ICWMC 2020

The Sixteenth International Conference on Wireless and Mobile Communications

ISBN: 978-1-61208-794-8

October 18 – 22, 2020

ICWMC 2020 Editors

Dragana Krstic, Faculty of Electronic Engineering, University of Nis, Serbia
Cosmin Dini, IARIA, USA/EU

ICWMC 2020

Foreword

The Sixteenth International Conference on Wireless and Mobile Communications (ICWMC 2020), held between October 18–22, 2020, followed on the previous events on advanced wireless technologies, wireless networking, and wireless applications.

ICWMC 2020 addressed wireless related topics concerning integration of latest technological advances to realize mobile and ubiquitous service environments for advanced applications and services in wireless networks. Mobility and wireless, special services and lessons learnt from particular deployment complemented the traditional wireless topics.

We take here the opportunity to warmly thank all the members of the ICWMC 2020 Technical Program Committee, as well as the numerous reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to ICWMC 2020. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the ICWMC 2020 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that ICWMC 2020 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the area of wireless and mobile communications.

ICWMC 2020 Chairs

ICWMC Steering Committee

Dragana Krstic, University of Niš, Serbia
Magnus Jonsson, Halmstad University, Sweden
Rajat Kumar Kochhar, Ericsson, Sweden

ICWMC 2020 Publicity Chair

Jose M. Jimenez, Universitat Politecnica de Valencia, Spain
Jose Luis García, Universitat Politecnica de Valencia, Spain

ICWMC 2020 Industry/Research Advisory Committee

Sivakumar Sivaramakrishnan, vToggle Ltd., New Zealand
Christian Makaya, IBM T.J. Watson Research Center, USA

David Navarro, Ecole Centrale de Lyon, France
Carl James Debono, University of Malta, Malta

ICWMC 2020

Committee

ICWMC 2020 Steering Committee

Magnus Jonsson, Halmstad University, Sweden
Dragana Krstic, University of Niš, Serbia
Rajat Kumar Kochhar, Ericsson, Sweden

ICWMC 2020 Publicity Chair

Jose M. Jimenez, Universitat Politecnica de Valencia, Spain
Jose Luis García, Universitat Politecnica de Valencia, Spain

ICWMC 2020 Industry/Research Advisory Committee

Sivakumar Sivaramakrishnan, vToggle Ltd., New Zealand
Christian Makaya, IBM T.J. Watson Research Center, USA
David Navarro, Ecole Centrale de Lyon, France
Carl James Debono, University of Malta, Malta

ICWMC 2020 Technical Program Committee

Afrand Agah, West Chester University of Pennsylvania, USA
Ali Kadhum M. Al-Quraby, University of Babylon, Iraq
Diego Alberto Godoy, Universidad Gastón Dachary, Argentina
Adel Aldalbahi, King Faisal University, Saudi Arabia
Rashid Ali, Sejong University, Seoul, Republic of Korea
Karine Amis, IMT Atlantique, France
Tran Hai Anh, Hanoi University of Science and Technology (HUST), Vietnam
Antonio Arena, University of Pisa, Italy
Kamran Arshad, Ajman University, UAE
Radu Arsinte, Technical University of Cluj-Napoca, Romania
Corey E. Baker, University of Kentucky, USA
Hadda Ben Elhadj, SM@RTS | Higher Institute of Informatics | Monastir University, Tunisia
Driss Benhaddou, University of Houston, USA
Vincent Beroulle, Grenoble INP, France
Robert Bestak, Czech Technical University in Prague, Czech Republic
Christos Bouras, University of Patras, Greece
Brik Bouziane, Eurecom School, France
Maurizio Bozzi, University of Pavia, Italy
An Braeken, Vrije Universiteit Brussel, Belgium
Ibtissem Brahmi, University of Sfax, Tunisia
Rodrigo Campos Bortoletto, Federal Institute of Education, Science and Technology of São Paulo - IFSP,

Brazil
Eric Castelli, CNRS / Laboratoire LIG, Grenoble, France
Riccardo Colella, National Research Council of Italy, Italy
Estefania Coronado Calero, Fondazione Bruno Kessler, Trento, Italy
Nicolae Crisan, Technical University of Cluj-Napoca, Romania
Enrico Del Re, University of Florence and CNIT, Italy
Sandesh Dhawaskar Sathyanarayana, University of Colorado Boulder, USA
Ding-Zhu Du, The University of Texas at Dallas, USA
Rishabh Dudheria, New York Institute of Technology - Nanjing campus, China
Faten Fakhfakh, National School of Engineering of Sfax, Tunisia
Souhir Feki, University of Carthage, Tunisia
Miguel Franklin de Castro, Federal University of Ceará, Brazil
Marco Furini, University of Modena and Reggio Emilia, Italy
Krishna C. Garikipati, Niantic Inc., USA
Jordi Garcia, CRAAX Lab - UPC BarcelonaTech, Spain
Carlo Giannelli, University of Ferrara, Italy
Xiang Gui, Massey University, New Zealand
Abdelaziz Hamdi, ISITCOM | University of Sousse, Tunisia
Wibowo Hardjawana, University of Sydney, Australia
Ali Kadhum Idrees, University of Babylon, Iraq
Terje Jensen, Telenor, Norway
Magnus Jonsson, Halmstad University, Sweden
Georgios Kambourakis, University of the Aegean, Greece
Madhan Raj Kanagarathinam, Samsung R&D Institute, India
Lutful Karim, Seneca College of Applied Arts and Technology, Toronto / Moncton University, Canada
Suleman Khan, Northumbria University, Newcastle, UK
Wooseong Kim, Gachon University, S. Korea
Rajat Kochhar, Ericsson, Sweden
Peng-Yong Kong, Khalifa University, United Arab Emirates
Dragana Krstic, University of Niš, Serbia
Vimal Kumar, University of Waikato, New Zealand
Mohamed Lamine Lamali, Univ. Bordeaux | LaBRI, France
Mohamed Latrach, ESEO / IETR - University of Rennes 1, France
Deyu Lin, Nanchang University, China
Eirini Liotou, National and Kapodistrian University of Athens, Greece
Jia Liu, Dalian University of Technology, China
Jian Liu, University of Tennessee, Knoxville, USA
Mohamed M. A. Moustafa, Egyptian Russian University, Egypt
Stephane Maag, Institut Mines Telecom / Telecom SudParis, France
Amel Meddeb Makhlouf, NTS'COM (New Technologies for System Communications) | ENET'COM (High School of Engineering in Electronics and Communications), Tunisia
D. Manivannan, University of Kentucky, USA
Hend Marouane, Sfax University, Tunisia
Aref Meddeb, University of Sousse, Tunisia
Hamid Menouar, Qatar Mobility Innovations Center (QMIC), Qatar
Sofien Mhatli, ISI Kef | University of Jandouba, Tunisia
Fabien Mieyeville, University of Lyon | Université Claude Bernard Lyon 1 | CNRS, France
Makoto Miyake, M-TEC Co. Ltd. | Mitsubishi Electric Corporation, Japan

Table of Contents

On Mass-Spring System Implementation in Cluster-Based MANETs for Natural Disaster Applications

Francisco E. Balart-Sanchez
Electronics Systems & Informatics Dept.
ITESO-Jesuit University of Guadalajara
Tlaquepaque, Mexico
email:franciscobalart@iteso.mx

Luis F. Gutierrez-Preciado
Electronics Systems & Informatics Dept.
ITESO-Jesuit University of Guadalajara
Tlaquepaque, Mexico
email:lgutierrez@iteso.mx

Francisco Cervantes-Alvarez
Electronics Systems & Informatics Dept.
ITESO-Jesuit University of Guadalajara
Tlaquepaque, Mexico
email:fcervantes@iteso.mx

***Abstract*—Communication after natural disasters is paramount. Disasters such as earthquakes, hurricanes and tsunamis leave the affected area reachable only to wireless devices. In such conditions, Mobile Ad-hoc Networks (MANETs) play a critical role. The issue of MANETs communication backbone can be addressed by self-organized cluster-based algorithms. The virtual backbone will maintain an efficient communication on the MANET, adapting to the dynamic topology changes thanks to its self-organized nature. Nevertheless, they do not take into account the node's mobility. If a node moves away from its neighboring nodes, connectivity will be lost and thus, network segmentation will occur. Therefore, it is fundamental to maintain the connectivity and the communication between nodes while exploring the area. In this paper, we propose the application of a mass-spring system on the Energy-Efficient Self-Organized Algorithm (EESOA) for Disaster Area applications. Results will show that our proposal performs best when deployment of MANET's nodes is dense while maintaining a connected network.**

Keywords–MANETs; self-organization; cluster-based algorithms; Mass-Spring; Disaster Area.

I. Introduction

Almost every year natural disasters such as earthquakes, hurricanes, typhoon, flood and tsunamis strike many areas of the world. After the catastrophic events, many lives are trapped in the post-disaster area. According to the "Golden 72 hours" principle, people that are trapped have a large chance of survival if they are rescued within the initial 72 hours [1]. Emergency response teams and volunteers need to communicate in order to perform their rescue operations. Thus, the connectivity of their communication devices is paramount in such situations. Nevertheless, communication systems which provide connectivity are usually down as a result of the disaster. The advance of mobile ad hoc networks (MANETs) has enabled their usage to address disaster situations thanks to the availability and infrastructure-less nature.

A Mobile Ad-hoc Network node, consists of an wireless electronic device, such as laptops, drones, smartphones and wearable technology which communicates among each other in a decentralized manner creating a structure-less network. Research in MANETs has intensified given the usage scenarios unveiled by catastrophic disasters on which device reachability is key. The advantage of wireless MANETs nodes over wired devices have yielded a new range of applications to aid on response of catastrophic disasters. Applications range from prior alert mechanism and post disaster infrastructure [2], provide a secure payment system in disaster areas [3], Simultaneous Wireless Information and Power Transmission (SWIPT) scheme [4], hybrid communication infrastructure systems using wireless devices and the remaining cellular antennas [5]. Other applications focus on post-disaster communication like human mobility based communication system [6], an earthquake communication platforms [7] or Unmanned Aerial Vehicles (UAVs) network deployment [8].

The aforementioned applications [2]–[8] assume the network is always connected and does not take into account the dynamic topology changes of the MANET. Such topology changes can be caused by node's mobility, obstacles causing connectivity loss, node's death, malfunction and node battery drain out. Additionally, another assumption is that MANET's nodes will always be within range, and thus, connected. There must be a mobility scheme, which prevents the nodes to go far from their neighbors causing network segmentation. Such mechanism, at the same time, must prevent the nodes to be too close to each other as well.

The contribution of this paper and ongoing research [9] is the evaluation of the application of a mass-spring system on a cluster-based algorithm for disaster area applications. Implementation of mass-spring on the MANET's nodes will control the node's mobility to have a connectivity-aware network. Simulation will show that the proposed approach performs best when deployment of the MANET's nodes is dense without losing connectivity. There are several applications of the mass-spring system: An indoor positioning and tracking localization scheme [10]; smart cities applications [11]; a positioning scheme when the number of anchor nodes is insufficient [12]; a study on implementing a mass-spring based algorithm for the optimal topology on a wireless network [13]; an anchor free Wireless Sensor Network (WSN) self-localization scheme [14]; a relaxation of the model for devices' self-deployment [15] and WSN localization [16].

The rest of this paper is organized as follows: Section II shows the related work. Section III presents the application of the mass-spring system on a cluster-based algorithm. Section IV establishes the testbed simulation. Section V shows the simulation results. Finally Section VI concludes this work and presents future challenges.

II. Related Work

The research surveyed in this section [5]–[7] [17] addresses the challenge of MANET's communication in disastrous areas.

A. Decentralized Algorithm for Maximizing Coverage and Lifetime in a Mobile WSN

Etancelin et al. [17] proposed a decentralized algorithm for maximizing coverage and lifetime in mobile wireless sensor networks (DACYCLEM). Their approach is to build

 ISBN: 978-1-61208-794-8

a connected dominating set (CDS) combined with a attraction and repulsion forces scheme to maintain connectivity. Thus, the problem addressed is to maximize the lifetime of a network while attempting to cover the maximum possible area. The solution offered by Etancelin et al. [17] is based on define coverage area as an objective and connectivity as a constraint. Their proposal is to combine the solution for each sub-problem addressed. For the backbone construction sub-problem, they used the approach proposed in [18]. For the connectivity between nodes sub-problem, in Table 1 of [18] they defined either the *attractive, repulsive* or *equilibrium* forces based on the nodes' states and their interaction. The separation of *critical backbone* and *backbone* is key for the behavior on the nodes forces interaction. Additionally, nodes' states are defined as active or standby, which will also affect the respective force defined at Table 1 of [18]. Finally DACYCLEM's algorithm 1([18]), was proposed with an initialization deployment phase. This proposal addresses the aforementioned sub-problems while maintaining connectivity as a constraint.

Although DACYCLEM shows promise, it does not consider the implications of "graceful degradation" defined in [19]. Also the battery consumption due to changing the node's state from standby to active does not seem to be taken into account. Another assumption is the nodes deployment distribution. For the purposes of their research, a random distribution of the nodes in the area is assumed. This is not realistic for disaster applications. Finally another caveat is that nodes will only start initialization once they reach a predefined meeting point.

B. MANET rescue information communication system

Verma et al. [5] presented a hybrid cellular-MANET architecture communication system. The proposal does not require modifying existing wireless infrastructure nor requires new technology but existing devices with Wireless Fidelity (Wi-Fi). The architecture consists of a sink node named *Control Station* (CS), which is connected to a vehicular *Base Station* (BS) in order to have internet and cellular service. Two *Access Point* (AP) types are defined based on the communication interface, Wi-Fi AP and Gateway AP (which uses cellular interface). Victim's devices are defined as *Mobile Devices* and *Notebooks*. The aforementioned architecture assumed the existence of a working BS, nevertheless, the architecture is robust enough to take into account broken BS causing no cellular coverage.

An energy and mobility aware, self organized routing protocol is proposed as well. APs are dropped and then register to the CS to keep their table updated. Once registered APs starts broadcasting to detect devices. Mobile devices respond to the broadcast message or use neighbor MANET nodes as relay nodes. Subscription is performed using unique physical address and a sequence number to avoid loops and old messages. The routing is defined by two processes: the *route discovery and message transmission* and the *route maintenance*. The route discovery scheme falls within the on-demand (reactive) type. The devices always will subscribe to the AP with minimum hop count. Route maintenance focuses on network topology changes. If a new node appears or an existing one moves the APs and CS will update their tables.

The limitations with this approach are, although it builds a MANET there is a sink node (CS). To have a sink node causes traffic to be higher in gateways nodes or rely nodes causing the *hotspot* problem, causing such nodes to drain their battery. The use of two technologies provides robustness but the switch between Wi-Fi and cellular schemes cases additional power consumption. This proposal assumes the network will always be connected, when mobility of rescuers, does not follow any scheme to ensure an connected network.

C. MANET-based communication platform

Jang et al. [7] outlined a MANET-based communication platform and information rescue system. It proposed to establish a temporary MANET by using WiFi-ready devices such as notebook PCs for the network construction. Thus, the architecture is not limited by the technology available post-disaster. Authors in [7] presented an "Autonomous P2P Ad-Hoc Group Communication Systems" (*P2Pnet*) as a serverless peer-to-peer communication MANET-base network. On top of the MANET, there is a peer-to-peer communication layer to support higher level communication services such as Push-to-Talk, two way radio and VoIP communications. The proposal in [7] assumed that there would be nodes with satellite communication capability such as mobile-base stations and Very Small Aperture Terminal (VSAT). The aforementioned nodes will perform gateway functions so all other nodes can access Internet through gateways.

Once the network is built, [7] introduced "Rescue Information System for Earthquake Disasters" (RISED). RISED main objective is to provide the most up-to-date rescue-related information. Such system is designed to support efficiently resource and information management for rescue mission operations in a catastrophic disaster. RISED is composed by 4 subsystems. The Disaster Assessment, fastest rescue route generation, health care & relief resources integration and wounded victim arrangement subsystems focus on specific task relying on the constructed MANET-based network. Authors in [7] assumes volunteers will be within range without any defined approach to ensure a connected network.

D. Unmanned Aerial Vehicle network deployment tool

Deruyck et al. [8] proposed a deployment tool for UAV-aided emergency network for large scaled disaster scenarios. Such UAVs will have a mounted base station which can be a femtocell base station. The deployment tool takes as input the following: human traffic and locations, disaster area 3D model environment and number of hours the communication service is required. With the 3D model path loss calculation is performed being either Line-Of-Sight (LOS) or Non-Line-of-Sight (nLOS). With the aforementioned the algorithm creates a list of all possible base stations. When all user locations are analyzed the network is then designed. The number of nodes calculated on the algorithm takes into account the number of drones in the facility. Once the UAV is on its dedicated position, the user will be able to connect to the BS. This approach generates a connected network thanks to the number of nodes calculated, still a scheme to maintain nodes within range and avoid collision among each other is not addressed.

E. Human mobility in disaster areas

Aschenbruck et al. [6], provided a realistic approach to model the mobility in a disaster area. Not only takes into account natural disasters, but human-caused disasters as well. Nevertheless, it has many assumptions such as relying on the civil protection "*separation of the room*" disaster tactics, which is unrealistic since the post-disaster terrain area could be inhospitable and unreachable. Their model does not simulate obstacles, a key factor in MANETs which causes changes on the MANET's topology. The metrics used, such as *relative mobility*, *average node degree*, *average link duration*, *minimum number of links node and its neighbors* (*mincut*) part from the assumption of a non dynamic topology network.

Relying on structured civil protection tactics assumptions provides an model which does not take into account the dynamic nature of MANETs. [6] assumptions does not take into account obstacles or MANET's nodes power making the model prone to network segmentation due to the lack of self-organization. Finally, the mobility distribution may follow the civil protection tactics, nevertheless in reality this can change drastically due to the terrain conditions. Mobility model is rigid, limited by the aforementioned civil protection tactics moreover, no approach is mentioned to avoid network segmentation when nodes are not within communication range.

III. Mass Spring Model On EESOA

From the surveyed work in section II ([5]–[7]), it can be concluded that the assumption of a connected network was made. A scheme that controls the MANET's nodes mobility to keep them within communication range, and consequently, maintain a connected network is not defined. Only [17] defines a mobility model since it defines connectivity as a constraint. Our proposal is the continuation of an ongoing research [9]. The problem of back-bone construction is already addressed by EESOA. Nevertheless, EESOA with the mass-spring model shows promise as a proposal for a connected-aware network. The novelty of this proposal is the combination of a mass-spring model with ESSOA. This provides a MANET with a virtual-backbone maintained by nodes that will have a mobility model which will maintain them connected and prevent collision. Finally leveraging from EESOA hello broadcast, nodes will share their position to neighbors within one hop. This will enable all MANETs nodes to compute all their neighbors mass spring force in a distributed manner. Interaction of mass-spring model with EESOA is described in section III-C.

The findings presented in this work are focused on the mass spring system combined with a cluster-based system in terms of number of survivors found and coverage area. Thus, EESOA [9] virtual-backbone algorithm is agnostic to removal of nodes in the network causing changes in the topology. Finally, pairing EESOA nodes with the mass-spring system, the network connectivity will be preserved in order to assist on search and rescue operations.

A. *EESOA for virtual backbone & efficient communication*

The Energy-Efficient Self-Organized algorithm, builds and maintains a virtual-backbone in a distributed manner. ESSOA constructs the virtual backbone through a 4-hierarchy cluster-based formation. Such roles are: Leader, Gateway, Bridge and Member. Each EESOA node will self-assign one of the 4 hierarchies role based on the information obtained from its neighbors within one-hop. The node with more neighbors and best quality criteria defined in [20] will have the Leader role. Leader will inhibit its neighbors with periodic broadcast messages. A Gateway node is an EESOA node inhibited by two or more nodes with the Leader role. A Bridge node is an inhibited node which have an inhibited neighbor from another cluster. A Member node is an EESOA node inhibited by a single leader. The hierarchy roles self-designation scheme is defined in detail in [20]. The algorithm used in the presented work is the result of an ongoing research, proposed at [9]. The proposal is an enhancement on the Bridges role-self-assignation that removes redundant links and minimizes broadcast messages and packet loss. The EESOA proposal is explained in detail in [9].

EESOA clustering [9] is shown in Figure 1. Without EESOA, communication between a node and all its neighbors will occur. Having no control on redundant links will cause unnecessary communication and problems such as broadcast storm. Therefore, the EESOA clustering will remove redundant links (non-backbone) and will construct a virtual backbone as shown in Figure 1. Thus, avoiding problems such as broadcast flooding and packet loss due to excessive redundant links.

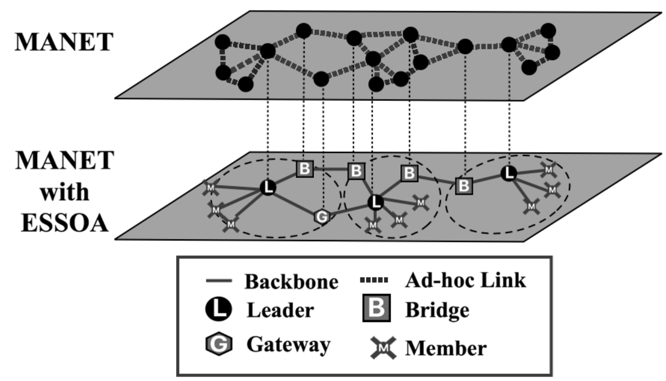


Figure 1. EESOA virtual backbone.

B. *The Mass Spring Model*

Node management such as maintaining a distance to avoid disconnection or preventing collision with neighboring nodes is not addressed on the surveyed work [5]–[7]. Maintaining connectivity within the network for search and rescue is paramount. The problem of construction and maintenance of a communication backbone is already addressed by EESOA. Nevertheless, EESOA provides a virtual back bone but does not avoid network segmentation. The problem of node management, such as keeping the nodes from going too far from their neighbors' range causing network segmentation and preventing nodes from being too close to each other, can be addressed by applying the mass-spring model to EESOA.

Application of mass-spring model in a MANET can give a connectivity awareness to the network and thus, address the problem of maintaining the nodes within range.

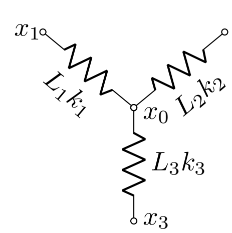


Figure 2. Mass-spring system with 3 elements

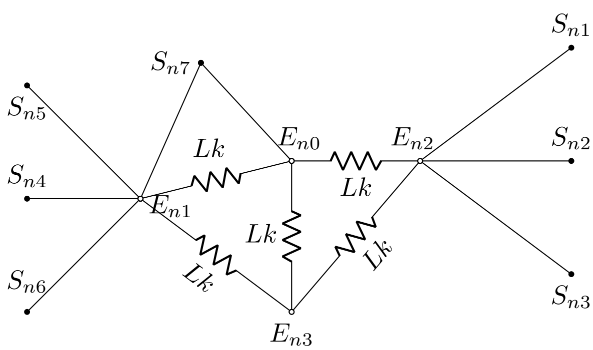
The mass-spring system maintains a minimum distance between the components of the system thanks to constant L. Also, will keep the node as close as possible to the point of equilibrium in which the sum of the forces is 0, otherwise, resultant force will move the node of position. Hence, the aim is to provide a flexible scheme which when combined with EESOA takes connectivity into account. An example of the aforementioned mass-spring system is shown in Figure 2.

Equation (1) describes the mass-spring systems with the force behavior affected by current positions (x), equilibrium distance (L) and the spring constant (k).

$$F_u = \sum_i \left[k_i(|x_i - x_u| - L_i)\frac{x_i - x_u}{|x_i - x_u|} \right], \quad i \neq u \qquad (1)$$

where:
x_i Position of the i^{th} node
x_u Position of $node\ u$
L_i Equilibrium distance for i^{th} node
k_i Spring constant for i^{th} node

Each ESSOA-MANET node will generate a mass-spring model with all its neighbors within one-hop. Depending on the neighbor node role given by EESOA [9], the constant k_i and equilibrium distance L_i will be defined accordingly.



k: EESOA mass-spring constants
o: EESOA nodes (E_{ni})
•: Survivor Nodes (S_{ni})

Figure 3. Mass-spring model between nodes

C. Mass-spring interaction with EESOA

The mass-spring application on EESOA consists on 2 parts. On first stage the EESOA node will generate the respective k spring constant as shown in Figure 2. Such constant will be role dependant. Further more the equilibrium distance L will be role dependant as well, making the mass spring model flexible. An example of an EESOA-based MANET with the mass-spring model is denoted in Figure 3.

On the second stage, the algorithm will iterate through all the nodes and their mass spring models. Then, it will generate a vector $\vec{v}$ which will determine the new position (x, y) of the EESOA node. Note that the algorithm will take into account the mass-spring model of its EESOA neighbor nodes to keep the equilibrium in the system as shown in Figure 3. Thus, the new position will be adjusted. Therefore, the node will not move away to cause network segmentation. Additionally, the new position will cause the neighbor nodes to adjust their vectors and new positions to maintain the equilibrium. Thus, the implementation of the mass-spring model on EESOA nodes provides a MANET, that addresses connectivity, which is key for disaster area search and rescue applications.

The aforementioned stages are represented in Algorithm 1. The First stage is denoted in Step 8, where if there is a EESOA neighbor $N(u)$ for a node *u*, it will generate the appropriate spring constant k_i according to the EESOA neighbor node. Subsequently it will compute the individual force generated between node *u* and it neighbor *v* while maintaining the minimum equilibrium range *L* defined on (1). The second stage in denoted no the loop in step 7 and the update on node *u* position in step 12. The resultant force of Neighbors of node u will denote vector $\vec{v}$ to update the node's position.

The mass spring algorithm will be performed on each *hello broadcast*, thus, being always updated with the position of Neighbors of node *u*. Additionally, it will take into account dynamic changes on the MANET topology, which will cause EESOA node role changes and thus, will update the spring constant k_i as well as the Force $F_{i,v}$. Here we can observe the interaction between the mass spring model and the EESOA algorithm. EESOA provides a back bone and the mass spring model provides connectivity awareness, both critical applications for search and rescue on disaster areas.

Algorithm 1 Mass-Spring Algorithm

1: $N(u) = Neighbors\ nodes\ within\ 1 - hop\ of\ node\ u$
2: $k_{u,v} = Spring\ constant\ between\ node\ u\ and\ v$
3: $F_{u,v} = Force\ between\ node\ u\ and\ v$
4: $F_T = Total\ Force$
5: **function** FIND_EQUILIBRIUM
6: $F_T := 0$
7: **for** All N(u) **do**
8: $\quad Neighbor\ Spring\ k_{u,v} \leftarrow GetSpring(u, v)$
9: $\quad Neighbor\ Force\ F_{u,v} \leftarrow GetForce(k_{u,v})$
10: $\quad F_T := F_T + Fu, v$
11: **end for**
12: $UpdateNodePosition(u, F_T)$
13: **end function**

IV. SIMULATION

In this section, we performed simulations to observe the behavior of the mass-spring model implementation on EESOA. Performance assessment will be conducted in terms of initial and final number of survivors found and coverage area.

A. Mass-spring model on EESOA on Java Simulator

A discrete-event Java-based simulator was implemented using the Graphstream library v1.0 [21] [22]. The aforementioned was chosen since the focus of this research is to evaluate the implementation of mass-spring model in a cluster-based algorithm on a dynamic MANET [21]. Data traffic and protocols evaluation is out of the scope of this research. We will call EESOA node to the implementation of a MANET node which will be performing EESOA defined at [9] when simulating. Thereupon mass-spring model will be built-in on each EESOA node. With the aforementioned, we are linking the mass-spring behavior to the hierarchies generated by the cluster-based algorithm. In addition, the mass-spring model on each EESOA

 ISBN: 978-1-61208-794-8

node will have a pre-defined set of k constants as well as equilibrium distances L for each EESOA node hierarchy. Thus, each time an EESOA node receives a `hello broadcast message`, the in-built mass-spring system will perform the Algorithm 1. Consequently, each EESOA node will generate a mass-spring model with the respective constant to all its neighbors within one-hop. Algorithm 1 implementation will take into account all the neighbor mass-spring models when computing the final movement vector $\vec{v}$. Equilibrium will be maintained by following (1). The prior defined constants L and k for each EESOA node will maintain a connectivity-aware behavior on the MANET's nodes by maintaining formation on each neighbor within one-hop. This will ensure that each node will try to stay within range L of its neighbors defined by (1).

The simulation presented in this work assumes that each node know the coordinates of its own position. Thus, the EESOA node will share its location coordinates with neighboring nodes on each periodic `hello broadcast message`. A minimum constant area range of reception of the node and non dynamic k and L constants are assumed for this simulation. With the previous defined implementation, the resulting MANET will have a virtual backbone thanks to EESOA while expanding the coverage area thanks to the mass-spring model without losing connectivity. Hence, the connectivity awareness-emergent behavior of the proposal. Note that the original vector $\vec{v}$ of movement might have been bigger but thanks to mass-spring model the node will maintain a range, hence, the connectivity emergent behavior.

B. Simulation Environment

The simulation was implemented on a java-based discrete-event simulator. For the graphic user interface and MANET simulation, the Graphstream library was used. The initial setup parameters for this simulation is defined in Table I.

TABLE I. SIMULATION SETUP

Parameter	Value
Simulation Area	50x50 mts
EESOA Nodes	20
Survivor Nodes	50
Mobility Model	Random Uniform Distribution
Java Version	Java SE 8
Graphstream Version	1.3
Node Range	10 mts
Survivor Groups	3

Figure 4 illustrates an example of a simulation setup with 10 EESOA nodes formation and a 30 survivor nodes distributed in a random uniform manner on a 50x50 mts grid.

C. Simulation Scenarios

To evaluate the performance of mass-spring implementation with EESOA we require to define scenarios, which represents realistic disaster circumstances. For the purposes of this research we will focus on the deployment configuration for both, either survivors or MANET drones. Disaster scenarios will constraint the survivors distribution on the affected area depending the catastrophe. On earthquakes, leaves groups of survivor trapped in a dense concentration, or in floods can leave survivors scattered on the area. Similarly, the deployment of drones in disaster areas depends on the terrain conditions. If

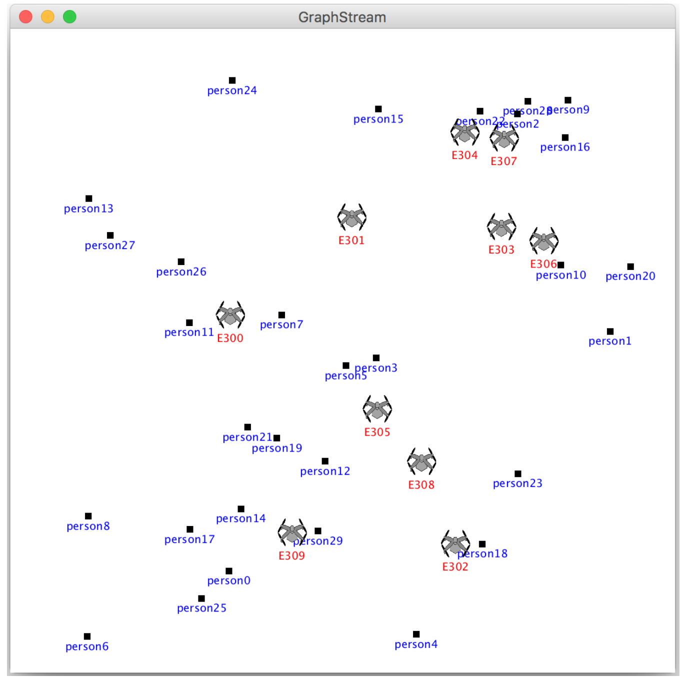


Figure 4. Simulation Example

terrain are inhospitable the deployment is required to be done by air otherwise they can be dropped in a scattered manner.

Therefore, we will define two configurations with which we will be able to generate such scenarios. Such configurations will be defined as ***SPREAD*** and ***DENSE***. For the MANETs nodes, such configuration will be translated in terms of deployment on the disaster area. Likewise, for the survivors this will be translated in terms of how the survivors are scattered or deployed across the disaster zone.

The first configuration will be named ***SPREAD***. For the survivors, this will be a random uniform distribution deployment across the simulation area. For the drones, will be translated in a connected graph placed on a random uniform distribution manner.

The second configuration will be named ***DENSE***. For the survivors, this will consist on a concentration of survivors. The groups of survivors will define the number of survivors per group. The groups of survivors will maintain a minimum distance among them. For the drones, a random position on the grid will be used as long as the condition that the generated graph is connected is fulfilled.

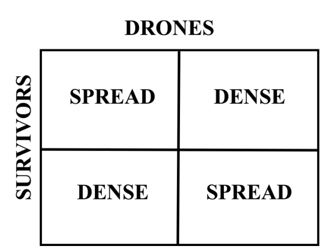


Figure 5. Deployment scenarios

 ISBN: 978-1-61208-794-8

The findings presented in this work, will cover a total of four scenarios that will be simulated as shown in Figure 5.

In Figure 7 it can be observed the initial state of the scenarios combination from Figure 5 in Figure 7a, 7c, 7e and Figure 7g. Likewise the final state will be shown in Figure 7b, 7d, 7f and Figure 7h.

SPREAD survivors with ***DENSE*** MANET deployment scenario. This scenario addresses circumstances in which the survivors are scattered across the affected area and the only way to deploy the drones is in a dense concentration such as air drop from an aircraft, helicopter, etc. An example of such simulation of this scenario is shown in Figure 7a and Figure 7b.

SPREAD survivors with ***SPREAD*** MANET deployment scenario. This scenario addresses circumstances in which the survivors are scattered across the affected area and drones can be spread across area. An example a simulation of this scenario is shown in Figure 7c and Figure 7d.

DENSE survivors with ***DENSE*** MANET deployment scenario. This scenario addresses circumstances in which the survivors are clustered across the affected area in groups and drones are deployed in a dense concentration. Such scenario denotes disasters in which the survivors are trapped and drones are deployed by air due to the inhospitable terrain to deploy them by ground vehicles. An example a simulation of this scenario is shown in Figure 7e and Figure 7f.

Finally ***DENSE*** survivors with ***SPREAD*** MANET deployment scenario. This scenario addresses circumstances in which the survivors are across the affected area in groups and drones can be spread across the area. Such scenario denotes disasters in which the survivors are trapped and drones can be deployed by air or ground. An example a simulation of this scenario is shown in Figure 7g and Figure 7h.

It can be observed in Figure 7b and Figure 7h that regardless the configuration deployment either ***DENSE*** or ***SPREAD*** the virtual back bone will be formed. Also note that that the nodes maintain a range of distance among them. Observe that for purposes of disaster applications, when we have a ***DENSE*** deployment for survivors, as shown in Figure 7e, if a MANET drone reaches one survivor of such group, neighboring survivors of such survivor could provide their data to the connected survivor.

D. Simulation Metrics

With the combination of the defined scenarios, metrics to evaluate the performance of the mass-spring implementation on EESOA are required. We will define the metrics based on the initial and final deployment. This will be applied for the MANET as well as the survivors. Thus, we have defined two metrics. Coverage Area (CA) which will be defined as an approximation of the cumulative area which each node of the MANET can receive any survivor signal, see (2) below.

$$CA \approx \bigcup_{i=1}^{n} A_i \tag{2}$$

Where:
A_i The area of each i^{th} ESSOA node
n The number of EESOA nodes

The second metric will be the number of the survivors found. Both metrics are key factors to take into account when deploying a MANET for disaster applications.

We will obtain the initial and final CA as well as the number of survivors found. The final metrics will be computed once the simulation have converged for comparison purposes. Given the mass-spring model and given and equilibrium distance defined on (1). We will define a converged state of the simulation once the nodes cannot longer move since the sum of those forces have cause them to reach the equilibrium. When the simulation converges, neither the CA or survivors found metrics will change from such converged time onwards.

E. MANET node

This work considers the node as an autonomous wireless mobile device with a non-rechargeable battery. It is assumed that the node knows its coordinates (x, y). The node coverage area will be assumed to be a r square. Therefore, the CA will be square centered on the MANET node regardless its (x, y) location as denoted in Figure 6.

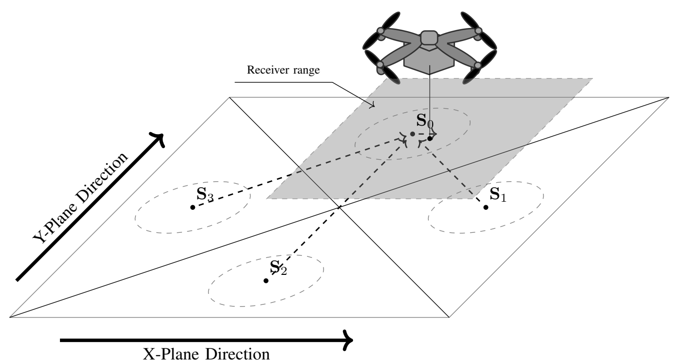


Figure 6. EESOA node coverage area

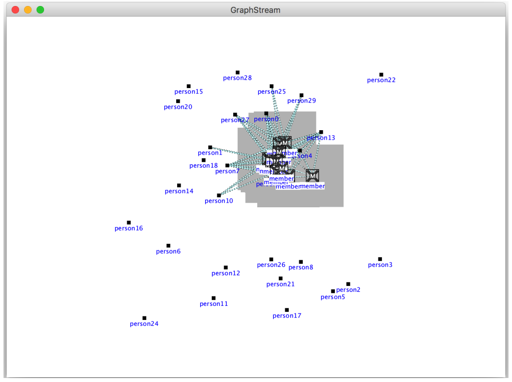
V. Simulation Results

Simulation was performed in a Java discrete-event simulator paired with the Graphstream library. The setup parameters for the is described in Table I. Simulation was performed with 15 drones and 50 survivors in a 50x50 mts grid area. The aforementioned was performed for the 4 scenarios defined in Figure 5. For each scenario, 10 simulations were performed until each simulation reached a converged state as defined in Section IV-C.

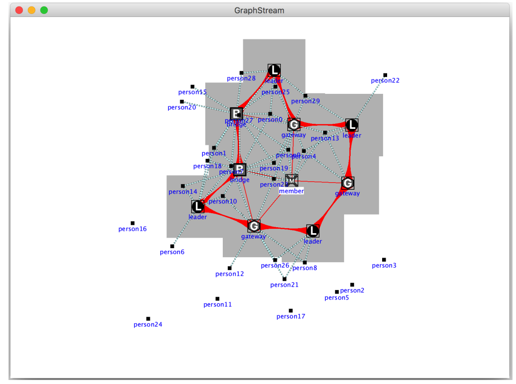
A. Dense Manet Spread Survivors Scenario

The final coverage area was significantly greater than the initial when the initial deploy configuration for nodes was ***DENSE*** as shown in Figure 8. On average, the final area showed an increase ratio of 3.7 and got to 82% from the ideal coverage area (1500 mts^2). Likewise, the final number of survivors found was greater than initial finding an average of 22 survivors (See Figure 9), showing an increase of 28% more survivors found.

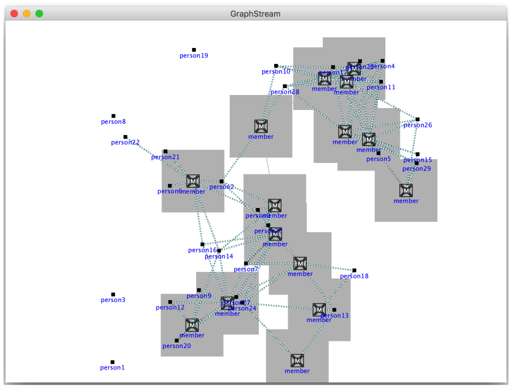
 ISBN: 978-1-61208-794-8



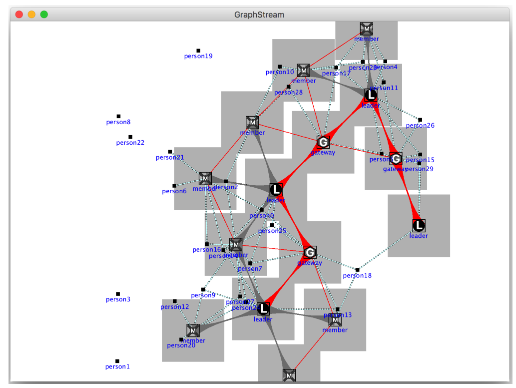
(a) Initial Dense MANET deployment with Spread survivors



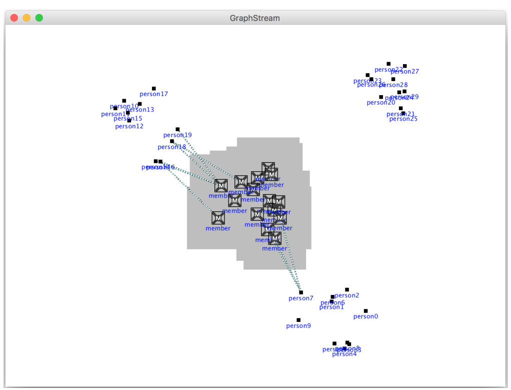
(b) Final Dense MANET deployment with Spread survivors



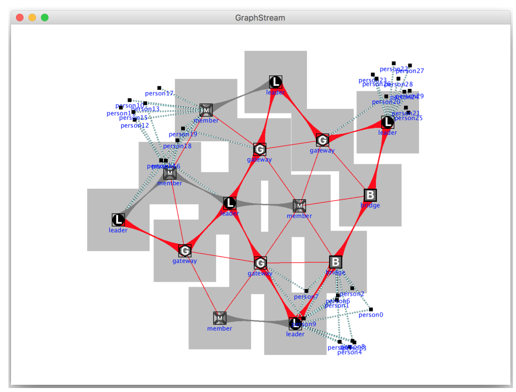
(c) Initial Spread MANET deployment with Spread survivors



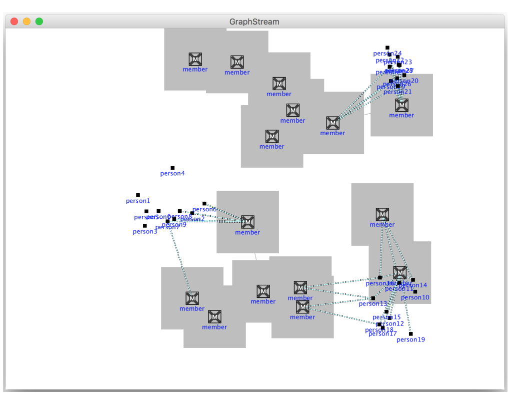
(d) Final Spread MANET deployment with Spread survivors



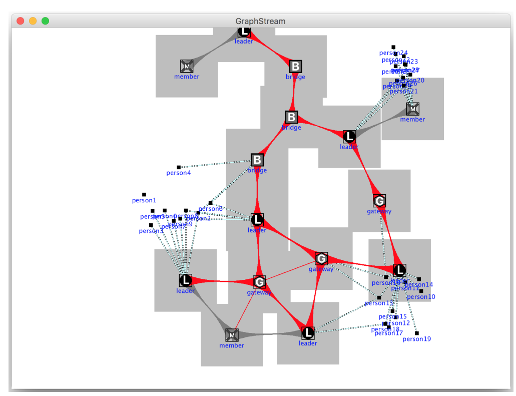
(e) Initial Dense MANET deployment with Dense survivors



(f) Final Dense MANET deployment with Dense survivors



(g) Initial Spread MANET deployment with Dense survivors



(h) Final Spread MANET deployment with Dense survivors

Figure 7. Initial and Final Simulation Scenarios Combination

 ISBN: 978-1-61208-794-8

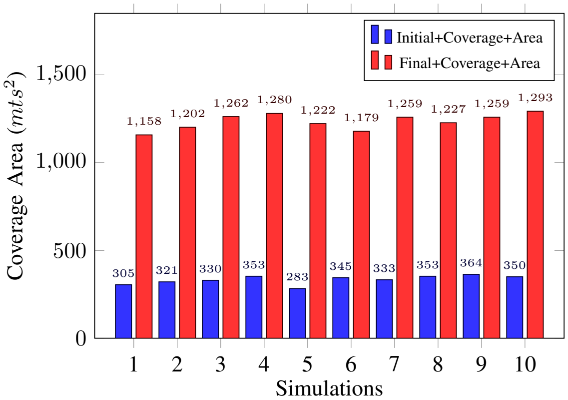


Figure 8. Dense MANET & Spread Survivors: Coverage Area

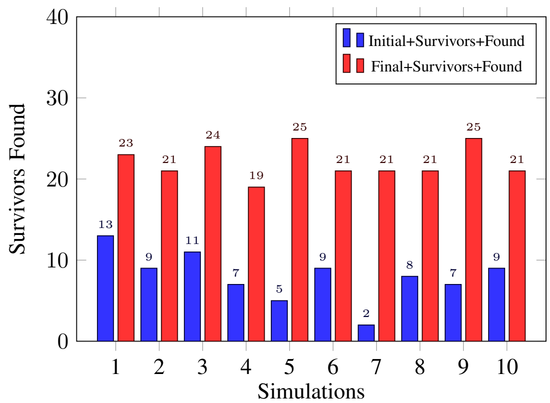


Figure 9. Dense MANET & Spread Survivors: Survivors Found

B. Spread Manet Dense Survivors Scenario

When deployment of drones was ***SPREAD*** the increase of CA against the initial state was less than when the configuration for drones was ***DENSE***. With a ratio of 1.4 as Shown in Figure 10. Also the final CA was 77% of the ideal coverage area. The number of survivors found was bigger than the ***DENSE*** MANET (See Figure 11). With ***SPREAD*** survivors with an average of 23. Thus, with an increase of 19.4% more survivors found against the model without the mass-spring.

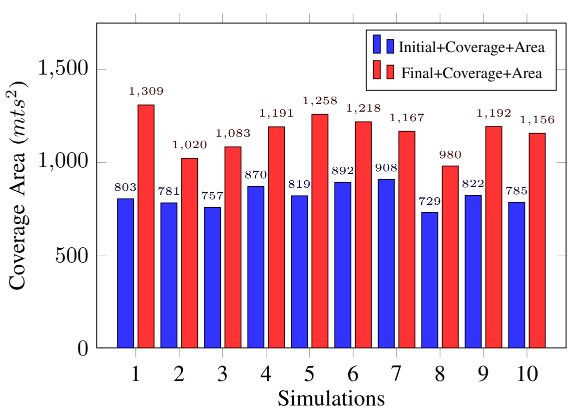


Figure 10. Spread MANET vs Dense Survivors: Coverage Area

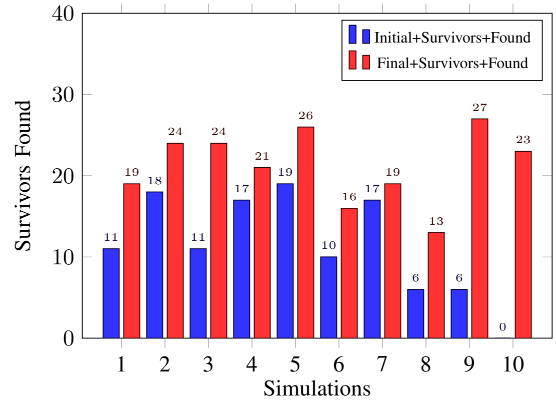


Figure 11. Spread MANET vs Dense Survivors: Survivors Found

C. Spread Manet Spread Survivors Scenario

On a ***SPREAD*** MANET configuration, increase ratio was similar against the ***SPREAD*** MANET with ***DENSE*** survivors scenario with a 1.43 increase ratio and $\sim$80% of the ideal coverage area (See Figure 12). On this configuration the percentage of survivors found not as significant against the two aforementioned scenarios with a increase of 9.2% (See Figure 13). This is consistent since CA increase was not significant, when ***SPREAD***, L limits further CA expansion.

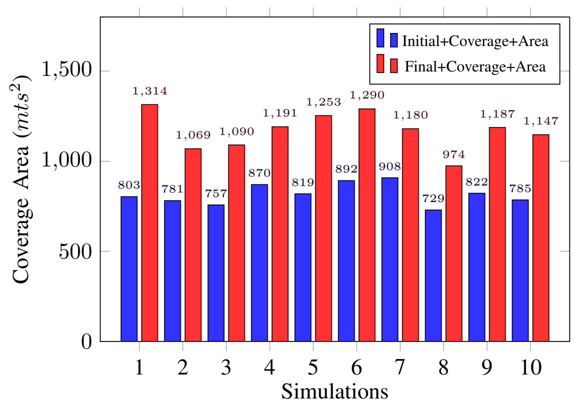


Figure 12. Spread MANET vs Spread Survivors: Coverage Area

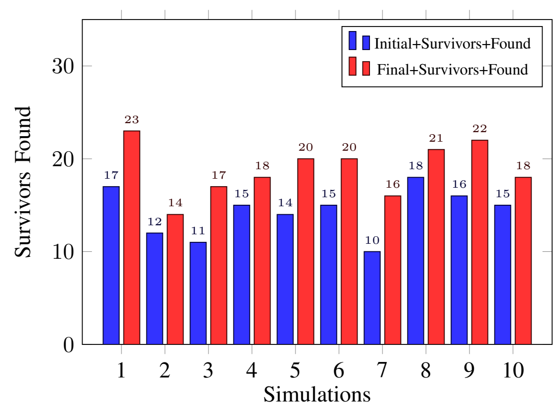


Figure 13. Spread MANET & Spread Survivors: Survivors Found

D. Dense Manet Dense survivors

As in scenario described in section V-A, with ***DENSE*** MANET deployment the increase ratio was 3.7 with an 83% of the ideal CA. CA comparison is shown in Figure 14. Similarly, as shown in Figure 15, the survivors found percentage increase against the initial state was 30% more survivors found. We can observe that on both scenarios V-A and V-D, when the deployment of nodes is ***DENSE***, performance is better.

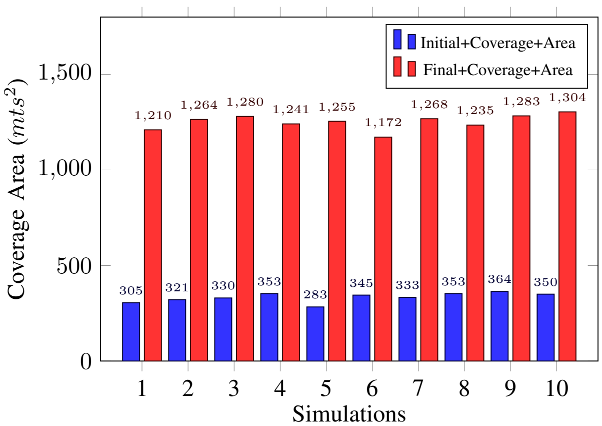


Figure 14. Dense MANET & Dense Survivors: Coverage Area

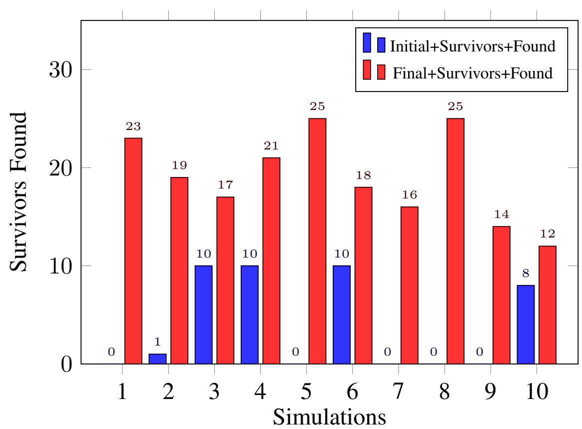


Figure 15. Dense MANET & Dense Survivors: Survivors Found

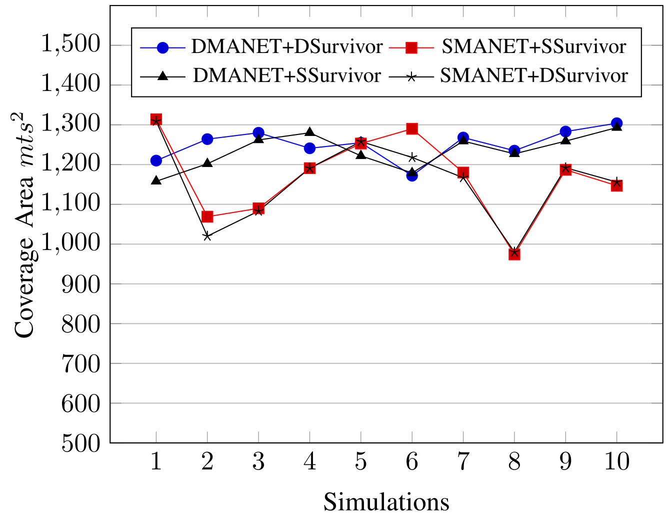


Figure 16. MANET & Survivors scenarios Area comparison

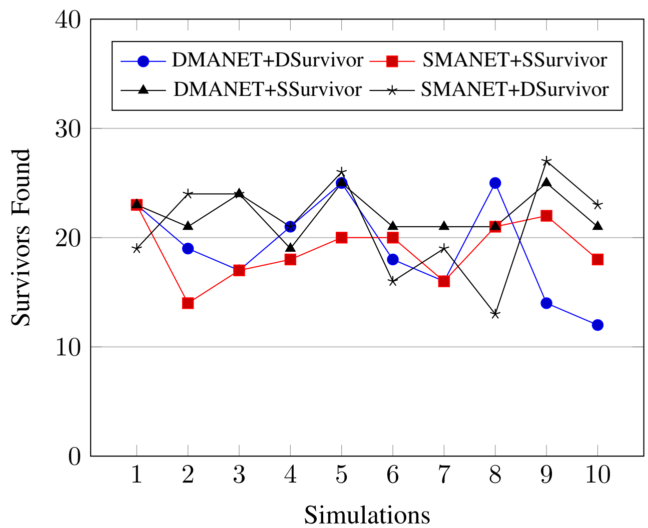


Figure 17. MANET & Survivors scenarios: Survivors comparison

To have a global perspective and for comparison purposes in Figure 16 and Figure 17 we show the final CA and number of survivors for the 4 scenarios. Nodes deployment are denoted by the prefix "D" for ***DENSE*** deployment and "S" for ***SPREAD***. Figure 16 shows an overall better performance for CA when the deployment of MANET nodes is ***DENSE***. In Figure 17 when the MANET nodes deployment is ***DENSE*** and survivors deployment is ***SPREAD*** performance is better.

VI. Conclusion and Future Work

This paper proposed the implementation of the mass-spring model on the EESOA cluster-based algorithm for natural disaster applications. A java-based discrete event simulator using the Graphstream library was developed as shown in Section IV-A. The decentralized mass-spring interaction among nodes provided a connected-awareness emergent behavior.

Simulation results have shown that the implementation of the mass-spring on EESOA shows promise. For coverage area the scenarios in which the MANET deployment configuration is ***DENSE*** with an average of 82% of the ideal CA and an increase ratio of at least 3.7. For the number of survivors found we can see that there is no clear improvement if the layout of the survivors is Dense ***DENSE*** or ***SPREAD***. Nevertheless, when the MANET configuration was ***DENSE*** we can see in Figure 17 a slight increase in performance with at least 28% increase against the initial state. The average of survivors found against the ideal (50) is at least 38%. For the cases in which the deployment of survivor was ***DENSE***, such 38% means we found more than one third of the survivors. The aforementioned shows promise when we have a group of survivors in a ***DENSE*** deployment. For the actual search and rescue operation, if we find at least one survivor of a group of survivors, neighboring survivors could use the connected survivor as relay.

Thanks to the mass-spring model implementation on the EESOA nodes, the nodes will always generate a vector $\vec{v}$ with which will try to achieve equilibrium on the system. Thus, taking into account the range of the nodes plus their L and k constants, nodes will expand as long as possible increasing the probability of find more survivors. The aforementioned will be performed without compromising connectivity.

The implementation of the mass-spring model on the EESOA cluster based algorithm shows promise in performance on scenarios when the MANET deployment is ***DENSE*** and the survivors layout on the disaster area is ***DENSE***. Hence, providing a de-centralized cluster based algorithm which is efficient for communication as shown in [9] while maintaining the connectivity as a constraint as defined on [17] by implementing the mass-spring model. Finally proposing a connectivity aware model with an self-organized emergent behavior.

Application of MANETs with UAVs for operations in disastrous areas is an undergoing increasing research field [8]. L and k constants parameter values for EESOA optimal performance is left for future research. Moreover optimal values for specific disaster scenarios such as high density survivors concentration (evacuation points) or uniform distribution (floods, typhoon) remains as an ongoing research. In future work simulations on a large scale scenario should be performed. Battery consumption should be included in future simulations as well as delay and propagation model. The challenge of an autonomous decentralized exploration algorithm that takes full advantage of the EESOA backbone and mass-spring system remains open. Future work includes the implementation of the proposed algorithm on real UAVs.

REFERENCES

[1] N. Islam and G. S. Shaikh, "Towards a disaster response system based on cognitive radio ad hoc networks," in *Proceedings of Second International, Conference on Next Generation Computing and Communication Technologies (ICNGCCT 2015)*, UAE, 2015.

[2] N. Kumar, A. Agrawal, and R. Ahmad Khan, "Emergency alert networks for disaster management: Applications perspective," in *2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)*, El Salvador, Aug 2018, pp. 1–5.

[3] B. Ojetunde, N. Shibata, and J. Gao, "Secure payment system utilizing manet for disaster areas," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 12, pp. 2651–2663, Dec 2019.

[4] J. A. L. Calvo, G. Alirezaei, and R. Mathar, "Wireless powering of drone-based manets for disaster zones," in *2017 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, Montreal, QC, Canada, Oct 2017, pp. 98–103.

[5] H. Verma and N. Chauhan, "Manet based emergency communication system for natural disasters," in *International Conference on Computing, Communication Automation*, Noida, India, May 2015, pp. 480–485.

[6] N. Aschenbruck, M. Frank, P. Martini, and J. Tolle, "Human mobility in manet disaster area simulation - a realistic approach," in *29th Annual IEEE International Conference on Local Computer Networks*, Nov 2004, pp. 668–675.

[7] H.-C. Jang, Y.-N. Lien, and T.-C. Tsai, "Rescue information system for earthquake disasters based on manet emergency communication platform," in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing (IWCMC 2009)*. New York, NY, USA: ACM, Jun 2009, pp. 623–627.

[8] M. Deruyck, J. Wyckmans, W. Joseph, and L. Martens, "Designing UAV-aided emergency networks for large-scale disaster scenarios," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 79, Apr. 2018.

[9] F. E. Balart-Sanchez, L. F. Gutierrez-Preciado, and J. G. Olascuaga-Cabrera, "Minimizing routing broadcast and packet loss in wireless ad-hoc networks with a cluster-based self-organized algorithm as mac protocol," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, Jan 2019, pp. 0499–0505.

[10] D. Konings, F. Alam, F. Noble, and E. M. Lai, "Springloc: A device-free localization technique for indoor positioning and tracking using adaptive rssi spring relaxation," *IEEE Access*, vol. 7, pp. 56 960–56 973, Apr 2019.

[11] M. Rath and B. Pati, "Appraisal of soft computing methods in collaboration with smart city applications and wireless network," *International Journal of e-Collaboration (IJeC)*, vol. 2018, pp. 27–42, Oct 2018.

[12] W. Yu, J. Choi, Y. Kim, W. Lee, and S. Kim, "Self-organizing localization with adaptive weights for wireless sensor networks," *IEEE Sensors Journal*, vol. 18, no. 20, pp. 8484–8492, Oct 2018.

[13] K. Derr and M. Manic, "Wireless sensor networks—node localization for various industry problems," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 752–762, June 2015.

[14] J. Eckert, F. Villanueva, R. German, and F. Dressler, "Distributed mass-spring-relaxation for anchor-free self-localization in sensor and actor networks," in *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, Maui, HI, USA, July 2011, pp. 1–8.

[15] J. Eckert, H. Lichte, F. Dressler, and H. Frey, "On the feasibility of mass-spring-relaxation for simple self-deployment," in *2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems*, Hangzhou, China, May 2012, pp. 203–208.

[16] S. Lee, H. Woo, and C. Lee, "Wireless sensor network localization with connectivity-based refinement using mass spring and kalman filtering," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, pp. 152–162, Dec 2012.

[17] F. G. Jean-Matthieu Etancelin, Andre Fabbri and M. Rosalie, "Dacyclem: A decentralized algorithm for maximizing coverage and lifetime in a mobile wireless sensor network," *Ad Hoc Networks*, vol. 87, pp. 174–187, May 2019.

[18] L. Bao and J. J. Garcia-Luna-Aceves, "Topology management in ad hoc networks," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing*, ser. MobiHoc '03. New York, NY, USA: ACM, Jun 2003, p. 129–140.

[19] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 5, no. 1, pp. 1–39, Feb. 2009.

[20] J. G. Olascuaga-Cabrera, A. Mendez-Vazquez, and E. López-Mellado, "A novel distributed energy-efficient self-organized algorithm for wireless ad hoc networks," in *2012 Eighth International Conference on Intelligent Environments*, Guanajuato, Mexico, June 2012, pp. 19–26.

[21] A. Dutot, F. Guinand, D. Olivier, and Y. Pigné, "Graphstream: A tool for bridging the gap between complex systems and dynamic graphs," in *Proceedings of Emergent Properties in Natural and Artificial Complex Systems. (EPNACS)*, Dresden, Germany, Oct. 2007.

[22] Litis - ri2c, documentation graphstream. [Online]. Available: http://graphstream-project.org/doc/ (Accessed May 4, 2020).

Cohort-Based Construct for Vehicular Cyber-Physical Systems

Imen Zidi and Abir Ben Ali

CRISTAL Laboratory
National School of Computer Sciences
Manouba, Tunisia
Email: zidi.imen@gmail.com, abir.benali@isetr.rnu.tn

Farouk Kamoun

SESAME Uuniversity
Tunis, Tunisia
Email: farouk.kamoun@sesame.com.tn

***Abstract*—Ensuring human life safety is inexorably the most critical objective of Intelligent Transportation System (ITS), which makes Intelligent Vehicular Network (IVN) the cornerstone of such system. Hence, in order to overcome network Quality of Service (QoS) degradation issues, several networking models for IVN have been proposed in the literature, namely cluster-based construction, cloud-based construction and platoon-based construction. Nevertheless, such constructions present several limitations, in terms of timeliness, connectivity and reliability, especially in critical environments. Therefore, we propose in this paper the design of a distributed construction based on "cohorts" and Neighbor-to-Neighbor (N2N) Communication, and we present the required cohort-managements distributed algorithms that ensure optimal IVN cohort-structuring and efficiency.**

Keywords–Cohort; Intelligent Vehicular Network; Cyber-Physical System; Safety.

I. Introduction

Saving road user's life is still the most imminent question of transportation systems since the automobile invention. Tightly associated with the automobile revolution and the population grown up, the road traffic condition turns into a critical social issue. The American National Highway Traffic Safety Administration (NHTSA) announces that 37 461 accidents related fatalities and 4.6 million injuries are recorded in 2016, and unfortunately this statistic continued to increase. In addition to, and according to European Transport Safety Council (ETSC) and NHTSA reports, more than 90% of road crashes are caused by human errors [1][2]. That is why, developing an Intelligent Transportation System (ITS) is considered as the main solution to achieve the goal of improving road traffic safety [3]. Thus, during the last decade, the road traffic safety challenge has attracted an interesting consideration from both academia and industry. Consequently, significant amount of resources are investigated around the world to develop safe and reliable ITS.

Initially, researches consider the paradigm of Autonomous Driving as a keystone for road safety and traffic efficiency, where an autonomous vehicle [2][5] is equipped with several computing, planning and sensing technologies providing different safety features, with the ability to discharge the human partially or totally from the driving task. However, autonomous vehicles are seen as isolated entities and cannot cooperate with their surrounding (vehicles or road equipment's). Thereby, a deaf autonomy cannot respond to the ITS' goal, which explains the need for autonomous vehicles cooperation mechanisms. Thus, tremendous attention was conferred to Collaborative Autonomous Driving which is mainly based on inter-vehicular communication, as described in [6].

Communicating vehicles are gathered into an unlimited-size self-organized network, characterized by dynamic topology, where inter-vehicular communication is based on broadcasting mode. Let us highlight the drawbacks behind this definition. Firstly, dynamic topology, caused by nodes' high mobility, is causing a grievous problem of dis-connectivity. Secondly, the broadcasting communication mode is suffering from the absence of feedback about the sent message reception/delivery, beside its ability to provoke network overflow, making a serious problem of transmission reliability. In addition, existing standards proposed in the literature to serve the vehicular environment are unable to guarantee bounded latency for safety-critical messages, resulting in a problem of timeliness.

Motivated by the necessity to surmount those limitations and by the evolution of distributed algorithms, we propose to structure the vehicular network into size-bounded vehicular string, so-called cohort, and we present the required cohort-managements distributed algorithms that ensure optimal vehicular network cohort-structuring and efficiency.

The remainder of this paper is organized as follows: in Section II, we briefly review the state of the art, by focusing on IVN and community converging towards such concept. We propose in Section III a cohort-based construct for Vehicular Cyber Physical System (VCPS) that we believe is more suitable for Safety-critical data dissemination. We propose in Section IV cohort management distributed algorithms. We conclude the paper in Section V.

II. State of The Art

Automotive industry has targeted to embed computerization into the vehicle driving task [7]. New vehicle models are integrating new features, impacting essentially the road traffic safety. The development is going further over time, and several manufactures around the world, like BMW, Tesla, Audi, Mobile Eye and Google, are in the race of Autonomous Driving System (ADS) development.

Autonomous driving system, also known as self-driving system, is based on on-board perception and sensing technologies, like radar, lidar, ultrasonic, optical sensors and camera. Such sensors are used to collect information from their environment. The collected data are gathered to create an accurate representation of the vehicle nearby surrounding. In addition, this data is also interpreted and analyzed, by an on-board processing unit, to help vehicle moving and reacting to safety-critical situations that might occur. Nevertheless, this solution has several limitations, which can be summed up in two points.

- Perception technologies performances can be lost due to equipment failure, obstacles and weather conditions. As example we can mention that radar sensors sight is limited by obstacles, optical and lidar sensors are influenced by bad weather conditions, e.g., lidar sensors cannot see when it rains.
- Being autonomous means acting according to its own system rules independently of external intervention from communication with other vehicles or infrastructures. This property turns it a passive and isolated entity, which can be a dangerous source in case of perception technologies lose.

Consequently, in order to overcome perception technologies limitations, system diversity and redundancies are required, similarly, to strategies used in most advanced fighter planes and deep-space satellites. Deploying a reliable vehicular communication strategy is a key redundant solution to support and defend the autonomy capacities. This principle explains the need for an intelligent vehicular network.

IVN is a vehicular self-organized network, generally providing the so-called vehicle-to-everything (V2X) communication, which can be vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I) communication, vehicle-to-pedestrian (V2P) communication, vehicle-to-bicycle (V2B) communication and vehicle-to-drone (V2D) communication. The most known and studied form of IVN in the literature, is Vehicular Ad hoc Network (VANET) [8][9][10]. Hereafter, we focus only on inter-vehicular communication V2V.

Safe transportation system reposes on real-time safety-critical (SC) inter-vehicular communication (IV) [11]. Thus, SC-IV communication algorithms and protocols are needed to coordinate IVN. IEEE 802.11p [12][13] is considered as the first standard designed for V2V and V2I communications. But unfortunately, this standard presents evident drawbacks essentially related to reliability issues, unbounded latency, security, unfairness of channel dedication. These limitations make, IEEE 802.11p standard, not suitable for real-time safety-critical applications. Moreover, the deployment of IEEE 802.11p standard requires huge investment in the network infrastructure, on-road units [9]. Then, motivated by the global deployment and commercialization of Long Term Evolution (LTE), authors in [9] propose an integrated solution for vehicular communication, both V2V and V2I, so called LTE-V, based on the time division LTE 4G technology. This proposition is expected to provide two communication modes: LTE-V-direct enabling short range direct and decentralized V2V communication, to support road safety applications requirements low latency and high reliability, and LTE-V-cell enabling centralized V2I communication. In addition, the solution provides high mobility support, optimized coverage and better resources allocation. In addition, direct Device-to-Device (D2D) based LTE V2V communication is proposed to guarantee inter-vehicular communication requirement in terms of latency and reliability [14][15][16].

All of these solutions are based on dynamic mesh topology, where nodes are characterized with a high mobility. Mobility, dynamic topology and unlimited density present serious impediments in front of reliability, connectivity and bounded latency guarantee. To alleviate as much as possible vehicular environment complexity, we propose to divide the set of vehicles in the roads into fully-distributed and bounded-size cyber-physical construct based-on directional communication, named cohort by G. Le Lann, [11][17]. Details about cohort are given in the following section.

III. Proposed Model/Solution

Breaking down the network into a fully-distributed, linear and size-bounded segment of consecutive vehicles is mainly inspired by the notion of platoons, which initially appeared around 1974. Due to the lack of space we cannot detail platoons characteristics and limitations, so, we recommend this work for more information [18].

A. Cohort Introduction and Specification

A cohort is a size-bounded ad hoc string of consecutive vehicles circulating on the same lane. Contrary to platoon, cohort is a fully-distributed cyber-physical construct based on perception technologies and directional Neighbor-to-Neighbor (N2N) communication. According to [11] cohort's concept is used to add some structuring to IVN and to achieve the road traffic safety. Consequently, the cohort construct is advanced, on one hand, to reduce the number of vehicle involved in rear-end braking crashes, and on the other hand, to alleviate interference and collision problems. The safety goals can be ensured by reducing, dramatically, incident and injury rates. Thus, safe longitudinal inter-vehicular spacing, as well as reducing velocities in the course of risk prone maneuvers are needed. The most important cohort characteristics are depicted on Figure 1.

A cohort Γ is a set of $n \leq n^{\bullet}$ (n is current cohort size and $n^{\bullet}$ is the max cohort size) contiguous vehicles, where the first member is called the cohort head and the last one is named the cohort tail [17][18]. Every cohort's member X is assigned a rank noted r_x, where, $1 \leq r_x \leq n^{\bullet}$. The cohort head is assigned the rank 1 and the cohort tail is assigned the rank n. A safe longitudinal spacing should be respected between the same cohort members and between cohorts circulating on the same lane. The inter-members gap (resp. the inter-cohort gap), so-called s_{xy} (resp. $S_{H/T}$), is bounded as follows $s^{\circ} \leq s_{xy} \leq s^{\bullet}$, (resp. $S^{\circ} \leq S_{H/T} \leq S^{\bullet}$) and tightly depends on the network density. Every isolated vehicle is considered as an isolated cohort where n =1.

Vehicles can freely leave their cohorts, by simple deceleration/acceleration or after a changing lane decision. However, after leaving its cohort, the vehicle X must join another

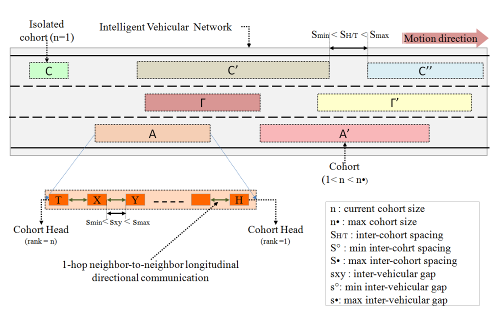


Figure 1. Cohort Specification.

cohort or creates its own one. Whatever, the decision is, joining an existing cohort or creating a new one, it cannot be carrying out arbitrarily. Actually, joining an existing cohort depends on two main factors, the cohort size, which cannot exceed the maximum value $n^{\bullet}$, and the available spacing to be inserted into, which must respect the constraint of safe inter-vehicle/cohort spacing.

Therefore, cohort management distributed algorithms are mandatory in such situation, to indicate the vehicle behavior. For the lack of space, we highlight, in this work, specifically, how a vehicle X must react after a lane changing maneuver (resp. a highway's first lane entrance). Several use cases are described hereafter, and different algorithms are proposed to show how these situations will be overcome.

B. System Model

All the use cases described afterwards, are supposed taking place on the highway. Then, we assume that the entire IVN on the highway is broken down into many cohorts of variable size. Each cohort is formed, as described above, by a bounded number of nodes moving in the same direction at a similar velocity. Cohort's members' cooperation is ensured by directional N2N communication. This communication paradigm is out of the scope of this paper, and for more details about N2N communication, we can refer to [17][19][20][21][22]. Periodic control messages exchange, equivalent of beaconing service in VANET and platoon, is essential for cohort management and local member data update.

In this paper, we focus on the lane changing maneuver. Accordingly, different use cases resulting from the lane changing maneuver are studied hereafter. Every maneuver, taking place on the road, is divided into cyber and physical phases. Our researches are concerned with the cyber ones.

Thus, cyber procedures are necessary to perform a safe and successful maneuver. The lane changing maneuver is governed by three cyber phases. Author in [19] has proposed a protocol so-called Zebra Protocol to cover up all these cyber phases. Details about these phases are given in the next section (IV-A). Theoretically, the cyber phases, presented there, must be executed by any vehicle tends to perform a lane change maneuver, even a highway first lane entrance, but practically, in some situation, only the first phase can be performed. Briefly, the first phase consists on diffusing a lane changing request. This situation can lead to the following hypotheses:

- The transmitted message m, is lost, and none of the vehicle X surrounding, had the opportunity to receive it, and this case is covered by the study in [19].
- None from the nodes who have received the message m is eligible to serve in this maneuver. So the eligible group is empty. In this paper we focus on this case.

The following use cases, studied in this work, result from the second hypotheses.

After changing its lane, and depending to the global network density, the vehicle X can be inserted in the middle of an existing cohort, in the inter-cohort spacing, or, in a free spacing, typically, the case of low density network.

IV. Cohort Management Distributed Algorithms

A. Middle Cohort Insertion

Let us start, firstly, by describing the procedure followed by the vehicle X to change its current moving lane safely. It is interesting to indicate that the same process is adapted when a vehicle Y is supposed to enter the highway.

We consider the scenario depicted on Figure 2. A vehicle X, member of cohort C', is at the position (x, y) and circulating on lane i, wants to move to the lane i±1. Otherwise, at time τ, X has the coordinates (x, y) and moving with at the velocity on the lane i. At the time $\tau + \varepsilon$, X wants to be at the position (x', y') on an adjacent lane i±1. This scenario is covered by three cyber phases, illustrated on Figure 3, as following:

Phase 1: X informs its surrounding that it wants change its lane and go to an adjacent one. In this purpose, X transmits a message m containing its current situational data at the time τ, called $\omega_\tau(X)$, and the wanted situational data at the time $\tau + \varepsilon$, called $\omega_{\tau+\varepsilon}(X)$. So m has this form; $m = [\omega_\tau(X) + \omega_{\tau+\varepsilon}(X)]$. The message m will be received by all the nodes in the Geocast coverage area of X.

Every vehicle who has received m has to verify its eligibility to positively response to this request. To test its eligibility, each node Y will compare its future situational data (at time $\tau + \varepsilon$) with the requested situational date at the same time. If these information are approximately close, Y announces itself as an eligible vehicle and informs its neighbors. Else Y ignores the message. The eligibility test is performed according to the procedure presented by Algorithm 1. At the end of this cyber phase a group of eligible vehicles is formed, so-called E. This group is marked on Figure 3 by the red rectangle.

Algorithm 1: Eligibility Procedure

```
Data: m ← [ω_τ(X) + ω_{τ+ε}(X)]
      d ← ω_{τ+ε}(Y)
begin
    if ω_{τ+ε}(X) and ω_{τ+ε}(Y) are close then
        // Y declares itself eligible
        eligible ← true
        // inform the rest of nodes
        generate(m_eligible)
        send(m_eligible)
    else
        // Y ignores m
        discard(m)
```

Phase 2: During phase 2, the eligible group members will cooperate together in purpose to decide the couple of nodes, who will participate practically in the physical phase of this maneuver, by creating the necessary spacing to insert X, this couple are called the actors [19].

This cooperation, is a sort of negotiation between these nodes and it requires the use of a consensus protocol. Agreement protocols are out of scope of this paper, but it is essential to mention that our research is based on the agreement protocol proposed by G. Le Lann in [17]. How the consensus protocol is working is demonstrated on Figure 3. Every node has to disseminate its own proposition, noted for example v_z. In our

 ISBN: 978-1-61208-794-8

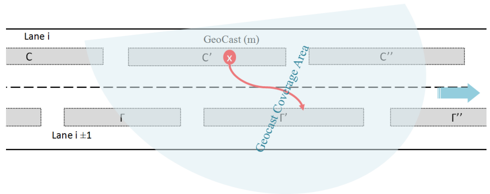


Figure 2. Middle cohort insertion request geocasting.

situation, v_z contains the couple of nodes considered by the node Z to be suitable as actors. The propositions are collected and propagated until reaching the two extremities of the E. When this collecting message arrives to the first (resp. last node) in E, it will be sent in the opposite direction, for example from the last one to the first one, and is-to-it. The messages coming from the E group extremities will be received by a same node and this node will take the final decision and disseminate it to the rest of E.

Phase 3: The actors, here are represented by the couple (Y, Z), will inform X by the decision resulting from the consensus protocols. This cyber phase ends up by triggering the maneuver physical phase.

B. Inter-Cohort Spacing Insertion

Let us consider the following scenario, X performs the geocast and waits, but no response is received. So X deducts that no vehicle is eligible to participate to its maneuver. Then X decides to move to the lane i±1. Consequently, two use cases are possible. After moving to lane i±1, X can be situated between two contiguous cohorts or in a free spacing. Free spacing insertion use case will be detailed in the next subsection, III-C. Hereafter, we focus on the second case. After changing its lane, as depicted on Figure 4, X is actually situated in the inter-cohort spacing, $S_{H/T}$, of two contiguous cohorts, Γ and Γ'. In such condition X must join Γ or Γ', or create its new cohort, if the available space permits, or leave this space if we are facing a compacted network.

In this section we propose a schema helping X to make the most suitable decision, in this situation. Furthermore, we assume that X is the only responsible of its future cohort selection, and this selection is based-on the distance separating X and this cohort. We, also, suggest that X will select the closest cohort, so we proceed as follows:

- Measure the distance separates X and Γ Tail's, so-called $D_{T/X}$, and the distance separates X and Γ' head's, so-called $D_{H/X}$.
- Compare $D_{H/X}$ and $D_{T/X}$, and then make decision.
- If $D_{T/X}$ is smaller than $D_{H/X}$, then X will try join Γ, else X will try join Γ'.

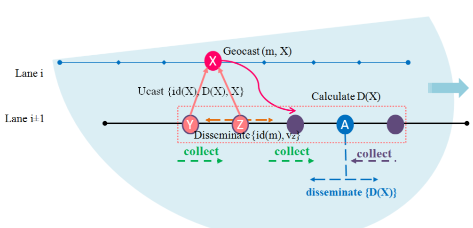


Figure 3. Lane changing maneuver cyber phases demonstration.

This mechanism is presented by the pseudo-code entitled Algorithm 3. After comparing $D_{H/X}$ and $D_{T/X}$, if $D_{T/X}$ is smaller than $D_{H/X}$, (resp. $D_{T/X}$ is smaller than $D_{H/X}$) X will send Cohort Tail Insertion Request to T (Γ tail), (resp. Cohort Head Insertion Request to H (Γ' head)), as shown on Figure 5-b, (resp. Figure 5-a). When the request is received, T (resp. H) must verify if its own cohort is able to support a new member, by checking the constraint of cohort size, $n < n^{\bullet}$. Consequently, the request will be approved only if $n < n^{\bullet}$ is true, see Algorithm 2. Then, X's reaction is depending on T's, (resp. H) reply. So, if the request is accepted, X will proceed according to Algorithm 4, (resp. Algorithm 5);

- X assigns itself a rank $n + 1$, (resp. rank 1).
- Accelerates until $D_{T/X}$, (resp. decelerate until $D_{H/T}$) respects the constraint of inter-vehicular spacing and $D_{H/X}$, (resp. $D_{T/X}$) respects the inter-cohorts gap.
- Sends a message m_x to the rest of the cohort, to help them updating their local data.

Algorithm 2: Request Acceptance Procedure

Data: $n, n^{\bullet}$
Result: *accept*
begin
  if $(n < n^{\bullet})$ **then**
    accept ← true
  else
    accept ← false
  return *accept*

If the request is rejected, X must react otherwise. So, the node has to perform the opposite request. X is going to try to join its successor cohort Γ', (resp. its predecessor cohort Γ), by performing, Cohort Head Insertion Request, (resp. Cohort Tail Insertion Request). And if the request is accepted, X has to proceed as described above. But the worst case condition is when the Cohort Head and Cohort Tail requests are rejected. Accordingly, we propose the following solution: X is going to verify whether, within the available spacing $S_{H/T}$, it is able to create its own cohort. Then, the lower bound of inter-cohort spacing must be respected.

If $SH/T \ll 2 * S^{\circ} + car_{size}$, then X must leave its current location. Leaving the current location can train other type of maneuvers like overtaking, or passing an entire cohort

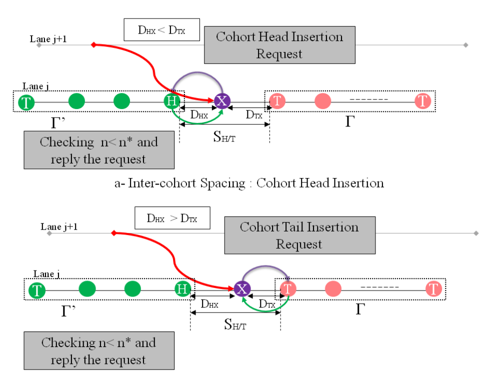


Figure 4. Inter-cohort spacing insertion illustration.

 ISBN: 978-1-61208-794-8

Algorithm 3: inter-Cohort Spacing Insertion

Data: $D_{H/X}, D_{T/H}, S^\circ, S^\bullet, s^\circ, s^\bullet$
$S_{H/T} \longleftarrow D_{H/X} + D_{T/H} + car_{size}$
begin
  if *($D_{H/X} \le S^\circ + care_{size}$)* **then**
    $r_x \longleftarrow 1$
  else if *($S^\circ \le S_{H/T} 2.S^\circ + car_{size}$)* **then**
    if *($D_{T/X} D_{H/X}$)* **then**
      cohortTailInsertionRequest()
    else if *($D_{T/X} D_{H/X}$)* **then**
      cohortHeadInsertionRequest()
  else
    leave()

or even a new lane changing maneuver. Actually, overtaking and passing an entire cohort is out of the scope of this work. In addition, it is interesting to mention that, X is also able to decide to perform one of these options even without performing cohort insertion request.

C. Free Spacing Insertion

Resume the same scenario described in the beginning of the last subsection (IV-B), and as mention there, in this section, we focus on the free spacing insertion use case. After performing its lane changing maneuver, X is located in a low density lane. And in this situation, one of the subsequent sub-cases is able to take pace.

1st sub-case: X goes into an almost empty lane i±1. The vehicle finds itself far away from any cohort. Consequently, X is forced to create a new cohort of size $n = 1$. Then, X is going to declare itself as a new isolated cohort by assigning a rank equal to 1. While respecting the allowed velocity, X has the choice to accelerate/decelerate to join distant cohorts, if they existed, or to keep its current speed.

2nd sub-case: In such situation X is located behind some cohort , as shown in Figure 5-b, and there is no close cohort following it. Or X is located in front of a cohort , as depicted in

Algorithm 4: Cohort Tail Insertion Request

begin
  send(requestToTail)
  wait()
  if *(acceptFromTail == true)* **then**
    $r_x \longleftarrow n + 1$
    if *($D_{T/X} \ge s^\bullet$)* **then**
      accelerate until $s^\circ \le D_{T/X} < s^\bullet$
    send(m_x)
  else if *(acceptFromTail == False)* **then**
    if *($D_{H/T} \le S^\circ + car_{size}$)* **then**
      decelerate until $D_{H/T} \ge S^\circ$
      cohortHeadInsertionRequest()
    else if *($D_{H/T} \le 2.S^\circ + car_{size}$)* **then**
      decelerate until $D_{T/H} \le S^\circ$ $r_x \longleftarrow n + 1$
    else if *($D_{H/T} \ge S^\circ$)* **then**
      leave()

Algorithm 5: Cohort Head Insertion Request

begin
  send(requestToHead)
  wait()
  if *(acceptFromHead == true)* **then**
    $r_x \longleftarrow 1$
    if *($D_{T/X} \ge s^\bullet$)* **then**
      decelerate until $s^\circ \le D_{H/X} < s^\bullet$
    send(m_x)
  else if *(acceptFromHead == False)* **then**
    if *($D_{H/T} \le S^\circ + car_{size}$)* **then**
      accelerate until $D_{H/x} \le S$
      cohortTailInsertionRequest()
    else if *($D_{H/T} \le 2.S^\circ + car_{size}$)* **then**
      accelerate until $D_{T/x} \le S^\circ$
      $r_x \longleftarrow 1$
    else if *($D_{H/T} \ge S^\circ$)* **then**
      leave()

Figure 5-a, and there is no cohort ahead. In both possibilities X has to join . Thus, we have, like in Section IV-B, either cohort tail insertion request, or cohort head insertion request, or also create a new independent cohort, with respect to the inter-cohort gap constraint. The main algorithm, solving this use case is presented by the pseudo-code, so-called, Algorithm 6.

In fact, within this use case X has more freedom to decide to create a new isolated cohort or to try to join the existing one. So, this use case is tightly close to X desire more than the constraint of available space, like the preceding subsection. Then, X behavior can be described as follow:

- X decides to create a new cohort, then, according to its location, X decelerates/accelerates to create the necessary inter-cohort gap, and assigns itself rank 1.
- X decides to join existing cohort, so, depending to its current location, X will send cohort tail or cohort head insertion request.

As described above, X will send a cohort tail insertion request to T, (resp. cohort head insertion request to H). Then, T (resp. H) treats the received request according to Algorithm 2, and sends its reply to the requestor. According to T's response, (resp. H's response), if the request is accepted, X

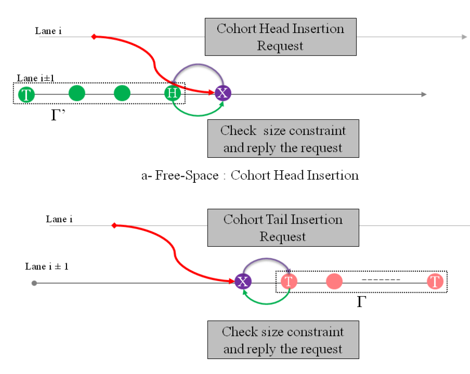


Figure 5. Free space insertion illustration.

Algorithm 6: Free Spacing Insertion Algorithm

```
Data: D_{H/X}, D_{T/X}, S°, S•
begin
    if (X decide to create new cohort) then
        if (X is behind ) then
            decelerate until S° ≥ D_{T/X} ≥ S•
        else if (X in front of ) then
            accelerate until S° ≥ D_{H/X} ≥ S•
    else if (X decides to jion an existing cohort) then
        if (X behind ) then
            cohortTailInsertionRequest()
        else if (X is in front of ) then
            cohortHeadInsertionRequest()
    else
        leave()
```

Algorithm 7: Free-Space Cohort Tail Insertion Procedure

```
begin
    send(requestToTail)
    wait()
    if (acceptFromTail == true) then
        r_x ⟵ n + 1
        if (D_{T/X} ≥ s•) then
            accelerate until s° ≤ D_{T/X} < s•
        send(m_x)
    else if (acceptFromTail == False) then
        decelerate until D_{T/H} ≤ S°
        r_x ⟵ 1
```

Algorithm 8: Free Space Cohort Head Insertion Procedure

```
begin
    send(requestToTail)
    wait()
    if (acceptFromHead == true) then
        r_x ⟵ 1
        if (D_{T/X} ≥ s•) then
            decelerate until s° ≤ D_{T/X} < s•
        send(m_x)
    else if (acceptFromHead == False) then
        accelerate until D_{T/H} ≤ S°
        r_x ⟵ 1
```

will proceed according to Algorithm 7, (resp. Algorithm 8).

The major difference between cohort head and cohort tail insertion procedures proposed for this use case and the ones described in the above section is the impact of space available for X to react. In such case, X has sufficient space to act freely.

V. Conclusion

In this paper, we explained the need to structure the IVN into fully-distributed and bounded-size vehicular strings named cohorts. These cohorts, cyber-physical systems based on short-range neighbor-to-neighbor directional communications, are purposed to alleviate as much as we can the complexity of vehicular environment and to ensure the road traffic safety, and to minimize dramatically the collision and interference problem. In this scope, we proposed, in this work, several algorithms to manage the vehicular behavior within several use cases, and for that we focus on the lane changing maneuver. In our future work we focus on implementing and testing these propositions.

References

[1] Automated Driving Systems 2.0: A Vision For Safety (reportNo: DOT HS 812 442), U.S Departement Of Transportation: National Highway Traffic Safety Administration, September 2017, www.nhtsa.gov.

[2] Prioritising the Safety Potential of Automated Driving in Europe, European Transport Safety Council (ETSC), April 2016, www.etsc.eu.

[3] An assessment of LTE-V2X (PC5) and 802.11p direct communications technologies for improved road safety in the EU, 5 December 2017, www.5GAA.org.

[4] L. Dedon, et al., "State Strategies to Reduce Highway and Traffic Fatalities: A Road Map for States", (Washington, D.C.: National Governors Association Center for Best Practices, February 2018).

[5] C-Y. Chan, "Advancements, prospects, and impacts of automated driving systems", *International Journal of Transportation Science and Technology*, vol. 6, issue 3, Sep. 2017, pp. 208-216, available: https://doi.org/10.1016/j.ijtst.2017.07.008.

[6] Y.Y. Nasrallah, I. Al-Anbagi, and H.T. Mouftah, "Enhanced Algorithms for the IEEE 802.11p Deployment in Vehicular Ad Hoc Networks", IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, Canada, 2017, pp.24-27.

[7] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations", *Transportation Research Part A: Policy and Practice*, vol. 77, Jul. 2015, pp. 167-181, available: https://doi.org/10.1016/j.tra.2015.04.003.

[8] M. Hadded, A. Laouiti, R. Zagrouba, P. Muhlethaler, and L. Azouz Saidane, "A Fully Distributed TDMA based MAC Protocol for Vehicular Ad Hoc Networks". [Research Report] Inria Paris Rocquencourt. 2015.

[9] S. Chen, J. Hu, Y. Shi, and L. Zhao, "LTE-V: A TD-LTE-Based V2X Solution for Future Vehicular Network", *IEEE Internet Of Things Journal*, vol. 3, issue 6, Dec. 2016, pp. 997 - 1005, DOI: 10.1109/JIOT.2016.2611605

[10] A. Dabboussi, et al., "Fault Tree Analysis for the Intelligent Vehicular Networks", IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh-Lebanon, 2018.

[11] G. Le Lann, "Safe Automated Driving on Highways–Beyond Today's Connected Autonomous Vehicles", Complex Systems Design Management Conference, Towards smarter and more autonomous systems, Paris-France, 2017.

[12] F. Raviglione, M. Malinverno, and C. Casetti, "Characterization and Performance Evaluation of IEEE 802.11p NICs", ACM Workshop on Technologies, mOdels, and Protocols for Cooperative Connected Cars (TOP-Cars) Catania-Italy, Jul. 2019, pp. 13–18, available: https://doi.org/10.1145/3331054.3331548.

[13] S. Baek, I. Lee, and C. Song, "A New Data Pilot-aided Channel Estimation Scheme for Fast Time-varying Channels in IEEE 802.11p Systems", *IEEE Transactions on Vehicular Technology*, vol. 68, Issue 5, May 2019, pp. 5169 - 5172, available: 10.1109/TVT.2019.2906358.

[14] J. Mei, K. Zheng, L. Zhao, Y. Teng, and X. Wang, "A Latency and Reliability Guaranteed Resource Allocation Scheme for LTE V2V Communication Systems", *IEEE Transactions on Wireless Communications*, vol. 17 , Issue 6, June 2018, pp. 3850 - 3860, available: 10.1109/TWC.2018.2816942.

[15] W. Sun, E.G. Strom, F. Brannstrom, Y. Sui, and K. C. Sou, "D2D-based V2V Communications with Latency and Reliability Constraints", IEEE Globecom Workshops (GC Wkshps), Austin, TX, USA, 2014, pp.1414-1419.

[16] Z. Liu, Y. Xie, K.Y. Chan, K. Ma, and X. Guan, "Chance-Constrained Optimization in D2D-Based Vehicular Communication Network", *IEEE*

Transactions on Vehicular Technology, Vol. 68, Issue 5, May 2019, pp. 5045 - 5058, available: 10.1109/TVT.2019.2904291.

[17] G. Le Lann, ”Fast Distributed Agreements and Safety-Critical Scenarios in VANETs”, International Conference on Computing, Networking and Communications, Santa Clara, CA, USA, Jan 2017, pp.7.

[18] D. Jia, k. Lu, J. Wang, X. Zhang, and X. Shen, ”A Survey on Platoon-Based Vehicular Cyber-Physical Systems”, *IEEE Communication Surveys Tutorials*, vol. 18, issue 1, 2016, pp. 263 - 284, available: 10.1109/COMST.2015.2410831

[19] G. Le Lann, ”On the Power of Cohorts-Multipoint Protocols for Fast and Reliable Safety-Critical Communications in Intelligent Vehicular Networks”, International Conference on Connected Vehicles and Expo (ICCVE), Beijing, China, Dec. 2012, pp. 35-42.

[20] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, ”A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks”, International Conference on Broadband Networks, San Jose, CA, USA, Oct. 2004.

[21] V. Kuo and R. Fitch, ”A Multi-Radio Architecture for Neighbor-to-Neighbor Communication in Modular Robots”, IEEE International Conference on Robotic and Automation, Shanghai, China, May 2011, pp. 5387-5394.

[22] G. Le Lann, ”Safety in Vehicular Networks-On the Inevitability of Short Range Directional Communications”, International Conference ADHOC-NOW, Athens, Greece, 2015, pp. 347-360.

Some Performance of Three-hop Wireless Relay Channels in the Presence of Rician Fading

Dragana Krstic
Faculty of Electronic Engineering, University of Niš,
Niš, Serbia
e-mail: Dragana.Krstic@elfak.ni.ac.rs

Petar Nikolic
TigarTyres
Pirot, Serbia
e-mail: nikpetar@gmail.com

Sinisa Minic
Faculty of Teacher Education in Prizren – Leposavic, University of Pristina- Kosovska Mitrovica,
Serbia
e-mail: sinisa.minic@pr.ac.rs

Zoran Popovic
Higher Technical School of Professional Studies,
Zvecan, Serbia
e-mail: z.popovix@live.com

***Abstract*—Three-hop wireless relay channels in the presence of Rician fading will be examined in this article. This system model is generated by the product of three independent, but not necessarily identically distributed, Rician random variables (RVs). Some important performance of this system, such as cumulative distribution function (CDF), outage probability (Pout) and average fade duration (AFD) of wireless relay communication system working over Rician multipath fading environment will be calculated and graphically presented. The fading parameters' impact will be analyzed based on the obtained graphs.**

Keywords- average fade duration (AFD); outage probability (Pout); random variables; Rician fading; three-hop relaying system.

I. INTRODUCTION

In mobile channels in the presence of multipath fading, properties of communications systems are disturbed significantly due to the signal envelope fluctuations [1][2]. It is of vital importance to characterize those random variations in terms of the fading characteristics and derive both first and second order [3][4]. The first order performance we will calculate here is outage probability (Pout).

The closed-form expressions for Pout, channel capacity (CC), and average symbol error probability (ASEP) are derived in [5] for amplify-and-forward (AF) multi-hop relay network in the presence of Rayleigh fading. Based on approximation of multi-hop relay by dual-hop relay systems, the analytical expressions are obtained for some scenarios.

A three-hop communication system, as we analyze, is illustrated in Fig. 1 [6]. It consists of the source node, denoted by (S), sending the information signal to the destination (D) with the help of two consecutive relays, namely R1 and R2. The AF relay nodes are assumed to be untrusted and hence, they can overhear the transmitted information signal while relaying.

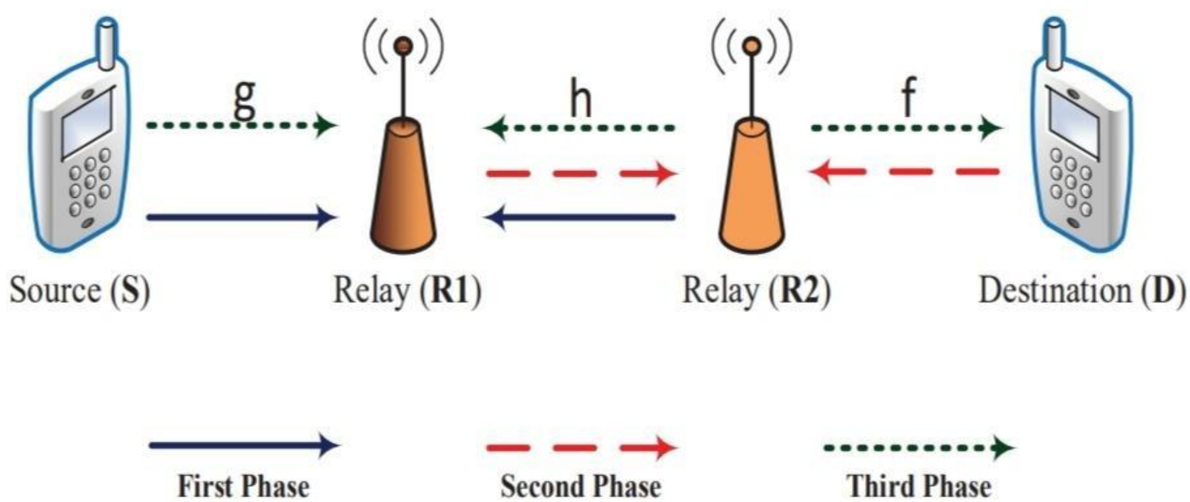


Figure 1. System model of a three-hop wireless relay [6].

All nodes are equipped with a single antenna operating in half-duplex mode. The consecutive relays are necessary helpers to deliver the information signal to the destination. This assumption is valid when the network nodes experience a heavy shadowing, or when the distance between terminals is large, or when the nodes suffer from limited power resources [6].

Three-hop system is analyzed in [7]. For three-hop relay system we will obtain the second order characteristics. The knowledge of second-order statistics of multipath fading channels (level crossing rate (LCR) and average fade duration (AFD)) can help us better understand and mitigate the effects of fading. For example, the AFD determines the average length of error bursts in fading channels [8]. So, in fading channels with relatively large AFD, long data blocks will be significantly affected by the channel fades than short blocks [9].

It is necessary to know this fact for choosing the frame length for coded packetized systems, designing interleaved or non-interleaved concatenated coding methods [10], optimizing the interleaver size, choosing the buffer depth for adaptive modulation schemes [11] [12], throughput (efficiency) estimation of communication protocols, ... Empirically-verified formulas for the LCR and AFD of common multipath fading models are necessary for all observed applications.

The output signal from multi-hop relay system is product of random variables (RVs) at hops outputs. In [13], multi-hop system in the presence of Nakagami fading is analyzed through N*Nakagami distribution as suitable for modeling of realistic wireless fading channels. Statistical analysis of cascaded Rician fading channels is given in [14]. Different performance is derived for both fading channels in terms of the Meijer G-function.

We observed different products of RVs and derived a number of system performance for dual and three-hop relay systems in closed forms in [15]-[18]. Wireless relay system with two sections (dual-hop) in κ-μ short term fading channel is observed in [15]. In [16], an analytical approach for evaluating performance of dual-hop cooperative link over shadowed Ricean fading channels is presented. All performance of product of three Rayleigh RVs are presented in [17] and the statistics of product of three Nakagami-*m* RVs is given in [18].

Here, we consider a three-hop relay channels as a special case of multi-hop relay network in the presence of Rician fading. This case is important for the channels where an optical line of sight is present. We opine that there are not enough reported works in this area.

This paper is organized through four sections. In introduction, the basic points are given. In the second section, the first order characteristics of the product of three Rician RVs are introduced. In the third section, the second order characteristics of the product of three Rician RVs are presented and graphs for all performance are plotted. The acknowledgement and conclusions close the article.

II. THE FIRST ORDER PERFORMANCE OF PRODUCT OF THREE RICIAN RANDOM VARIABLES

For description of three-hop wireless relay system it is necessary to derive the first-order characteristics of the product of three Rician RVs.

A. PDF of Product of Three Rician RVs

Rician fading is a stochastic model for radio propagation where the signal arrives at the receiver by several different paths when one of the paths, typically a line of sight signal or some strong reflection signals, is much stronger than the others. In Rician fading, the amplitude gain is characterized by a Rician distribution. It was named after Stephen O. Rice [19].

Rician RVs x_i have Rician distribution [19]:

$$p_{x_i}(x_i)=\frac{2(\kappa_i+1)}{\Omega_i e^{\kappa_i}}\sum_{j_i=0}^{\infty}\left(\frac{(\kappa_i+1)\kappa_i}{\Omega_i}\right)^{j_i}\frac{1}{(j_i!)^2}\cdot$$
$$\cdot x_i^{2j_i+1}e^{-\frac{\kappa_i+1}{\Omega_i}x_i^2},\ x_i\geq 0, \quad (1)$$

where Ω_i are mean powers of RVs x_i, and κ_i are Rician factors. Rician factor is defined as a ratio of signal power of dominant component and power of scattered components. It can have values from [0, ∞].

A random variable x is product of three Rician RVs [17 eq. (2)]:

$$x=\prod_{i=1}^{3}x_i\ , \quad (2)$$

which implies: $x_1=x/\,x_2\,x_3$.

Probability density function of product of three Rician RVs x is [20, eq. (7)]:

$$p_x(x)=\frac{2(\kappa_1+1)}{\Omega_1 e^{\kappa_1}}\sum_{j_1=0}^{\infty}\left(\frac{(\kappa_1+1)\kappa_1}{\Omega_1}\right)^{j_1}\frac{1}{(j_1!)^2}\cdot$$
$$\cdot\frac{2(\kappa_2+1)}{\Omega_2 e^{\kappa_2}}\sum_{j_2=0}^{\infty}\left(\frac{(\kappa_2+1)\kappa_2}{\Omega_2}\right)^{j_2}\frac{1}{(j_2!)^2}\cdot$$
$$\cdot\frac{2(\kappa_3+1)}{\Omega_3 e^{\kappa_3}}\sum_{j_1=0}^{\infty}\left(\frac{(\kappa_3+1)\kappa_3}{\Omega_3}\right)^{j_1}\frac{1}{(j_3!)^2}\cdot$$
$$\int_0^{\infty}dx_2\int_0^{\infty}dx_3\,x_2^{-1-2j_1+2j_2}x_3^{-1-2j_1+2j_3}$$
$$\cdot x^{2j_1+1}e^{-\frac{\kappa_1+1}{\Omega_1}\left(\frac{x}{x_2x_3}\right)^2-\frac{\kappa_2+1}{\Omega_2}x_2^2-\frac{\kappa_3+1}{\Omega_3}x_3^2}. \quad (3)$$

B. CDF of Product of Three Rician RVs

Cumulative distribution function (CDF) of product of three Rician RVs is:

$$F_x(x)=\int_0^{\infty} dt p_x(t)=$$

$$=\frac{2(\kappa_1+1)}{\Omega_1 e^{\kappa_1}}\sum_{j_1=0}^{\infty}\left(\frac{(\kappa_1+1)\kappa_1}{\Omega_1}\right)^{j_1}\frac{1}{(j_1!)^2}\cdot$$

$$\cdot\frac{2(\kappa_2+1)}{\Omega_2 e^{\kappa_2}}\sum_{j_2=0}^{\infty}\left(\frac{(\kappa_2+1)\kappa_2}{\Omega_2}\right)^{j_2}\frac{1}{(j_2!)^2}\cdot$$

$$\cdot\frac{2(\kappa_3+1)}{\Omega_3 e^{\kappa_3}}\sum_{j_1=0}^{\infty}\left(\frac{(\kappa_3+1)\kappa_3}{\Omega_3}\right)^{j_1}\frac{1}{(j_3!)^2}\cdot$$

$$\int_0^{\infty} dx_2 \int_0^{\infty} dx_3 x_2^{-1-2j_1+2j_2} x_3^{-1-2j_1+2j_3} e^{-\frac{\kappa_2+1}{\Omega_2}x_2^2-\frac{\kappa_3+1}{\Omega_3}x_3^2}$$

$$\int_0^{x} dt t^{2j_1+1} e^{-\frac{\kappa_1+1}{\Omega_1}\frac{t^2}{x_2^2 x_3^2}}=$$

$$=\frac{2(\kappa_1+1)}{\Omega_1 e^{\kappa_1}}\sum_{j_1=0}^{\infty}\left(\frac{(\kappa_1+1)\kappa_1}{\Omega_1}\right)^{j_1}\frac{1}{(j_1!)^2}\cdot$$

$$\cdot\frac{2(\kappa_2+1)}{\Omega_2 e^{\kappa_2}}\sum_{j_2=0}^{\infty}\left(\frac{(\kappa_2+1)\kappa_2}{\Omega_2}\right)^{j_2}\frac{1}{(j_2!)^2}\cdot$$

$$\cdot\frac{2(\kappa_3+1)}{\Omega_3 e^{\kappa_3}}\sum_{j_1=0}^{\infty}\left(\frac{(\kappa_3+1)\kappa_3}{\Omega_3}\right)^{j_1}\frac{1}{(j_3!)^2}\cdot$$

$$\int_0^{\infty} dx_2 \int_0^{\infty} dx_3 x_2^{-1-2j_1+2j_2+2j_1+2} x_3^{-1-2j_1+2j_3+2j_1+2}$$

$$\cdot e^{-\frac{\kappa_2+1}{\Omega_2}x_2^2-\frac{\kappa_3+1}{\Omega_3}x_3^2}$$

$$\cdot\frac{1}{2}\left(\frac{\Omega_1}{\kappa_1+1}\right)^{j_1+1}\gamma\left(j_1+1,\frac{\kappa_1+1}{\Omega_1}\frac{x^2}{x_2^2 x_3^2}\right). \qquad (4)$$

Rayleigh fading is a model for stochastic fading when there is no line of sight signal. Because of that it is considered as a special case of the more generalized concept of Rician fading. Rayleigh fading is obtained for Rician factor κ=0. For this reason, derived expressions for CDF of product of three Rician RVs can be used for evaluation a CDF of product of three Rayleigh RVs, also for CDF of product of two Rayleigh RVs and Rician RV, and CDF of product of two Rician RVs and Rayleigh RV. The obtained results can be used in performance analysis of wireless relay communication radio system with three sections in the presence of multipath fading. This means that derived CDFs are used for the next cases: 1) when Rician fading is present in all three sections ($\kappa_i \neq 0$, i=1,2,3), then 2) when Rayleigh fading is present in all three sections ($\kappa_1=\kappa_2=\kappa_3=0$), the next 3) when Rayleigh fading is present in two sections and Rician in one ($\kappa_1=\kappa_2=0$, $\kappa_3 \neq 0$), and 4) when Rayleigh fading is present in one and Rician fading in two sections ($\kappa_1=0$, $\kappa_2 \neq 0$, $\kappa_3 \neq 0$). A case with κ →∞ present the scenario without fading.

C. *Outage probability of Product of Three Rician RVs*

The outage probability is an important performance measure of communication links operating over fading channels. Outage probability is defined as the probability that information rate is less than the required threshold information rate Γ_{th}. Pout is the probability that an outage will occur within a specified time period:

$$P_{out}=\int_0^{\Gamma_{th}} p_x(t)dt, \qquad (5)$$

where $p_x(x)$ is the PDF of the signal and Γ_{th} is the system protection ratio depending on the type of modulation employed and the receiver characteristics [21].

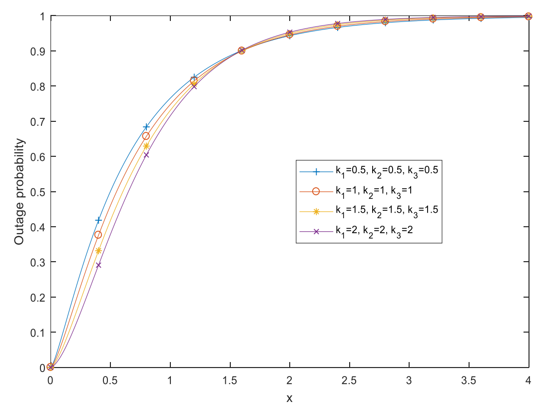


Figure 2. Outage probability of product of three Rician RVs versus signal envelope x for different values of Rician factor κ_I and signal power Ω=1.

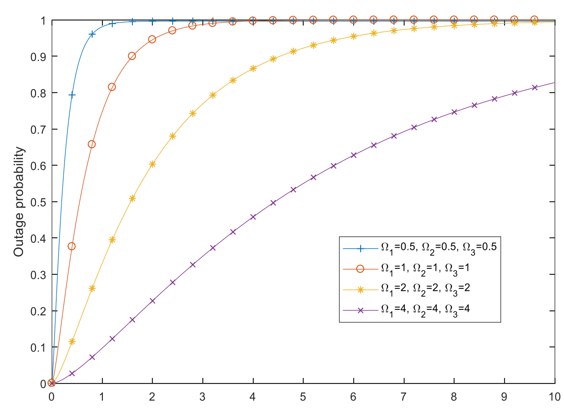


Figure 3. Outage probability of product of three Rician RVs depending on signal envelope for different values of signal power Ω_i and Rician factor κ=1.

Using (4), Pout can be expressed as:

$$P_{out} = F_x\left(\Gamma_{th}\right). \tag{6}$$

Plots of the outage probability, for different values of parameters, are shown in Figs. 2 and 3. The choice of parameters is intended to illustrate the broad range of shapes that the curves of the resulting distribution can exhibit. It is evident that performance is improved with an increase in Rician factors κ_i. Also, higher values of fading powers $\mathbf{\Omega}_i$ tend to reduce the outage probability and improve system performance, as it is expected.

III. The Second Order Performance of the Product of Three Rician Random Variables

Level crossing rate (LCR) and average fade duration (AFD) of the signal envelope are two important second-order statistics of wireless channel. They give useful information about the dynamic temporal behavior of multipath wireless fading channels.

A. LCR of Product of Three Rician RVs

Level crossing rate is one of the most important second-order performance measures of wireless communication system, which has already found application in modelling and design of communication system but also in the design of error correcting codes, optimization of interleave size and throughput analysis.

The envelope LCR is defined as the expected rate (in crossings per second) at which a fading signal envelope crosses the given level in the downward direction [4]. The LCR of RV tells how often the envelope crosses a certain threshold x [22]. We should determine the joint probability density function (JPDF) between x and $\dot{x}$, $p_{x\dot{x}}\left(x\dot{x}\right)$ first, then apply the Rice's formula [19, Eq. (2.106)] to finally calculate the LCR. LCR is defined as [2]:

$$N_x = \int_0^\infty d\dot{x}\,\dot{x}\,p_{x\dot{x}}\left(x\dot{x}\right). \tag{7}$$

LCR of product of three Rician RVs is derived in [23, eq. (20)]:

$$N_x = \frac{1}{\sqrt{2\pi}}\pi f_m \frac{\Omega_1^{1/2}}{\left(\kappa_1+1\right)^{1/2}} \cdot \frac{2\left(\kappa_1+1\right)}{\Omega_1} \cdot \frac{2\left(\kappa_2+1\right)}{\Omega_2} \cdot \frac{2\left(\kappa_3+1\right)}{\Omega_3} \cdot$$

$$\cdot\sum_{i_1=0}^{\infty}\sum_{i_2=0}^{\infty}\sum_{i_3=0}^{\infty}\left(\frac{\kappa_1\left(\kappa_1+1\right)}{\Omega_1}\right)^{i_1}\frac{1}{\left(i_1!\right)^2}\left(\frac{\kappa_2\left(\kappa_2+1\right)}{\Omega_2}\right)^{i_2}\frac{1}{\left(i_2!\right)^2}$$

$$\cdot\left(\frac{\kappa_3\left(\kappa_3+1\right)}{\Omega_3}\right)^{i_3}\frac{1}{\left(i_3!\right)^2}x^{2i_1+1}$$

$$\cdot\int_0^\infty dx_2\int_0^\infty dx_3\left(1+\frac{x^2}{x_2^4x_3^2}\frac{\Omega_2}{\kappa_2+1}\frac{\kappa_1+1}{\Omega_1}+\frac{x^2}{x_2^2x_3^4}\frac{\Omega_3}{\kappa_3+1}\frac{\kappa_1+1}{\Omega_1}\right)^{1/2}\cdot$$

$$\cdot x_2^{-2i_1-1+2i_2+1}x_3^{-2i_1-1+2i_3+1}e^{-\frac{\kappa_1+1}{\Omega_1}\frac{x^2}{x_2^2x_3^2}-\frac{\kappa_2+1}{\Omega_2}x_2^2-\frac{\kappa_3+1}{\Omega_3}x_3^2} \tag{8}$$

Last integral can be solved by using Laplace approximation theorem for solution the two-fold integrals solved in [24] through equations (22)-(29):

$$\int_0^\infty dx_2\int_0^\infty dx_3\, g\left(x_2,x_3\right)e^{\lambda f\left(x_2,x_3\right)} =$$

$$= \frac{\pi}{\lambda}g\left(x_{20},x_{30}\right)e^{\lambda f\left(x_{20},x_{30}\right)}\frac{1}{\left(B\left(x_{20},x_{30}\right)\right)^{1/2}}. \tag{9}$$

We give in this subsection some new graphs for normalized LCR of product of three Rician RVs depending on this product x with Rician factor κ_i and average power Ω_i as parameters of curves in Figs. 4 and 5.

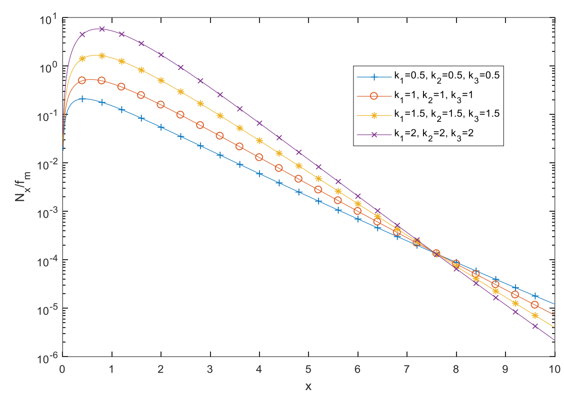


Figure 4. LCR normalized by f_m depending on signal envelope x for various values of Rician factor κ_i and signal power $\mathbf{\Omega}$=1.

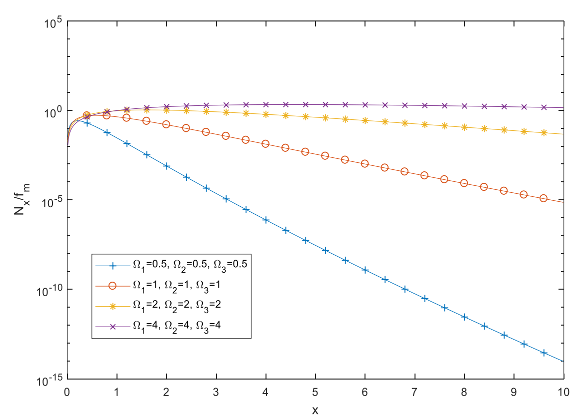


Figure 5. LCR normalized by f_m versus signal envelope x for various values of signal powers $\mathbf{\Omega}_i$.

LCR grows as Rician signal power increases. The impact of signal envelope power on the LCR is higher for bigger values of Rician factor κ_i. LCR increases with increasing of Ω_i for all values of signal envelope. The impact of signal envelope on the LCR is larger for higher values of the signal envelope when Ω_i changes. It is important bring to mind that system has better performance for lower values of the LCR.

B. AFD of Product of Three Rician RVs

Average fade duration measures how long a signal's envelope or power stays below a given target threshold derived from the LCR [4]. According to that, AFD is [25, eq. (9)]:

$$T_x(x) = \frac{P(x \le X)}{N_x(x)} = \frac{\int_0^X p_x(x)dx}{N_x(x)}. \tag{10}$$

The numerator is the cumulative distribution function of x from (4), and $N_x(x)$ is LCR given in (8) [26].

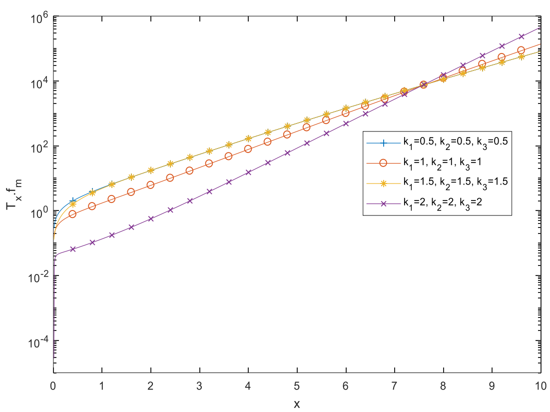


Figure 6. AFD normalized by f_m versus signal envelope x for different values of Rician factor κ_i and signal powers Ω_i=1.

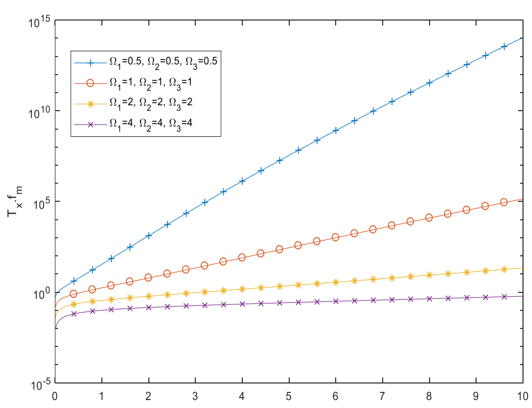


Figure 7. AFD normalized by f_m depending on signal envelope x for κ=1 and different values of signal powers Ω_i.

The normalized AFD ($T_x f_m$) of product of three Rician RVs is plotted in Figs. 6 and 7 versus signal envelope x. One can see that for higher values of κ_i and lower x, AFD has smaller values. Also, it is visible from Fig. 7 that AFD increases for all signal envelopes and lower Ω_i. The impact of Ω_i is bigger at higher envelopes.

IV. CONCLUSION

Due to transmit power limitations, the multi-hop communication in relay systems is introduced for improving the quality of transmission in cellular and ad hoc networks. These benefits of multi-hop relays are especially visible in rural areas with small population and low level of traffic density.

In this work, we presented previously determined formulas for the PDF and LCR and derived important expressions for CDF, Pout and AFD of the three-hop wireless relay system in the presence of Rician fading. This system output signal is the product of three Rician RVs.

Outage probability is defined as the point at which the receiver power value falls below the threshold (where the power value relates to the minimum signal or signal to noise ratio (SNR) within a cellular networks). It is said that the receiver is out of the range of Base Station in cellular communications. Average fade duration is used to determine how long a user is in continuous outage. This is important for coding design.

Based on the presented results it is possible to anticipate the behavior of the real wireless relay system in the presence of analyzed fading. Future works will introduce general fading distributions in consideration of three-hop relay systems' performance.

ACKNOWLEDGMENT

This article was realized under the projects: TR-33035 and III-44006 of the Ministry of Education, Science and Technological Development of the Republic of Serbia.

REFERENCES

[1] P. M. Shankar, Fading and shadowing in wireless systems, Springer, New York Dordrecht Heidelberg London. 2012, DOI 10.1007/978-1-4614-0367-8.

[2] G. L. Stüber, Principles of Mobile Communications, 2nd ed., MA, USA, Springer, 2001. ISBN 978-1-4614-0364-7

[3] M. K. Simon and M. S. Alouini, Digital communication over fading channels, (2nd ed.). New York, Wiley-IEEE Press. ISBN: 978-0-471-64953-3, 2004.

[4] A. Goldsmith, Wireless Communications, Cambridge University Press, 2005, DOI: https://doi.org/10.1017/CBO9780511841224

[5] A. Panajotovic, N. Sekulovic, A. Cvetkovic, and D. Milovic, "System performance analysis of cooperative multihop relaying network applying approximation to dual-hop relaying network", Int. J. Commun Syst. 2020; e4476, p. 1-10, https://doi.org/10.1002/dac.4476

[6] A. Kuhestani, M. T. Mamaghani, and H. Behroozi, "A new secure multi-hop untrusted relaying scheme", ArXiv, Corpus ID: 162184290, May 2019.

[7] D.-H. Kim, Y.-C. Ko, and S. Park, “Three-hop MIMO relaying systems in Gaussian broadcast channels”, 2nd International Conference on Signal Processing and Communication Systems, ICSPCS, Australia, Gold Coast, 15-17 December 2008. doi:10.1109/icspcs.2008.4813661

[8] C. Wang and D. Xu, “A study on burst error statistics and error modelling for MB-OFDM UWB systems”, IET Seminar on Ultra Wideband Systems, Technologies and Applications, 2006, p. 244-248, DOI: 10.1049/ic:20060518

[9] A. Abdi, K. Wills, H. A. Barger, M.-S. Alouini, and M. Kaveh, “Comparison of the level crossing rate and average fade duration of Rayleigh, Rice, and Nakagami fading models with mobile channel”, 52nd Vehicular Technology Conference IEEE VTS Fall VTC2000, Boston, MA, USA, pp. 1850-1857, DOI: 10.1109/VETECF.2000.886139

[10] J. M. Morris and J. L. Chang, “Burst error statistics of simulated Viterbi decoded BFSK and high-rate punctured codes on fading and scintillating channels,” IEEE Trans. Commun., vol. 43, pp. 695-700, 1995.

[11] A. J. Goldsmith and S. G. Chua, “Variable-rate coded M-QAM for fading channels", IEEE Trans. Commun., vol. 45, pp. 1218-1230, 1997.

[12] G. N. Onoh, T. L. Alumona, C. O. Ezeagwu, “Adaptive modulation techniques for capacity improvement of BER in WCDMA”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 4, Issue 9, September 2015, pp. 3537-3542.

[13] G.K. Karagiannidis ; N.C. Sagias ; T. Mathiopoulos, “The N*Nakagami fading channel model”, 2005 2nd International Symposium on Wireless Communication Systems, Siena, Italy, 5-7 Sept. 2005, pp. 185-189, DOI: 10.1109/ISWCS.2005.1547683

[14] I. Ghareeb and D. Tashman, “Statistical analysis of cascaded Rician fading channels”, International Journal of Electronics Letters, November 2018. doi:10.1080/21681724.2018.1545925

[15] D. Krstic, M. Stefanovic, R. Gerov, Z. Popovic, “Wireless relay system with two sections in κ-μ short term fading channel”, The Twelfth Iinternational Conference on Wireless and Mobile Communications, ICWMC 2016, Barcelona, Spain, Nov. 13 - 17, 2016, pp. 110 - 114.

[16] A. Cvetković, J. Anastasov, S. Panić, M. Stefanović, D. Milić,.”Performance of dual-hop relaying over shadowed Ricean fading channels”, Journal of Electrical Engineering, 2011, 62(4), pp. 244–248. doi:10.2478/v10187-011-0039-6

[17] D. Krstic, P. Nikolic, Z. Popovic, M. Stefanovic, “First and second order characteristics of wireless three-hop relay channel with presence of Rayleigh fading”, Journal of Telecommunications and Information Technology (JTIT), no. 2/2020, pp. 36-44, https://doi.org/10.26636/jtit.2019.130018

[18] D. Krstic, P. Nikolic, I. Vulic, S. Minic, M. Stefanovic, “Performance of the product of three Nakagami-m random variables”, Journal of Communications Software and Systems (JCOMSS), vol.16, no. 2, June 2020, pp. 122-130, Special Issue on Internet of Things: Hardware and Software Solutions, http://dx.doi.org/10.24138/jcomss.v16i2.989

[19] S. O. Rice, “Mathematical analysis of random noise”, Bell System Technical Journal, 23(3), 1944, pp. 282–332. doi:10.1002/j.1538-7305.1944.tb00874.x

[20] D. Krstic, P. Nikolic, Z. Popovic, S. Minic, and M. Stefanovic,”Moments of signals over wireless relay fading environment with line-of-sight”, accepted for presentation at SoftCom 2020, Hvar, Croatia, September 17-19, 2020.

[21] I. Trigui, A. Laourine, S. Affes, and A. Stephenne, “Outage analysis of wireless systems over composite fading/shadowing channels with co-channel interference”, IEEE Wireless Communications and Networking Conference, 5-8 April 2009, Budapest, Hungary

[22] W. C. Jakes, Microwave Mobile Communications. Piscataway, NJ: IEEE Press, 1994.

[23] D. Krstic, M. Stefanovic, M. M. B. Yaseen, S. Aljawarneh, P. Nikolić, „Statistics of the product of three Rician random processes with application”, International Conference on Data Science, E-learning and Information Systems 2018 (Data'18), Madrid, Spain, October 1-2, 2018. DOI: 10.1145/3279996.3280015

[24] J. L. Lopez and P. J. Pagola, “A simplification of the laplace method for double integrals. Application to the second appell function”, Electronic Transactions on Numerical Analysis, vol. 30, 2008.

[25] T. T. Tihung and C. C. Chai, “Fade statistics in Nakagami-lognormal channels”, IEEE Transactions on Communications, 1999, 47(12), pp. 1769–1772. doi:10.1109/26.809692

[26] X. Dong and N. C. Beaulieu, “Average level crossing rate and average fade duration of selection diversity”, IEEE Communications Letters, 5(10), 2001, pp. 396–398, doi:10.1109/4234.957373

Towards a Methodology for the Development of Routing Algorithms in Opportunistic Networks

Diego Freire
Dept. of Information and Communications Engineering
Universitat Autònoma de Barcelona
Barcelona, Spain
email: diego.freire@deic.uab.cat

Sergi Robles
Dept. of Information and Communications Engineering
Universitat Autònoma de Barcelona
Barcelona, Spain
email: sergi.robles@uab.cat

Carlos Borrego
Dept of Mathematics and Computer Science
Universitat de Barcelona
Barcelona, Spain
email: carlos.borrego@ub.edu

***Abstract*—This paper introduces a methodology for the development of routing algorithms that takes into consideration opportunistic networking. The proposal focuses on the rationale behind the methodology, and highlights its most important stages and components. It also discusses the importance of two core elements in the process of protocol designing: the scenario selection, based on essential characteristics, and the choice of standard evaluation metrics. As of now, there has been no common methodology for developing new routing algorithms, and this has led to proposals difficult to compare, to evaluate, and lacking a rigorous objectivity ensuring fairness. Thus, there is the urgent need to propose, agree, and use a common methodology for the development of routing algorithms.**

Keywords*—*Opportunistic networks; routing algorithms; development methodology; emulation systems.

I. Introduction

The efficiency and performance of a network depends completely on the routing algorithm. Nodes can be sparsely or densely distributed, there can be few or many messages, node buffers can be small or large, but at the end of the day, the responsibility of forwarding all messages from the source to the destination in the best way possible lies with the routing algorithm. Thus, the development of such protocols is of paramount importance for the sake of networks in general, and especially critical in challenged networks like opportunistic ones. In these last type of networks, nodes are irregularly distributed, not always accessible and message forwarding is only possible when there is a transient contact opportunity. In these conditions, the store, carry and forward strategy of Delay Tolerant Networking helps connecting the unconnected parts of the net.

Unfortunately, the process of developing new routing algorithms has not been in the focus of research, and this has led to disputable quality proposals, difficult to compare between them, and almost impossible to determine if they suit best for a given scenario. Although many proposals include simulated experiments repeated in several conditions, with different data sets, and even including very detailed network configurations, such as radio protocols, and interference models, they still lack the basic scientific approach allowing repeatability and comparison. It is true that many of these papers introduce the confrontation to other routing algorithms, but even in this case, the scenario selection and particular configuration is not guaranteed to observe, intentionally or not, a rigorous objectivity ensuring fairness. Moreover, few of these proposals present a final implementation showing its feasibility and allowing a realistic performance evaluation under real world conditions.

Traditional networks have an end-to-end path available to transmit messages between nodes, but in Opportunistic Networks, this end-to-end path may never exist, delays and disruptions are part of the behaviour; therefore, opportunistic strategies makes communication possible. In the development of a routing algorithm, evaluation and testing are done by some assumptions (e.g., unlimited resources, limited resources, a limited number of messages, unlimited creation of messages, among others). These assumptions seek to recreate a real-world OppNet, but complexity and variability increases within each characteristic studied.

Consequently, there is the urgent need to propose, agree, and use a common methodology for the development of routing algorithms that also takes into consideration extreme scenarios, such as opportunistic networking. The process has to go from the basic idea for the routing strategy, to the mathematical analysis, model, simulation, software implementation of the algorithm, emulation, and finally the application of the routing strategy, testing real code in real scenarios. In this paper, we get grips with the problem, and introduce the basic rationale for such a methodology, highlighting its most important stages and components, and discussing the importance of two core elements in the process of protocol designing: scenario selection, based on essential characteristics, and standard evaluation metrics. We expect this methodology to faster the adoption

 ISBN: 978-1-61208-794-8

of a common scientific approach to the development of new routing algorithms, and to give firm leverage in the production of high quality routing algorithms for OppNet.

The rest of the paper is structured as follows. Section II introduces the state of the art on opportunistic networks, evaluation strategies and development methodologies. Section III presents the methodology in our proposal. Then, scenarios and metrics are shown in Section IV. Finally, Section V discusses our contributions and implications.

II. Related Work

In this Section, we study the state of the art of the development of routing algorithms in the opportunistic networks field, the evaluation strategies and methodology used in development of new opportunistic routing algorithms

A. Opportunistic networks

An opportunistic network [1], also known as OppNets [2], is a set of mobile devices commonly called nodes that exchange information between them exploiting direct communication opportunities to perform an end-to-end transfer of data. Nodes communicate with each other even if an end-to-end route never exist [3]. Furthermore, nodes are not supposed to possess or acquire any knowledge about the network topology. With the growth of the use of mobile devices in recent years, opportunistic networks have become a significant field of research. Opportunistic networks allow a flexible and highly dynamic connection between the nodes [4]. Any node can join or leave the network at any time.

The applications of opportunistic networks [5] are cellular network offloading, communication in challenged areas, censorship circumvention and proximity-based applications and Internet of Things (IoT) [6], among others. Topology network is continuously changing due to the constant movement of the nodes, and the communication routes between senders and receivers are neither direct nor static. This communication capability allows the use of opportunistic networks in new applications. Before opportunistic networks, applications based their operation on an end-to-end connection path, however, when such connection is not possible, opportunistic networks present a solution, since the information is sent ”opportunistically” hop by hop between source to destination using the ”Store-Carry-and-Forward” approach [7].

B. Evaluation strategies in opportunistic routing algorithms

A standard methodology that allows the evaluation of routing algorithms in the OppNets field does not exist. Nevertheless, the nonexistence of a comparing method does not mean that a comparison is not possible.

One of the main ways of evaluating opportunistic routing algorithms is measuring their performance when sending information from a source to a destination. Some authors model message dissemination performance by analysing first the behaviour of the OppNet when some characteristics of the network vary, such as density, size of the messages, duration of the contacts, etc. [8].

Regarding the use of datasets for network behaviour simulation, and according to [9], most authors use several common scenarios like Haggle [10], MIT [11] or Cambridge [12]. Finding good scenarios to evaluate routing algorithms is not easy. The elevated cost of deploying real test-beds and the non-existence of a suitable simulator accounting for all real characteristics make it really difficult to find adequate traces to perform realistic simulations [9].

C. Methodology in the development of new opportunistic routing algorithms

A small part of the research community that works on challenged networks, such as opportunistic networks has pointed out the necessity of finding new methodologies in the development of new opportunistic routing algorithms. Their concern is focused on involving the engineering process in all stages between an original network proposal and its validation in real applications. The problem is that a lot of networks research proposals in this context rely solely on simulations to validate the proposed protocols without going any further.

The authors of studies like [13], draw attention to the fact that network decisions, such as routing or delivery ones are rarely implemented in real network platforms. Additionally, if they are, the validation of the proposed code is usually performed at a very small scale. That is why, there has been an enormous effort from this part of the research community on developing new emulation platforms to help with this problem. By using emulation tools, demanding scenarios can be tested and provide a a lightweight emulation solution that bridges the gap between pure simulation and real-world experimentation.

III. Methodology for developing routing algorithms

Using a sensible, sound methodology is indispensable to get good routing algorithms. This methodology has to observe the basic scientific method, allowing repeatability, fair comparison, and common scenario representation. In this Section we propose the basic steps of the process of developing new routing algorithms fulfilling the aforementioned requirements, and discuss about the selection of the test scenarios and performance metrics for comparison.

A. Methodology stages

The methodology has seven well differentiated stages, as shown in Figure 1:

1) Conception: First it comes the initial idea behind the algorithm, the conception of the mechanisms. This is normally triggered by some essential feature of the scenario, such as high node density, or by a particular theory, such as the history of encounter of nodes and its transitivity.

2) Model: After the initial stage of conception, the idea must be reified into a particular mathematical model, which can then be analyzed formally.

3) Analysis: Once the proposal is modeled, it can be analysed. During this analysis, the mechanisms and procedures can be checked, some theoretical results can be obtained, and basic limitations can be identified.

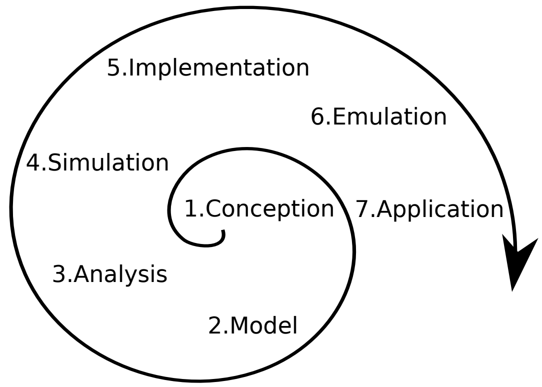


Figure 1. Methodology for developing routing algorithms consisting of seven stages.

4) Simulation: The next stage is simulation. In a simulator, the model can be tested in a given set of scenarios. Eventhough these scenarios involve datasets that come from the real world (e.g., real traces from vehicles or people), or even if the simulator simulates very accurately all network protocols involved, the model under evaluation is usually executed based on pseudo-code. This does not prove that the system being designed can eventually be deployed and used for real. Results obtained through simulation can be deceptive, creating a misleading feeling of scientific correctness. Indeed, as observed in [14], the credibility of simulation results tends to decrease as the use of simulation increases.

5) Implementation: The final validation of a routing algorithm should always be based on real full-featured code (accounting for example for memory management or concurrency issues), rather than on the pseudo-code used in simulations. In this stage, a code is produced so that the algorithm can be used on a real scenario. The implementation itself shows the feasibility of the algorithm.

6) Emulation: Testing real code in real conditions can be difficult and tricky, especially when these situations may involve the mobility of hundreds of nodes during hundreds of hours. Emulation is an approach that helps with this respect, allowing to run real code in tightly controlled (and repeatable) conditions. This stage is the link between a proof-of-concept implementation and the deployment of a software that is useful in the real world and behaves as predicted.

7) Application: The last stage of this methodology is testing the routing algorithm in a real environment, with real devices and users. This is the ultimate test that shows how the designed algorithm behaves in the real world and allows to evaluate.

The application of the methodology should not be strictly sequential. Some of the work in one stage can help to improve some of the previous stages. For example, the results of the analysis can help modifying the model to take into account a new variable, or the emulation results can help to detect and correct bugs of the implementation.

Applying a methodology like the one described is necessary, but not enough to produce good quality routing algorithms. There are two elements that have also to be considered: the scenarios, and the performance metrics. The simulation and emulation stages need some scenarios, including the position of nodes during a time window and the messages that are sent along with other information. This is important for two reasons. In the first place, these scenarios have to be public to reproduce the results at any time, and to fairly compare different routing algorithms in the same conditions. Secondly, the scenarios need to be representative of the real environments the routing algorithm is going to be used in. The second element to be considered is the performance metrics of the algorithm. Again, there are two main reasons for this. The first one is that to evaluate how good is a routing algorithm for a given scenario, there have to be some evaluation functions. These functions, or metrics, will tell how the network performs when this routing algorithm is in operation, and thus can determine for which scenarios it is more appropriate. The second reason is that these metrics allow a direct comparison to other protocols for the same scenario.

IV. SCENARIOS AND METRICS IN OPPORTUNISTIC NETWORKS

Different scenarios and metrics are generally used in articles to measure the performance of Routing Algorithms. As it is difficult to reproduce real-world conditions, the use of scenarios tries to create a model of them, assuming performance will be similar. To be in the safe side, many papers use several scenarios to show the algorithm has a large scope of applicability. However, articles use to pay little or no attention to the selection and definition of these scenarios, neglecting the importance they deserve in the significance of the results.

A. Components

Scenarios of OppNet consist of a set of nodes and their positions during a time frame. When analysing the behaviour of a routing algorithm on a scenario, more details have to be provided, such as a set of messages (with recipients and size), and the communication range of the nodes.

Nodes in an OppNet normally communicate wirelessly. Nodes can receive, drop, store, carry and forward messages. When a node receives a message, the decision whether a message must be stored, carried, dropped or forwarded is made by the routing algorithm. The routing algorithm makes the decision of which nodes a message is forwarded to.

As we talk before scenarios are a representation of real-world, therefore their characteristics must help to reproduce certain real-world behaviour. Among others, the characteristics of a scenario may include the set of positions, granularity, node range, node density, and buffer size. For the sake of simplicity, we can consider the scenario as the set of nodes, the set of messages and the contacts between nodes:

$$S = (Nodes, Messages, NodeContacts) \quad (1)$$

 ISBN: 978-1-61208-794-8

B. Selection of scenarios

As we have seen, scenarios play a very important role for the development of routing algorithms. As diversity is a key factor to guarantee representation of real world applications, different sources of scenarios have to be considered. They can be synthetically created, which allows to force some scenario characteristics, like a given node density. They can also come from real world traces captured in live situations. As suggested by Kotz et al. in [15], create a new scenario is expensive and challenging. The Community Resource for Archiving Wireless Data At Dartmouth (CRAWDAD) allows sharing data sets across the scientific community. The real-world data help us to understand the behaviour of real users. Common well-known scenarios already used in literature [16], like Cambridge, Info5, Taxis, MIT or Haggle could also be used as possible scenarios. Within the many scenarios that have different characteristics, scenario selection is a crucial part of the development of a new opportunistic routing algorithm. The output performance of some scenarios is the same, even that those scenarios do not share characteristics.

Because it is impossible to test the routing algorithms in all possible scenarios, making a selection of scenarios is required. This process have to be scientifically justified, to be representative enough and avoid any possible bias. Just having different traces that generate different results without analyzing the entire spectrum of action of the OppNet comprehensively would result insufficient. These fine selection of scenarios will act as a representation of the whole scope of opportunistic networks.

C. All-in-One scenario trap

A valuable scenario aims to be a good representation of reality. This representation must introduce as many elements as the real event contains, but this could end up into an unrealistic task due to the number of characteristics involved. Our research found more than seventy characteristics used as tuning settings of the so-called scenarios. Given those seventy characteristics, even limiting the operativity of each characteristic as binary, the number of the scenarios is unrealistic to manage. Therefore, modelling a scenario requires a balance between simplification and real-world accuracy has a direct implication of usability. Not every characteristic must be taken into account. Those characteristics that are not involved in the scenarios are going to be present in the other phases of the routing algorithm development. Oversimplification of characteristics could lead to a useless representation of the phenomena, and the results are not useful. Our proposal claims that instead of build an "All-in-One" scenario, the development of a set of different scenarios, where those scenarios must give different performance results with the same algorithms.

D. Performance metrics

In a scenario, messages have to be delivered from the origin to the destination taking advantage of the communication opportunities. To achieve this, in this process, several copies of the same message are generated. Messages can be successfully delivered, they can be dropped, for example if there is not enough buffer for them, or they may not reach their final destination, for example because their life time is over. A metric is a function that gives the measure of a certain property of a given scenario, such as message drop, latency, node inter-contact time, delivery ratio, overhead ratio, delivery cost, average number of hops, wastage index or average delay, among others.

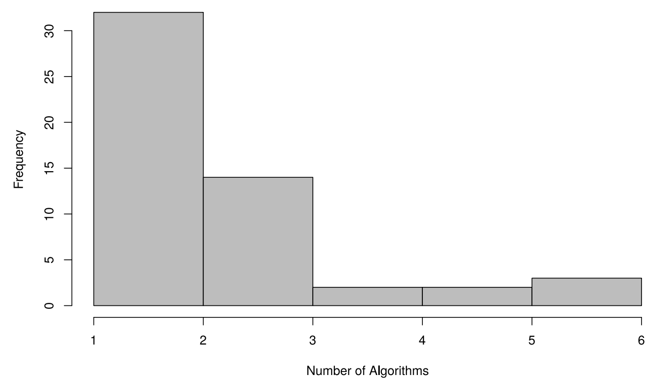


Figure 2. Number of compared-to routing algorithms

The evaluation function of an algorithm in a scenario provides the set of some metric measurements for that scenario, as shown in (2). The result of this evaluation is multidimensional, for having just one number to compare different algorithms does not allow an accurate comparison. An algorithm may be better for a specific metric, but worse for another one. It is the final application that will determine which algorithm is the most appropriate, and therefore it is convenient to preserve the whole set of metric results to have a better idea on how the algorithm behaves.

The evaluation function can be represented as:

$$M = M_1, M_2, ..., M_n$$

$$Eval(A, S, M) = (M_1(A, S), M_2(A, S), ..., M_n(A, S)) \quad (2)$$

where $Eval$ is the evaluation function, A is the routing algorithm, S is the scenario, M is the set of metric functions, and M_i is the measurement of the metrics.

Metrics should always refer to the same measurable properties, thus all proposals have to use exactly the same names for the metrics to avoid confusion.

E. Routing comparison

Our research shows how the performance comparison has been carried out so far when a new opportunistic routing algorithm has been presented; and how these practices could lead up to unfair comparisons. We studied more than 50 opportunistic routing algorithms.

A comparison helps to evidence the improvement in the performance of a given task. Figure 2 shows the number of comparisons founded in the papers on routing algorithms in the literature. Then, Figure 3 is a cloud graph where edges indicate that the two routing algorithms connected are directly compared in some paper. This graph emphasizes the number of comparisons of a routing algorithm, The bigger the size of the font, the more times an algorithm has been compared to.

From the literature on routing algorithms, the information shown in Figure 2 and Figure 3 reaffirms our concern about a fair comparison. We found that approximately a 62% of the algorithms tests their performance with one or two algorithms when they are presented. On the other hand, less than 5% of the reviewed algorithms present a comparison with 6 algorithms. No algorithm which is compared with more than 6 others has been found.

In Epidemic routing, when a message needs to be routed from a source to a destination, the algorithm sends the message to all of their reachable neighbours. The algorithm does not have to make any decision whether to send a message or not. Having that in mind, the implementation of an Epidemic algorithm is not difficult at all. Figure 2 shows that most of the literature makes less than 2 comparisons and Figure 3 indicates the Epidemic routing is the most compared-to algorithm. That means that the comparison is centred around Epidemic routing and that routing algorithms are not been compared between them. Moreover, the few algorithms used in the comparisons are those that are implemented in traditional simulators. This is probably due to fact that the scientific community is paying more attention to the simplicity of the experimentation design rather than to the scientific soundness.

Our approach is that every algorithm could be evaluated in a fairway. That means, be able to compare apples with apples.

The use common evaluation function (as defined in (2)) in the analysis of an algorithm in a scenario provides a deterministic outcome, thus avoiding intentional or unintentional bias. With a methodological performance evaluation, we can pick the best algorithms of our interest.

We know that opportunistic networks are a challenging field; therefore, the traditional way to develop routing algorithms is not enough to go from the idea to the application.

V. Discussion

When a new routing algorithm is proposed in the field of opportunistic networking, the proposal uses its own evaluation metrics and scenarios. Thus, even though these proposals normally compare their protocol to others, the testing environment, chosen scenarios, metrics and conditions do not guarantee that the comparison is totally fair. It is very easy to, unintentionally, create a bias favouring their own proposal just by selecting a scenario with some specific characteristics for which the algorithm has been designed to take advantage. In most cases, reproducing the results of a given proposal is practically impossible because the full scenario data is not publicly available, the way of applying the metrics is not completely clear, or simply because the implementations (or

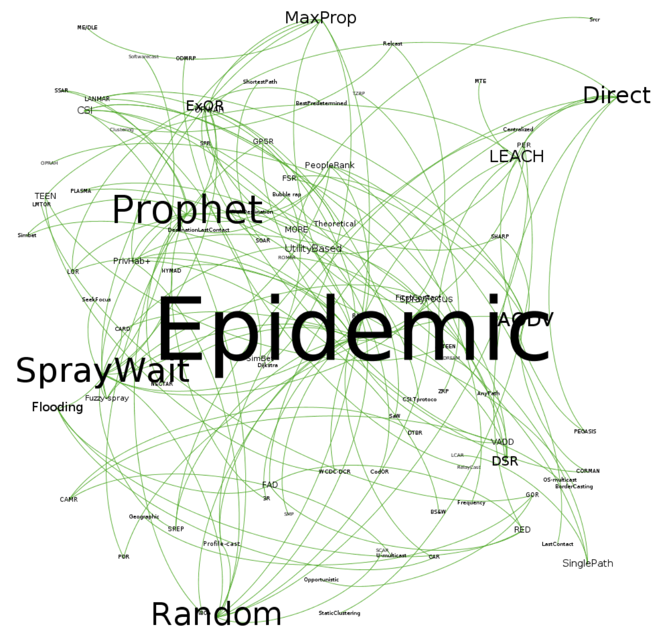


Figure 3. Cloud graph of routing algorithms comparison, edges indicates a direct comparison between a pair of routing algorithms in a paper

models of the protocol) are not given. As suggested by Bajpai et al. in [17], the research on computer networks is more and more accepting research proposals that are non-reproducible as long as they appear plausible to the manuscript reviewers. We agree with this study on the importance and challenges on reproducibility.

This situation applies to routing algorithms in general, but is particularly notorious in the case of opportunistic networks, where there is more variety of scenarios and conditions. This does not facilitate at all the selection of a good routing algorithm for a certain application, for example, and the creation process of new protocols is as well weakened for no validated references are available to fairly compare them to other proposals.

A way of alleviating these effects and giving better prospects to the (useful) development of new routing algorithms in ooportunistic networking is by using a methodology like the one presented in this paper. This can decisively help on the difficult task of starting a cultural change on routing algorithm development, proposal evaluation, and algorithm selection.

VI. Conclusions

In this paper, we have presented a methodology for the development of routing algorithms in Opportunistic Networking based on seven stages. Following this methodology, the development of new routing algorithms will improve , increasing their quality and fair comparison to others. Additionally, we have discussed the importance of two core elements in the

 ISBN: 978-1-61208-794-8

process of protocol designing: the scenario selection and the choice of standard evaluation metrics.

ACKNOWLEDGMENT

This work is partly funded by Secretaria de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT, ECUADOR), by the Catalan AGAUR 2017SGR-463 project, and by the Spanish Ministry of Science and Innovation TIN2017-87211-R project.

REFERENCES

[1] J. Dede, et al. ”Simulating Opportunistic Networks: Survey and Future Directions”. IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1547–1573, 2018. https://doi.org/10.1109/COMST.2017.2782182

[2] C. Borrego, et al. ”A mobile code bundle extension for application-defined routing in delay and disruption tolerant networking.” Computer Networks, vol. 87, pp. 59-77, 2015

[3] C. M. Huang, K. C. Lan, and C. Z. Tsai. ”A survey of opportunistic networks. Proceedings” - International Conference on Advanced Information Networking and Applications, AINA, pp. 1672–1677, 2008. https://doi.org/10.1109/WAINA.2008.292

[4] R. Kaur, (2017). ”Optimal Technique for Information Uphold due to discontinuous Communication on AD Hoc Mobile Network”. GADL Journal of Invention in Computer Science and CommunicationTechnology, vol. 3, no. 6, pp. 2455–5738, 2017.

[5] S. Trifunovic, S. T. Kouyoumdjieva, B. Distl, L. Pajevic, G. Karlsson, and B. Plattner. A decade of research in opportunistic networks: Challenges, relevance, and future directions. IEEE Communications Magazine, vol. 55, no. 1, pp. 168–173, 2017. https://doi.org/10.1109/MCOM.2017.1500527CM

[6] M. Cuka, D. Elmazi, M. Ikeda, K. Matsuo, and L. Barolli. ”IoT Node Selection in Opportunistic Networks: Implementation of Fuzzy-based Simulation Systems and Testbed”. Internet of Things, vol. 8, pp. 100105, 2019. https://doi.org/10.1016/j.iot.2019.100105

[7] Dede, J. et al. ”Simulating Opportunistic Networks: Survey and Future Directions”. IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp.1547–1573, 2018. https://doi.org/10.1109/COMST.2017.2782182

[8] E. Hernández-Orallo, M. Murillo-Arcila, C. T. Calafate, J. C. Cano, J. A. Conejero, and P. Manzoni. ”Analytical evaluation of the performance of contact-Based messaging applications”. Computer Networks, vol. 111, pp. 45–54, 2016. https://doi.org/10.1016/j.comnet.2016.07.006

[9] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz. ”Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges”. IEEE Communications Surveys and Tutorials, vol. 14, no. 2, pp. 607–640, 2012. https://doi.org/10.1109/SURV.2011.041911.00093

[10] A European Union funded project in Situated and Autonomic Communications, retrieved 07, 2020. https://ica1www.epfl.ch/haggle/

[11] N. Eagle, A. Pentland and D. Lazer, ”Inferring social network structure using mobile phone data”, Proceedings of the National Academy of Sciences, vol. 106 no. 36, pp. 15274-15278, 2009.

[12] J. Leguay, A. Lindgren, J. Scott, T. Friedman, J. Crowcroft, P. Hui, CRAWDAD data set upmc/content, 2006. Retrieved 07, 2020. http://crawdad.cs.dartmouth.edu.

[13] A. Sánchez-Carmona, F. Guidec, P. Launay, Y. Mahéo, and S. Robles. ”Filling in the missing link between simulation and application in opportunistic networking”. Journal of Systems and Software, vol. 142, pp. 57-72, 2018. https://doi.org/10.1016/j.jss.2018.04.025

[14] S. Kurkowski, T. Camp, and M. Colagrosso. ”MANET simulation studies: the incredibles”. ACM SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no.4 , pp. 50-61, 2005. https://doi.org/10.1145/1096166.1096174

[15] D. Kotz and T. Henderson. Crawdad: A community resource for archiving wireless data at dartmouth. IEEE Pervasive Computing, vol. 4, no. 4, 12-14, 2005, https://doi.org/10.1109/MPRV.2005.75

[16] N. Magaia, C. Borrego, P. Pereira, and M. Correia, ”PRIVO: A privacy-preserving opportunistic routing protocol for delay tolerant networks.” 2017 IFIP Networking Conference (IFIP Networking) and Workshops, pp.=1-9, 2017

[17] V. Bajpai, M. Kühlewind, Mirja, J. Ott, J. Schönwälder, and A. Sperotto, and B. Trammell. ”Challenges with reproducibility”. Proceedings of the Reproducibility Workshop 2017. 2017. https://doi.org/10.3929/ethz-b-000197662

Considerations for Designing Private and Inexpensive Smart Cities

Jasmine DeHart
Department of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
Email: dehart.jasmine@ou.edu

Corey E. Baker
Department of Computer Science
University of Kentucky
Lexington, KY, USA
Email: baker@cs.uky.edu

Christan Grant
Department of Computer Science
University of Oklahoma
Norman, Oklahoma, USA
Email: cgrant@ou.edu

***Abstract*—The expectation of people and futurists is that all respectable cities will become Smart Cities in the near future. Two main barriers stand in the way of the evolution of cities. First is cost, the transformation into a smart city is expensive (e.g., between $30 Million and $40 Billion) and only a few cities are able to obtain the resources required for upgrades. Second, many citizens equate the data collection and surveillance of smart city technology with aggressive infringements on privacy. In this paper, we describe how citizens, city planners, and companies can develop smart cities that do not require crippling loans and are respectful of privacy.**

Keywords–smart city; privacy; networks.

I. INTRODUCTION

Ubiquitous technology has long been an expectation of the 21st century. Recently, the concept of a Smart City has led cities, developers, and citizens to pursue idyllic improvements to municipal infrastructure. Smart city designs tend to require Internet of Things (IoT) devices to be connected in order to retrieve the data generated by the devices. Unfortunately, significant costs are incurred when deploying sensors equipped with 5G or WiFi connectivity due to data subscription fees [1] [2]. As the number of cities that want to become "smart" increases, innovative ways of transforming a conventional city into a smart city need to be investigated. Aspiring smart cities are predicated on the belief that socioeconomic impact will yield a return on investment for smart cities, but financiers have been apprehensive [3].

While innovations in technology continue, citizens are critical about how unvetted smart cities can violate intrinsic rights [4]. People are inventing methods to disguise themselves from surveillance systems using fashionable masks [5]. Citizens also depend on other products to curtain themselves from other devices, such as smart speakers [6] [7]. However, laws are consistently being passed to ensure the responsibility of the city or company protects the privacy of the citizens [8] [9].

In remainder of this paper, we introduce and discuss the concepts of low-cost and privacy-enabled smart cities. In Section 2, we focus on defining what a smart city is and the requests of the top seven applicants that were apart of the 2015 Smart City Challenge [10]. In Section 3, we discuss the large monetary costs smart cities have invested to become "smart" along with some opinions on how to reduce cost. In Section 4, we discuss the infringements of privacy that smart cities produce and then, we propose innovative ways cities can protect their citizens. Lastly, we conclude by summarizing the insights and future direction of this research.

II. HOW CAN A CITY BECOME "SMART"?

Establishing what technologies create a smart city can include many intricate components. To define the essence of a Smart City, we start by establishing the basic universal technologies that all smart cities require. In 2015, the United States Department of Transportation announced the Smart City Challenge which asked cities in America to create an integrated, smart, and efficient transportation system built on data, applications, and technology in an effort improve the lives of its citizens [10]. Figure 1 displays U.S. cities that are currently smart cities or are interested in becoming "smart" (the circle area denotes the population size). Of these, the Smart City Challenge received 78 applicants describing what a smart city looked like for their community.

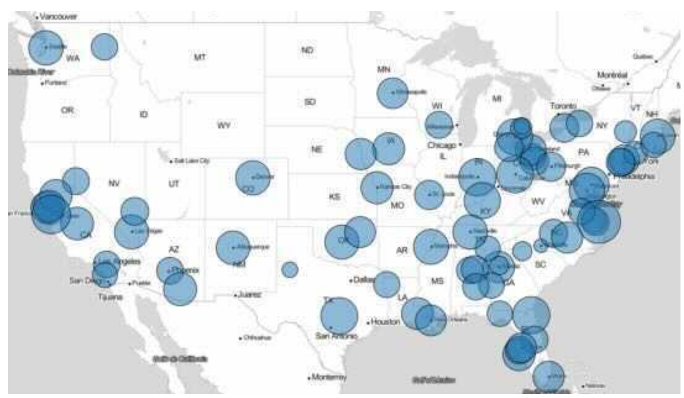


Figure 1. Current and potential smart city locations in the United States.

The list of technologies have been derived from the top seven applications from the Smart City Challenge. From this challenge, the seven cities were chosen as finalist include: Columbus (Ohio), Austin (Texas), Denver (Colorado), Kansas City (Missouri), Pittsburgh (Pennsylvania), Portland (Oregon), and San Francisco (California). Following this competition, these finalist serve as a foundation for cities hoping to become smarter. These cities request several technologies and components, such as:

- Electric vehicle charging stations
- Electric/autonomous public transportation vehicles
- Connected vehicles using a smart grid
- User mobile applications
- Traffic signaling priority

To integrate these technologies, the cities use sensors, video, Global Positioning Systems (GPS), and radio signals from pedestrians, vehicles, and equipment. These cities also use these video and GPS feeds for license plate recognition and to track crime related incidents. The goal of becoming a smarter city revolves around connecting under-served communities to opportunities, decreasing health disparities, reducing air pollution, and increasing the mobility of citizens by relieving congestion of roadways.

Assisting low socioeconomic and disabled citizens has risen to the forefront of smart city development strategies. In an effort to make these advancements more inclusive of those communities, the smart cities have proposed the use of:

- *Smart kiosks* enable advanced payment options by incorporating additional features, such as braille and voice feedback
- *Electronic signs* provide visual and audio cues to pedestrians
- *Autonomous car sharing* allows commuters first and last mile transportation with a reduction in costs
- *Information screens* provide real-time transportation updates through audio and video

With the incorporation of these additional technologies, we see these cities become more inclusive and smarter for all. On top of an already costly smart city, these specialized technologies raise an additional cost along with continually maintaining all aspects of these technologies.

III. Low-Cost Smart Cities

Smart City projects can be extremely expensive to deploy and manage. Cities around the world such as San Diego, New Orleans, London, and Songdo have either proposed or invested in Smart City projects that cost between \$30 Million and \$40 Billion. In addition to the cost of deploying and maintaining the IoT devices themselves, a significant portion of the expense is a result of providing Internet connectivity via 5G or WiFi to those devices. These costs are a major barrier to the widespread deployment of Smart City technology and the social benefits that may ensue from that technology [11].

To alleviate the costs, opportunistic communication, such as Delay Tolerant Networks (DTNs) can be used as a backbone for Smart City communication to facilitate data that does not have real-time Quality of Service (QoS) constraints. DTNs traditionally provide opportunistic networking connections in areas with little to no infrastructure. Messages are delivered with some delay which is directly correlated with the layout, density, and mobility of nodes in the network [12] [13]. Recognizing that some data are needed in real-time, edge-computing can be utilized as long as the placement of internet-connected nodes are optimized in the network. For data that can tolerate delays, the natural movement of people and vehicles through a city to transfer data between nodes. In this way, the citizens become an integral part of the smart city network itself.

In order for low-cost Smart Cities to flourish and DTNs as backbone to be practical, both the technology questions related to the devices and the network itself, as well the social aspects of how people and vehicles move through a city must be addressed. For almost 20 years there has been a substantial amount of research in opportunistic communications and delay tolerant networks; unfortunately real-world deployments traditionally fall short of their simulated counterparts [14]. Related efforts, [13], [15]–[22], have proven the ability to deliver messages when connections are intermittent, but generally are limited to performing within simulation environments [23].

IV. Privacy-Enabled Smart Cities

With the use of smart city technologies, how does a city ensure privacy and security for its citizens? Cities will become a 24 hour hub for collecting information about the mobility and efficiency of transportation, but also personally identifying information of its' travellers [24]. In the Smart City Challenge [10], the applicants describe the possible risks and mitigation strategies with the deployment of these cities. From these concerns, we focus on the risks associated with the citizens in those environments. The main concerns for smart city citizens revolve around data sharing, individual privacy, system security, data privacy, and data management. In Table I, we explore each smart city and if these smart city risks will be addressed in the development of their city.

TABLE I. OVERVIEW OF THE MAIN SMART CITY CONCERNS FOR CITIZENS SELF-IDENTIFIED BY THE CITIES.

City	Data Sharing	Individual Privacy	System Security	Data Privacy	Data Management
Columbus, OH	–	–	–	–	–
Austin, TX	√	–	√	√	√
Denver, CO	–	–	√	√	–
Kansas City, MO	√	√	√	–	–
Pittsburgh, PA	–	√	–	√	√
Portland, OR	√	–	–	√	√
San Francisco, CA	√	√	–	–	–

Each city (rows) either discusses (√) or does not mention (–) the privacy risk of a technology (columns). Data sharing and data privacy concerns are addressed by the majority (4 of 7) of the cities. Individual privacy, system security, and data management are each addressed by three of the cities. In Table II, we reviewed these Smart City proposals and assessed a score based on a Likert Scale (Excellent, Average, Poor) from these five categories (Data Sharing, Individual Privacy, System Security, Data Privacy, & Data Management). From the proposal and discussion, a city will receive:

- Excellent: The proposal has thorough discussion about the risks and mitigation strategies related to topic and a solid plan of action.
- Average: The proposal has moderate to little discussion about the risks and mitigation strategies related to topic and a general plan of action.
- Poor: The proposal has little to no discussion about the risks and mitigation strategies related to topic and no plan of action.

Columbus is the only city without a risk analysis in their proposal. This city will develop their plan during the implementation of their city, but would this be enough? Immediately after winning, Columbus created the Smart City Program Office to assess possible risks and mitigate them. Of the finalists, none of these cities provide a detailed description of the protection they will provide their citizens in their proposals. To mitigate the proposed risks these cities seek to: (1) implement standards from government and industry, (2) anonymize or mask sensitive personal data, and (3) partner with cyber-security experts and government.

TABLE II. RATING OF PRIVACY DISCUSSION BY CITY.

City	Data Sharing	Individual Privacy	System Security	Data Privacy	Data Management
Columbus, OH	Poor	Poor	Poor	Poor	Poor
Austin, TX	Poor	Poor	Excellent	Excellent	Excellent
Denver, CO	Poor	Poor	Poor	Average	Poor
Kansas City, MO	Poor	Average	Excellent	Poor	Poor
Pittsburgh, PA	Poor	Poor	Poor	Average	Poor
Portland, OR	Average	Poor	Poor	Average	Average
San Francisco, CA	Poor	Poor	Poor	Poor	Poor

Beyond security breaches and attacks, what protection will these cities use to ensure the privacy of those who want to remain anonymous in an "always on" city? Researchers have investigated the concerns of privacy leaks and the types of privacy leaks on social media [25]. These privacy leak concerns can be expected in a smart city where citizens are continually being monitored. To help cities protect their citizens, we propose the use of a visual mitigation library used for videos and images based on existing literature [26]. This work provides a foundation for several mitigation techniques used for social media networks, however these same technologies can be implemented to protect the citizens from surveillance concerns and privacy issues. Beyond the citizen's concern for anonymity or protection of minors, there is a concern for the type of information that is leaked in a public setting.

A. *ViperLib: Mitigation Library*

We seek to expand this work as a foundation for the need of mitigation techniques in video surveillance. Everyday people purchase items with their credit or debit cards, carry identification, or use keys (virtual and physical passcodes). This type of sensitive content will be captured in those videos and image feeds [27] [28], with the use of a redaction spectrum we can ensure that content will not be leaked to others. Studies have shown that the use of obfuscation methods [29]–[31] can protect individual privacy.

To address this concern, we suggested the deployment of the *ViperLib*. This mitigation library will allow the Smart Cities to choose how and where they want to integrate this technology. As proposed by [26], mitigation techniques can be integrated into mobile applications, servers, IoT devices, and comprehensive systems. Techniques, such as obfuscation (e.g., adversarial noise, blurring, blocking), interception, and blind vision can be integrated into this library easily ready for use. The library can also facilitate active engagement strategies for alerting authorized personnel about pertinent privacy concerns and suggesting the possible mitigation strategies for that visual content. These types of alerting strategies are similar to *Chaperone Bot or Privacy Patrol* from previous works [26]. The *ViperLib* open-source library can be integrated into existing "off-the-shelf" packages. Citizens can select the privacy protection features that must be integrated into deployed systems. Such libraries can provide safety, security, and peace of mind to the citizens that reside in those areas.

V. Conclusion & Future Work

In summary, this paper argued that Smart Cities have the capability to be both private and inexpensive in deployment and for long term sustainability. During planning and implementation of these cities, officials along with citizens should further consider the high cost and privacy concerns associated with their development choices. The need for privacy mitigation in Smart Cities extends from the protection of personally identifying information to the choice of anonymity and protect of minors. Beyond the deployment of the *ViperLib*, we proposed the use of DTNs to lower the cost of Smart Cities and allow citizens assist the in the transmission of data across the city. Deploying traditional IoT infrastructure is prohibitively expensive for most cities and expanded developments introduces privacy risks. However, low-cost smart cities and privacy-enabled technologies can achieve the goals of smart cities while allowing citizens to feel secure and protected.

Future research considers the potential effects of security for cyber-physical systems in real IoT deployments. To do this, we will collaborate with Louisville, Kentucky, a Smart City Applicant, to discuss future strategies and deployment plans for *ViperLib* as part of NSF Grant (#1952181).

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1952181.

References

[1] J. Paradells, C. Gómez, I. Demirkol, J. Oller, and M. Catalan, "Infrastructureless smart cities. Use cases and performance," *2014 International Conference on Smart Communications in Network Technologies, SaCoNeT 2014*, pp. 1–6, 2014.

[2] E. Max-Onakpoya *et al.*, "Augmenting cloud connectivity with opportunistic networks for rural remote patient monitoring," in *2020 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2020, pp. 920–926.

[3] Deloitte, "The challenge of paying for smart cities projects," Deloitte, Tech. Rep., 2018, last accessed on 09/01/2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-ps-the-challenge-of-paying-for-smart-cities-projects.pdf

[4] J. E. Smith, "As San Diego increases use of streetlamp cameras, ACLU raises surveillance concerns," Aug. 2019, last accessed on 09/01/2020. [Online]. Available: https://lat.ms/33AzG7I

[5] A. Harvey, "Cv dazzle: Camouflage from computer vision," *Technical report*, 2012.

[6] J. Morse, "There's a privacy bracelet that jams smart speakers and, hell yeah, bring it," last accessed on 09/01/2020. [Online]. Available: https://mashable.com/article/bracelet-jams-alexa-smart-speakers/

[7] Y. Chen, H. Li, S.-Y. Teng, and S. N. Z. Li, "Wearable microphone jamming," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2020, pp. 1–12.

[8] C. Doctorow, "The case for ... cities that aren't dystopian surveillance states," *The Guardian*, Jan. 2020, last accessed on 09/01/2020. [Online]. Available: https://www.theguardian.com/cities/2020/jan/17/the-case-for-cities-where-youre-the-sensor-not-the-thing-being-sensed

[9] H. Devlin, "AI systems claiming to 'read' emotions pose discrimination risks," *The Guardian*, Feb. 2020, last accessed on 09/01/2020. [Online]. Available: https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks

[10] U. D. of Transportation, "Smart city challenge," Jun 2017, last accessed on 09/01/2020. [Online]. Available: https://www.transportation.gov/smartcity

[11] O. Madamori, E. Max-Onakpoya, C. Grant, and C. Baker, "Using delay tolerant networks as a backbone for low-cost smart cities," in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2019, pp. 468–471.

[12] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 55.

[13] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay-tolerant networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 11, pp. 1576–1589, 2011.

[14] C. E. Baker, A. Starke, T. G. Hill-Jarrett, and J. McNair, "In vivo evaluation of the secure opportunistic schemes middleware using a delay tolerant social network," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 2537–2542.

[15] R. Cabaniss, S. S. Vulli, and S. Madria, "Social group detection based routing in delay tolerant networks," *Wireless networks*, vol. 19, no. 8, pp. 1979–1993, 2013.

[16] P. Costa, C. Mascolo, M. Musolesi, and G. P. Picco, "Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 5, pp. 748–760, 2008.

[17] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant manets," *Mobile Computing, IEEE Transactions on*, vol. 8, no. 5, pp. 606–621, 2009.

[18] W. Gang, W. Shigang, L. Cai, and Z. Xiaorong, "Research and realization on improved manet distance broadcast algorithm based on percolation theory," in *Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on*. IEEE, 2012, pp. 96–99.

[19] W.-j. Hsu, D. Dutta, and A. Helmy, "Csi: A paradigm for behavior-oriented profile-cast services in mobile networks," *Ad Hoc Networks*, vol. 10, no. 8, pp. 1586–1602, 2012.

[20] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Service Assurance with Partial and Intermittent Resources*. Springer, 2004, pp. 239–254.

[21] M. Musolesi and C. Mascolo, "Car: context-aware adaptive routing for delay-tolerant mobile networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 2, pp. 246–260, 2009.

[22] A. K. Gupta, J. K. Mandal, and I. Bhattacharya, "Comparative performance analysis of dtn routing protocols in multiple post-disaster situations," in *Contemporary Advances in Innovative and Applicable Information Technology*. Springer, 2019, pp. 199–209.

[23] A. Picu and T. Spyropoulos, "Dtn-meteo: Forecasting the performance of dtn protocols under heterogeneous mobility," *IEEE/ACM Transactions on Networking*, vol. 23, no. 2, pp. 587–602, 2014.

[24] R. Sánchez-Corcuera, A. Nuñez-Marcos, J. Sesma-Solance, A. Bilbao-Jayo, R. Mulero, U. Zulaika, G. Azkune, and A. Almeida, "Smart cities survey: Technologies, application domains and challenges for the cities of the future," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, p. 1550147719853984, 2019.

[25] J. DeHart, M. Stell, and C. Grant, "Social media and the scourge of visual privacy," *Information*, vol. 11, no. 2, p. 57, 2020.

[26] J. DeHart and C. Grant, "Visual content privacy leaks on social media networks," *arXiv preprint arXiv:1806.08471*, 2018.

[27] R. Hoyle, R. Templeman, D. Anthony, D. Crandall, and A. Kapadia, "Sensitive lifelogs: A privacy analysis of photos from wearable cameras," in *Proceedings of the 33rd Annual ACM conference on human factors in computing systems*. ACM, 2015, pp. 1645–1648.

[28] M. Korayem, R. Templeman, D. Chen, D. Crandall, and A. Kapadia, "Enhancing lifelogging privacy by detecting screens," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 4309–4314.

[29] T. Orekondy, M. Fritz, and B. Schiele, "Connecting pixels to privacy and utility: Automatic redaction of private information in images," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 8466–8475.

[30] Y. Li, N. Vishwamitra, B. P. Knijnenburg, H. Hu, and K. Caine, "Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, 2017, pp. 1343–1351.

[31] T. E. Boult, "Pico: Privacy through invertible cryptographic obscuration," in *Computer Vision for Interactive and Intelligent Environment (CVIIE'05)*. IEEE, 2005, pp. 27–38.

 ISBN: 978-1-61208-794-8