this scenario in terms of delivery rate and overhead ratio. The fact that the proposed routing outperformed PRoPHET and Epidemic Routing shows that the protocol makes wise decisions on what bundles to forward and how to use the limited resources.

5 Performance Comparison

PDR is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%). This parameter is also called "success rate of the protocols", and is described as follows:

$$\text{PDR} = ((\text{Send Packet no})/(\text{Receive packet no})) \times 100$$

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

$$X = C/T$$

Where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Average end-to-end delay Average end-to-end delay signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

$$D_{end-end} = N(d_{trans} + d_{prop} + d_{proc}$$

Where delay end-end= end-to-end delay, dtrans= transmission delay, dprop= propagation delay,dproc= processing delay,dqueue= Queuing delay and N= number of links.

TABLE 1 Packet Delivery Ratio

Protocols	Buffer size				
	2	4	6	8	10
Epidemic	0.34	0.43	0.5	0.6	0.73
PRoPHET	0.43	0.45	0.58	0.73	0.79
Spray And Wait	0.51	0.57	0.61	0.85	0.84
Proposed SFSR	0.64	0.7	0.84	0.95	1.0

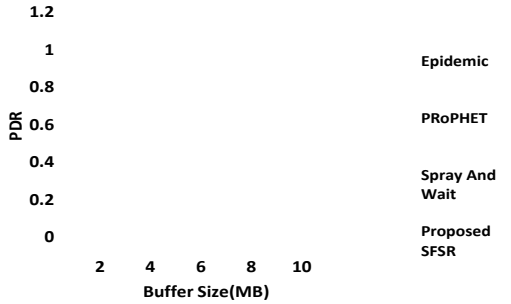


Fig. 5. Comparison of different protocol vs Packet delivery ratio

Fig .5 shows packet delivery ratio against Buffer size. It shows that the Proposed SFSR protocol has a better throughput in the different size of buffer.

TABLE 2: Average Latency

Protocols	Buffer size				
	2	4	6	8	10
Epidemic	4673	4765	5873	6894	8435
PRoPHET	3745	3646	4638	5873	7874
Spray And Wait	2547	2896	3689	4876	6474
Proposed SFSR	1457	2643	3457	4328	5757

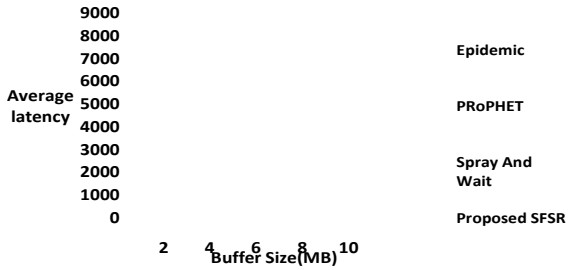


Fig. 6. Average latency as function of buffer size

Fig 6 shows the average delay of a message as the buffer size varies. Similar to the delivery ratio, the result shows that the performance of *SFSR* is better than those of PRoPHET, and Epidemic.

TABLE 3: OVERHEAD RATIO

Protocols	Buffer size				
	2	4	6	8	10
Epidemic	77	66	55	52	48
PRoPHET	68	61	48	45	41
Spray And Wait	59	52	43	39	36
Proposed SFSR	51	46	38	35	31

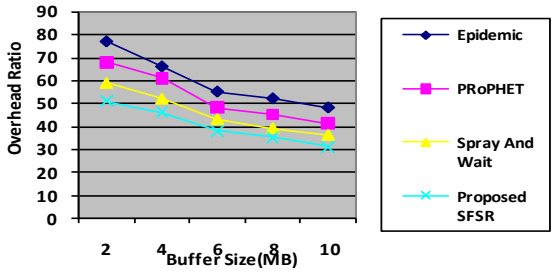


Fig 7: Overhead ratio as function of buffer size

Fig. 7 *SFSRs ss*as the simulation results indicate, the copies of each messsage are much less than PRoPHET and Epidemic Routing protocols.

6 CONCLUSION AND FUTURE WORK

This paper has presented a new method to dynamically select the forwarding list according to the situation. This mechanism to select the relaying node from the available node list is supported by a fuzzy logic system which takes into account the bandwidth, energy of the node, priority of the message and the density of the network. By means of fuzzy logic, the effectiveness of SFSR protocol is able to reduce the energy consumption per transmission and also could use less resource. As future work, we intend to implement the protocol in a network simulation where realistic propagation conditions and realistic battery performance are taken into account.

REFERENCES

[1] Delay Tolerant Networking Research Group. http://www.dtnrg.org.

[2] Conti, M., Crowcroft, J., Giordano, S., Hui, P., Nguyen, H.A., & Passarella, A.(2008). Minema. Hugo Miranda, Luis Rodrigues,Benoit Garbinato (Ed.), “Routing issues in Opportunistic Networks”. Springer.

[3] Mamoun H. M., “Efficient Routing Scheme for Opportunistic Networks ”, International Journal of Engineering and Technology, Vol. 2, No 6, pp. 940-945, June 2012.

[4] Hemal Shah, Yogeshwar P. Kosta, “Exploiting Wireless Networks, through creation of Opportunity Network – Wireless-Mobile-Adhoc-Network (W-MAN) Scheme”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Volume.2, No.1, March 2011,99-110.

[5] A. Vahdat and D. Becker, “Epidemic routing for partially connected ad hoc networks”, Tech. Rep. CS-2000-06, CS Dept., Duke University, April 2000.

[6] Lindgren et al, “Probabilistic Routing in Intermittently Connected Networks”, Mobile Comp. and Comm. Rev, vol. 7, no. 3, pp. 19- 20, July 2003.

[7] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Spray and wait: Efficient routing in intermittently connected mobile networks”, In Proceedings of ACMSIGCOMM workshop on Delay Tolerant Networking (WDTN’5), pp 252-259, 2005.

[8] J. Burgess, B. Gallagher, D. Jensen and B. N. Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks," Proceedings of 25th IEEE International Conference on Computer Communications, Barcelona, 23-29 April 2006, pp. 1-11. doi:10.1109/INFOCOM.2006. 228

[9] J. LeBrun, C.-N. Chuah, D. Ghosal, and M. Zhang, “Knowledgebased opportunistic forwarding in vehicular wireless ad hoc networks,” In IEEE Vehicular Technology Conference(VTC), pp. 2289–2293, May 2005.

[10] J. Leguay, T. Friedman, V. Conan, "DTN Routing in a Mobility Pattern Space", presented at ACM SIGCOMM Workshop on Delay Tolerant Networking, 2005

[11] Hui, P. and Crowcroft, J. (2007) “Bubble rap: forwarding in small world dtns in every decreasing circles”, Technical report, Technical Report UCAM-CL-TR684. Cambridge, UK: University of Cambridge.

[12] Boldrini, C., Conti, M., Jacopini, I., & Passarella, A.(2007, June). “HiBOp: A History Based Routing

Protocol for Opportunistic Networks". Paper presented in the Proceedings of the WoWMoM 2007, Helsinki.

[13] Hemal Shah and Yogeshwar. P. Kosta , "Routing Enhancement Specific to Mobile Environment Using DTN", International Journal of Computer Theory and Engineering, Vol. 3, No. 4, August 2011

[14] T. Spyropoulos K. Psounis, C. S. Raghavendra "Efficient routing in intermittently connected mobile networks" The multiple copy case IEEE\ACM Trans. on Networking, Volume. 16, 2008.

[15] Wang, Guizhu, Bingting Wang, and Yongzhi Gao. "Dynamic spray and wait routing algorithm with quality of node in delay tolerant network."Communications and Mobile Computing (CMC), International Conference on. Volume. 3. IEEE, 2010.