ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.2, Pages : 07-12 (2016)
Special Issue of ICCECT 2016 - Held at The Savera, Chenna, India
http://www.warse.org/IJETER/static/pdf/Issue/iccect2016sp02.pdf

Co-operative Adaptation Strategy To Progress Data Transfer In Opportunistic Network

G. Stephanie Vianna[1], S. Neelavathy Pari[2]
[1]Student, MIT, Anna University, India, stephyg1992@gmail.com
[2]Assistant Professor, MIT, Anna University, India, neela_pari@yahoo.com

***Abstract*— Mobile nodes in the wireless network aid in fast and efficient data transfer among the nodes. In MANET, a complete route establishment is done between the sender and receiver, before the commencement of message transfer. On the contrary, Opportunistic Network starts the packet transfer as soon as the message is ready and finds the next hop node that could reach the destination. Hence the nodes may or may not get the opportunity to do the transmission. This remains the greatest disadvantage in OppNet. Another challenge that exists, is the process of finding the next hop node, excluding selfish and malicious node and to deliver the message to the destination. This could be resolved by implementing a self-adaptation strategy where nodes make self-analysis using Prisoner's Dilemma (PD), a non-zero game in Game Theory. Each node selects its own strategy and does data transmission. Depending on the behaviour of nodes, they receive payoffs. Similarly each node makes a self-estimation of their performance and compares with other nodes in the network. As a result, nodes can make a change of strategy in order to improve their performance. By iterating this process, non-cooperative nodes can be made to cooperate. This will in turn improve the message delivery probability of the overall system. Simulation results show that the delivery ratio of the message has been improved to 40 percent, when the nodes make self-adaptation strategy. These highly cooperating nodes can help to make efficient recommendations of useful information as per user's interests.**

Keywords*— *opportunistic network; cooperation; Prisoner's Dilemma; delivery probability

INTRODUCTION

Wireless networking is the process of communication among the nodes without any wired media. The nodes remain scattered and blind about the location of its neighboring nodes. Since the network is without any infra-structure, it faces huge threats and is highly vulnerable to the outside world, may be attackers or intruders. There are various wireless networks in existence namely, Mobile Adhoc Network (MANET), Vehicular Adhoc Network (VANET), Wireless Sensor Network (WSN). These traditional networks have the need for the end nodes to be in communication path. The sender and receiver node pairs could be able to reach them. But the path to reach them may not be known in advance. In that case, the sender node sends route request to all the near-by nodes. The nodes that have the path information to reach the destination will send the route reply in the reverse direction or keeps forwarding the request. Thus it makes a dynamic route discovery and establishment.

Opportunistic Network (OppNet) comes into play if both sender and receiver cannot establish a route for data transmission. Mobile or fixed nodes are involved in the data transmission. OppNet has its applications in opportunistic computing, recommender system data offloading etc [20]. The nodes can cover a range of about 100-300 meters. Each node does the function of node discovery and next-hop message exchange. The message routing happens in the form of "store-carry-and-forward" (SCF) strategy and routed in opportunistic fashion. This SCF strategy [11] has a better performance than the traditional direct communication link. This method also saves the energy consumption for about 30 times greater than the traditional method. In case of delay tolerant network, SCF can save 70% of energy consumption [16] when implemented in cellular network. It also exhibits load balancing [12], when a hot cell can't handle the traffic and the traffic gets shared by other less or free cells. They make communication even if there doesn't exists a route between them [14].

There is no need for the nodes to possess information about the network topology. If no path appears, the data is buffered and carried along till the nodes come in contact. Thus, contacts between nodes are viewed as an opportunity to move data closer to the destination. The process of data dissemination can take place in numerous methodologies [2] [3], [20], [21], [15]. Routing [14] data packets also remains a greater challenge in opportunistic network along with other challenges [19]. This is because of the absence of knowledge about the network topology. This will in turn have an impact on the performance of the network. Hence, there exists a trade-off between the performance and the topology knowledge. The routing algorithms can be characterized as direct, flooding based, prediction based, coding based and context based.

A. Need for cooperation in OppNet

Cooperation among nodes plays a vital role in all wireless mobile networks [6] so as in opportunistic network too. There is a greater need for nodes to cooperate because exercising cooperation can result in spectral efficiency and SNR gain [17]. This cooperation also influences the delivery probability in the network. If there is no cooperation among nodes in the network, then there is high possibility of packet dropping. The nodes can even behave malicious and may result in data modifications. These selfish nodes influenced the performance of routing [17], [18], [14].

B. Strategies in Game Theory

Game Theory has a greater application in understanding numerous complex real world scenarios. They contain many tools and insights in solving problems in any discipline. It has its application in psychology, political science, computer science, astronomy etc. There exists many strategies in Game Theory namely cooperative or non-cooperative, symmetric or asymmetric, zero game or non-zero game, simultaneous or sequential etc. Prisoner's Dilemma is a non-zero game that can find optimal solution in the dilemma faced. Maintaining a less memory of the previous happenings in PD is recommended for its efficient functioning. The Tit-for-Tat (TFT) strategy is the traditional one that has knowledge about the opponent's last move. It can also be done with a zero memory or with a forgettable memory called Tit-for-Tat – with forgiveness (TFT-WF) after a fixed interval. But TFT outperforms TFT-WF.

The major significance of the paper is summarized as (1) Cooperation among nodes is highly important in OppNet to maintain an appreciable delivery ratio. The first step is to organize a static environment of different classes of nodes in the network environment. (2) Later SAS is used to induce cooperation among nodes in the same network environment. This will be performed in dynamic case where nodes have to do self-estimation group wise.

The paper is organized as follows; Section II describes the related work in broader context. Section III gives the proposed system with its flow diagram. Section IV details the SAS with PD explanations. It specifies the behavior of various nodes and their dynamic adaptation strategy process in theoretical manner. Section V gives the simulation design with detailed explanation of 3 cases. The paper is concluded in Section VI followed by references.

RELATED WORK

A. Node classification

In order to make nodes cooperate in data transfer, *Misra et al* has proposed a new mechanism Distributed Information – based Cooperation Ushering Scheme (DISCUSS) in [5]. DISCUSS is done by the inspiration of the Evolutionary theory. In this theory, the players change their strategy in order to survive in the game by making self-estimation and comparison with the other strategy. The nodes are made into 3 groups namely Co-operators (C), Exploiter (E) and Isolators (I). The opportunistic network is said to be Strategy Defined-Opportunistic Mobile Network (SD-OMN), if the nodes follow a strategy with a set consisting of {C, I, E}. This strategy can change to promote data delivery ratio. It includes two phases that are repeated for every generation interval (t). They are Acquiring information and Strategy adaptation phases. For every generation interval, the nodes calculate the delivery probability, DP. If finds the maximum of Weighted Average Delivery Probability (WADP) to be lesser than DP, then change the group. By this way the number of C nodes will increase in the network and increase the overall message delivery ratio.

In order to investigate the cooperativeness among the nodes *Sujata et al* has evaluated the RCP methodology in [22]. The nodes in the network are classified into co-operators, exploiters and isolators. The nodes were allowed to take up their strategy. With these nodes set in the network, the message delivery ratio is analysed. There has been an increase in the delivery ratio to about 20-35% when the nodes behave cooperative. It has been found that the exploiters were found to do best, whereas on the whole co-operators were found to outperform and make other nodes to change their strategy.

B. Improve cooperation

Source nodes send packet to destination with the help of relay nodes. These relay nodes must do its transmission correctly. Hence an optimal relay mechanism HERA [8] has been proposed. For the usage of relay nodes, a payment mechanism is used. HERA is composed of three components: 1) an optimal relay assignment algorithm, 2) a payment mechanism for source nodes, and 3) a payment mechanism for relay nodes. HERA is a centralized approach where the system administrator collects and maintains the payment to relay nodes. A Strictly Dominant Equilibrium Strategy is used such that selfish nodes make maximum utility of relay nodes. VCG payment method is used to check the payments made for the service by the source node. This prevents the relay node from lying and gaining profit. A relay node can be connected to many source nodes. Hence optimal relay assignment algorithm is used to find the best relay node. The system has higher capacity if a relay node is connected to many source nodes; secondly no source node must be left without assignment to relay node.

To improve the cooperation among nodes, *Levente et al* used Nash Equilibrium Strategy in [1]. They have developed a game theory that stimulated cooperation among nodes and thereby discouraging selfish nodes. This on the whole increased the message delivery rate. Consider when a person wants to download some interesting thing from others he does that and benefits from it. He remains selfish and don't save and distribute it for the benefits of others. If this prevails, the QoS will decrease accordingly. The proposed mechanism includes that, when a user downloads a message he is prompted to give a message in return. In this each node has a list of messages that they need to forward. This list is forwarded to other node. If a node U finds the needed message.

Nodes that don't cooperate in data transmission is one that is said to misbehave. Those nodes may be malicious or selfish nodes. Malicious nodes are those that intentionally don't behave normally in order to cause damage in the system. Selfish nodes are those that misbehave for its own benefit. Both this behaviour will affect the performance of the system. A probabilistic misbehaviour detection system, iTrust [10] has been proposed by *Zhu et al*. Trusted Authority (TA) helps in checking the behaviour of nodes periodically. iTrust has two phases, including routing evidence generation phase and routing evidence auditing phase. The number of nodes affects the number of contact history in a particular time. When there is large number of nodes, then the malicious nodes can be identified correctly and misidentified rate is also less. Whereas when the nodes are in lesser no, the probability of finding malicious nodes is less and a larger percentage of misidentifying happens. The nodes mobility (speed) has no effect in the system.

Dynamic trust management protocol [7] is designed for secure routing in the presence of malicious and selfish nodes by *Chen et al*. A malicious node can cause attacks like self-promoting, bad- mouthing and ballot attacks. The attack can be random or collaborative attacks. The trust value is evaluated by both direct and indirect trusts. The proposed work considers trust composition, trust aggregation, trust formation and application level trust optimization. Consider healthiness, unselfishness and energy to find out selfish and malicious nodes in the network. These metrics are used to find the trust values in both direct and indirect observations.

A node can behave selfish in two ways: social and individual selfishness. *Li et al* [4] has taken two relaying schemes namely two-hop relaying and epidemic relaying. The impact of this selfish nodes is studied and performance is analysed with the message transmission delay and transmission cost. Continuous Markov chain is used for modelling the message passing process. Two-hop relaying is one where the source node and send the message to any other nodes, the relay node can forward to multicast destinations and the destination can never forward the message. In epidemic routing, the message can be forwarded to all neighbours but the destination cannot forward the message to any node. The messages are simply flooded to other nodes. Two states are taken when considering Markov chain model. They are transient state and absorbing state. In transient states, the nodes are forwarded and reaches the absorbing state. The result found is the selfish behaviour influences the epidemic relaying than two-hop relaying.

C. Self-adaptation strategy

Dayong et al [9] has given a self-adaptation strategy employed by players in game. In this, players are assumed to be nodes in the network. They are made to cooperate by making a self-estimation and comparing the payoffs received by them and other nodes. Evaluation is done with four types of games namely simultaneous, strictly alternative, randomly alternative and random games. A player can take either of two options namely cooperate or defect. It follows the knowledge possessed by the players.

PROPOSED SYSTEM

Nodes can be generally classified as cooperative and non-cooperative nodes. These two types make a greater impact on the network performance. Cooperative nodes always exercise complete cooperation during the data transmission. Whereas among the non-cooperative nodes, some may exhibit selfish behavior and others may do malicious activities. These selfish nodes in order to save their time, energy or other resources, may use other nodes for transmitting their data packets. Those nodes that use other cooperative nodes as free-riders are called exploiters. Some nodes that never get into the process of data forwarding, instead receive the packet by checking the destination address are called isolators. If the destination address on the data packet matches with its own address, it receives the packet; otherwise drops the packet.

A. System Model

Based on forwarding or dropping of messages by nodes, the nodes can be classified as co-operators C, exploiters E and isolators I. The network performance is measured by varying the number of C, E and I nodes in the network. The impact of such behaviors is analyzed by the performance of message delivery using synthetic and real-life traces. The simulation results confirm the formation of a Rock- Scissors-Paper (RSP) cycle [23]. The System is analyzed as static and dynamic scenarios. In static case, the number of C, E and I nodes remains same. Each node remains in their own strategy as chosen by them. In dynamic case, the number of C, I and E nodes will keep changing. This is achieved using Self-Adaptation Strategy (SAS). The flow diagram of SAS is given in Fig 1

B. Self- Adaptation Strategy (SAS)

Cooperation among nodes is significant in opportunistic mobile network. In order to improve cooperation in the network, we propose a self- adaptation strategy as in Table 1. This works with the local information available with the nodes. This strategy aims in maximizing the overall network performance especially on the message delivery ratio. It is the ratio of number of messages created to the number of messages delivered by a node. Each and every node makes their own choice of strategy among two groups namely cooperative G_c and non-cooperative G_{nc} groups. They also calculate their performance that is obtained as a result of the strategy selected. Each node does this self-analysis and may or may not change their strategy based on the comparison. If finds their performance to be less than the other groups strategy, they may change their strategy in order to gain greater rewards. By iterating the process among all nodes in the network, even the non-cooperative nodes can be made to cooperate. This is to motivate the available exploiter and isolator nodes to change into cooperative nodes.

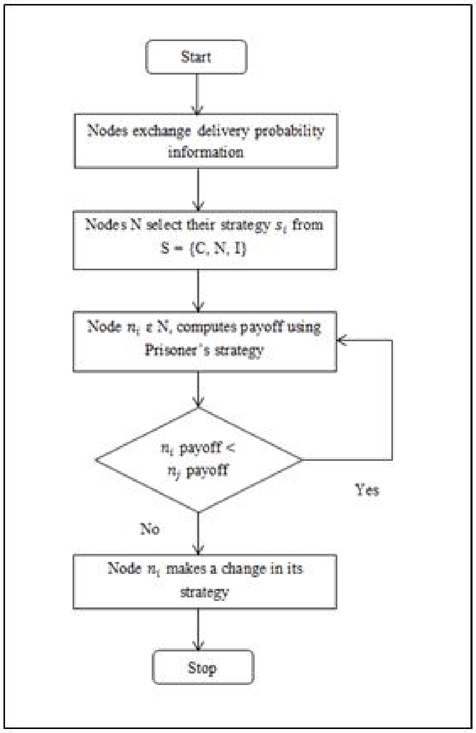
Start
Nodes exchange delivery probability information
Nodes N select their strategy s_i from S = {C, N, I}
Node n_i ε N, computes payoff using Prisoner's strategy
n_i payoff < n_j payoff
Yes
No
Node n_i makes a change in its strategy
Stop

Fig 1: Self-Adaptation Strategy

C. Mathematical Model

Analysis done using mathematical and computational modelling is highly beneficial in finding out the complete and complex working in the system. Here the nodes can make up their actions or strategies in the network. For each strategy made, they gain corresponding payoffs as mentioned in the payoff matrix in Table 2. This matrix is given on the basis of Prisoner's Dilemma (PD), a Game Theory strategy to decide on various critical situations where dilemma exists.

Table 1: Self – adaptation strategy

Algorithm : SAS (Node n_i, Strategy s_i)	
Input	Node, Set of Strategy {C, E, I}
Output	Strategy change to increase cooperation

```
   /* Payoffs given to each node are
   T- temptation, S-sucker, P-punishment, R-
reward*/
   payoff =0; // for new node initially
       do{
           for each player $n_i$ in the network {
             select a strategy $s_i$
             keeps data transmission with its
               neighbors $n_j$
             compares strategy and gets the payoff
               (T/R/P/S)
           }
       }// goes till the simulation
```

The dilemma that prevails in our network is like nodes will exhibit cooperation or not. PD can handle large number of nodes [24] in iterative fashion using Iterative Prisoner's Dilemma (IPD). Various environments are analysed with IPD concept in [23].

D. Prisoner's Dilemma

Prisoner's Dilemma is a classic non-zero game in Game Theory. The game is played in terms of suspects. In this, both of the prisoners who have been arrested are given a bargain. The prisoners get rewards (imprisonment) with respect to their replies to the investigation. Each prisoner aims to minimize the number of years spend in prison. The game is as follows: If both prisoners confess, they are given a reward, R. If they both lie, they are given a reward (punishment), P. If one confesses and the other lies, then the person who confessed will be given a reward (sucker payoff), S; and the other is given a reward (temptation payoff), T. The inequality to be followed are, T>R>P>S and 2R>T+S.

The basic two behaviors are cooperation and non-cooperation, which can be mapped to cooperate and defect respectively. The two groups that can be formed are G_c and G_{nc}. The cooperators, C fall under G_c; then exploiters, E and isolators, I are placed in G_{nc}. All nodes in the group G_c

exhibit pure cooperation in data transmission; whereas the nodes in the group G_{nc} may or may not cooperate.

Table 2: Payoff Matrix

	Confess C	**Defect D**
Confess C	R,R	S,T
Defect D	T,S	P,P

R – Reward, P – Punishment, S – Sucker, T – Temptation

The cases that can be examined are pure cooperate in G_c and 3 different behaviors in group G_{nc}. They may be pure cooperation, pure defect and partial cooperation and defection. Suppose the game iterates for 5 times and payoff value be T=5, R=1, P=3, S=0.

Case 1: Pure Cooperation Vs Pure Cooperation
Player 1: CCCCC
Player 2: CCCCC

The payoff obtained by the player, P1 from G_c is 5 years and the player, P2 belonging to G_{nc} also obtains 5 years. Neither of the two players has lost, because both are given the minimum number of years for imprisonment say 1 year.

Case 2: Pure Cooperation Vs Pure Defection
Player 1: CCCCC
Player 2: DDDDD

In this case, the payoff obtained by both players P1 and P2 are 0 and 25 years. Here the nodes in the group G_c are benefited irrespective of the behaviour of nodes in opposite group G_{nc}.

Case 3: Pure Cooperation Vs Cooperation and Defection
Player 1: CCCCC
Player 2: CDCDC

In this scenario, player 1 gives pure cooperation whereas player 2 may exercise both cooperation and defection. Hence the number of years sentenced for imprisonment is 3 and 13 respectively. The co-operator nodes have gained their payoff when compared to the exploiter and isolator nodes.

SIMULATION DESIGN

This section gives an overview of the simulation setup. The SAS was implemented in ONE simulator [13]. The nodes are grouped and each group shares some common parameters like message buffer size, radio range and mobility model. Since different groups can have different configurations simulation with pedestrians, cars and public transportation are possible. Epidemic routing was used for simulation. This chapter gives the results obtained from the implemented code. It is obvious that the system implemented has outperformed and has given a high delivery probability.

Table 3: Common parameters considered during simulation

Parameters	Value
Simulation Time	600 s
Interfaces	Bluetooth, High speed interface
Routing	Epidemic Oracle Router
Message size	500KB-1MB
Buffer size	5MB
Node movement speed	2-5
Message TTL	300 min

The above general settings have been set for the executed of the ONE simulator. The work has been tested with 50 mobile nodes in the simulated area. Data packets are forwarded among nodes and reach the destination when they come into the range. Varying number of co-operators are set and delivery probability of different values are obtained. It is done with three cases and comparison of all three is plotted in a graph. The static case is plotted in Fig.2 where there are 75%, 20% and 5% of I, E, C nodes respectively which yields 0.06 delivery ratio. The second bar set has 60%, 20% and 30% of I, E, C nodes respectively with 0.065 delivery ratio. Final bar set consists of 26%, 26% and 48% of I, E and C nodes respectively with 0.0741

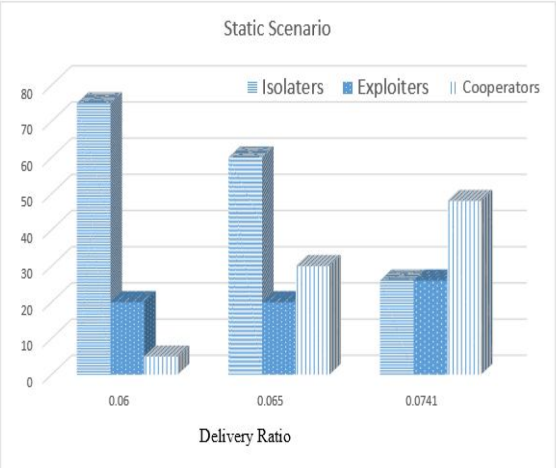

Fig 2: Delivery Ratio for Static Scenario

With the same scenario the dynamic case has been measured and the graph is given in Fig. 3. The first bar set gives 0.49 as delivery ratio with 75%, 20% and 5% of I, E, C nodes respectively. The second set gives 0.97 delivery ratio with 60%, 20% and 30% of I, E, C nodes respectively. The final set has 26%, 26% and 48% of I, E and C nodes respectively and gives the delivery ratio of

1.56 The graph shows that the presence of greater number of co-operator nodes in the network has improved the message delivery ratio in both cases. Similarly the delivery ratio in static scenario is found to be less by 40% than the dynamic case, this is because the nodes in the latter case have incorporated the dynamic SAS methodology.

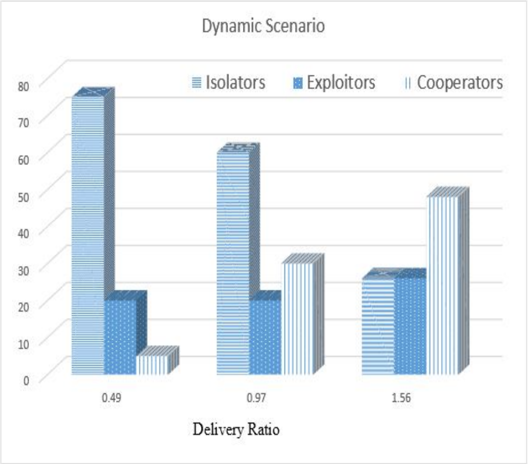

Fig 3: Delivery Ratio for Dynamic Scenario

CONCLUSION

In conclusion, a self-cooperative system has been designed to promote data transmission in an Opportunistic network. Among the three classes of nodes namely cooperates(C), exploiters (E) and isolators (I) various behaviors are addressed. The evaluation of the performance is done in two cases. One with the static number of C, E and I nodes. In the dynamic environment, the Prisoner's Dilemma strategy is used. Here nodes make a self-estimation among themselves and change their strategy. This finally makes the non-cooperating nodes in the network to become cooperative. With this working, the performance regarding the delivery probability has been evaluated and analyzed. The result and analysis showed that, the dynamic case implemented using the Prisoner's Dilemma Strategy has given 40% of increase in delivery ratio than the static case.

REFERENCES

[1] Levente Buttyán, László Dóra, Márk Félegyházi, István Vajda,"Barter trade improves message delivery in opportunistic networks", Elsevier Ad Hoc Networks 8, 2010

[2] Radu-Ioan Ciobanu, Radu-Corneliu Marin, Ciprian Dobre, Valentin Cristea, "Interest-awareness in data dissemination for opportunistic Networks", Elsevier, August 2014

[3] Radu I. Ciobanu, Ciprian Dobre, "Data Dissemination in Opportunistic Networks", February 2012

[4]Yong Li, Guolong Su, Dapeng Oliver Wu, Depeng Jin, Li Su, and Lieguang Zeng, "The Impact of Node Selfishness on Multicasting in Delay Tolerant Networks", IEEE Transactions On Vehicular Technology, Vol.60, No.5, June 2011

[5] Sudip Misra, Sujata Pal, and Barun Kumar Saha, "Distributed Information-Based Cooperative Strategy Adaptation in Opportunistic Mobile Networks", IEEE Transactions On Parallel And Distributed Systems, Vol.26, No.3, March 2015

[6] Khajonpong Akkarajitsakul, "Cooperative Packet Delivery in Hybrid Wireless Mobile Networks: A Coalitional Game Approach", IEEE Transactions On Mobile Computing, Vol. 12, No. 5, May 2013

[7] Ing-Ray Chan, F.Bao, M.J.Chang, J-H Cho, "Dynamic Trust Management for Delay Tolerant Netoworks and Its Application to Secure Routing" , IEEE Transcations On Parralel And Distributed Systems, Vol.25, No.5, May 2014

[8] Dejun Yang, Xi Fang, Guoliang Xue, "HERA: An Optimal Relay Assignment Scheme for Cooperative Networks", IEEE Journal On Selected Areas In Communications, Vol.30, No.2, February 2012

[9] Dayong Ye and Minjie Zhang, "A Self-Adaptive Strategy for Evolution of Cooperation in Distributed Networks", IEEE Transactions On Computers, VOL. 64, NO. 4, APRIL 2015

[10] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, and Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions On Parallel And Distributed Systems, Vol.25, No.1, January 2014

[11] Panayiotis Kolios, Vasilis Friderikos, Katerina Papadaki, "Store Carry and Forward Relay aided Cellular Networks"

[12] Panayiotis Kolios, Vasilis Friderikos, Katerina Papadaki, "Load Balancing via Store-Carry and Forward Relaying in Cellular Networks"

[13] A. Keranen, J. Ott, and T. Karkkainen, "The ONE simulator for DTN protocol evaluation," in Proc. 2nd Int. Conf. SIMUTools, 2009, pp. 55:1–55:10.

[14] Nessrine Chakchouk, "A Survey on Opportunistic Routing in Wireless Communication Networks", IEEE Communications Surveys & Tutorials,2015

[15] Luciana Pelusi, Andrea Passarella, and Marco Conti, "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks", IEEE Communications Magazine, 2006

[16] Panayiotis Kolios, Vasilis Friderikos, and Katerina Papadaki, "Energy-Efficient Revlaying via Store-Carry and Forward within the Cell", IEEE Transactions On Mobile Computing, Vol. 13, January 2014

[17] J.S. Chen J.X. Wang, "Cooperative transmission in wireless networks using incremental opportunistic relaying strategy", The Institution of Engineering and Technology, Vol. 3, March 2009

[18] Yong Li, Pan Hui, Depeng Jin, Li Su, and Lieguang Zeng, "Evaluating the Impact of Social Selfishness on the Epidemic Routing in Delay Tolerant Networks", IEEE Communications Letters, Vol. 14, November 2010

[19] Leszek Lilien, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta, "Opportunistic Networks: The Concept And Research Challenges In Privacy And Security"

[20] Guo Da, Cheng Gang, Zhang Yong, Song Mei, Amanda Metthews, "Data Distribution Mechanism over Opportunistic Networks with Limited Epidemic", China Communications, June 2015

[21] Thrasyvoulos, Konstantinos Psounis, Cauligi S. Raghavendra, "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks"

[22] Sujata Pal, Sudip Misra, Barun Kumar Saha, "Rock-Scissors-Paper Cycle of Cooperation Strategies in Opportunistic Mobile Networks", IEEE International Conference on Communications 2013

[23] Richard Brunauer, Andreas Locker, Helmut A. Mayer , "Evolution of Iterated Prisoner's Dilemma Strategies with Different History Lengths in Static and Cultural Environments", ACM, March 2007

[24] Miklos N. Szilagyi, "An Investigation of N-person Prisoners' Dilemmas", Complex Systems Publications, Inc., 2003