An address allocation protocol for ad hoc networks through pollen dispersion algorithms

Giuseppe Roa Osorio
Department of Systems Engineering
National University of Colombia.
Bogotá Colombia
groao@unal.edu.co

Joaquín F. Sánchez
Software Engineering Unit and TIC
Manuela Beltran University
Bogotá, Colombia
joaquin.sanchez@docentes.umb.edu.co

Juan P. Ospina
Department of Systems Engineering
National University of Colombia
Bogotá, Colombia
jpospinalo@unal.edu.co

Jorge E. Ortiz
Department of Systems Engineering
National University of Colombia
Bogotá, Colombia
jeortizt@unal.edu.co

***Abstract*—Due to the huge constellation of appliances and devices that will be connected to the Internet in the coming years, dealing with the task of identifying the receivers of hundreds of messages, represents a fundamental challenge for the future telecommunication networks. In this paper, biologically inspired computing is used to propose a simple but effective solution to deal with the problem of addressing in large-scale communication systems in which machine-to-machine interactions are a fundamental part of the operating conditions. We introduce the main aspects of our proposal and present three simulation scenarios in NS-3 to evaluate the performance the model.**

***Index Terms*—Machine-to-machine, IPv6, Ad hoc networks, Self-configuring networks, Address allocation.**

I. Introduction

The vertiginous increase of devices capable of interchange data has supposed critical challenges to the current telecommunication networks [1]. How to deal with the amount of traffic generated? How to identify, within the constellation of devices, the receiver of a message? How to manage the amount of signaling required to support the TCP/IP architecture? Is it needed to endow of resources simple appliances to support the stack of IPv6? These are some of the questions that arise when imagining the design of future networks.

The massification of mechanisms dedicated to data interchange in daily devices has been one of the pillars in the conception of Internet of Things (IoT). However, in many cases, the interaction of communications is not between humans but between machines with specific purposes. This kind of interactions, called machine-to-machine (M2M), supposes an important change in a series of conditions that should be managed by the network protocols to enable the communication with the rest of the existing networks [2].

An interesting approach to this paradigm is the Ad-Hoc networks, in which the human interactions to establish the connection is not needed, and there is a high degree of nodes autonomy. However, several current Ad-Hoc implementations are limited to stand-alone networks. There would be a great potential if this kind of systems had the ability to connect to the Internet [3], [4].

In some cases, a node is used as a gateway to the Internet, supporting inside connectivity with specific routing protocols for Ad-Hoc networks and, simultaneously, connectivity between sub-networks to the Internet. In implementations of mobile Ad-Hoc networks (MANETs), an option implies to support the TCP/IP architecture directly over the network [5].

Given the extensive integration of new highly heterogeneous devices, establishing a scheme that universally identifies each node, even the simplest ones in operation, would lead to an increase of networks complexity and therefore, an increase in costs that would be counterproductive for a global distribution and implementation of IoT.

II. Mobile Ad-Hoc Networks (MANET) dynamics

Mobility, power consumption limitations, links instability and nodes dynamic behavior in Ad-Hoc networks cause several network events. These events must be studied to guarantee that self-configuring address allocation protocols operate under these conditions. Following, the most important events are mentioned [6]–[9]:

Initialization: it corresponds to the network starting mechanism. It can be independent or in group:

Independent: a node can start independently. It self-allocates an address and is the network "origin" to which other nodes can connect gradually (See Figure 1a).

Group: almost simultaneously a node group starts its link functions creating cooperatively a network (See Figure 1b).

Partitioning: it is the dynamic network division into several sub-networks. Then, by multiple causes, one or more nodes leave the network inducing address leaks. There are two types of partitions:

978-1-7281-1614-3/19/$31.00 ©2019 IEEE

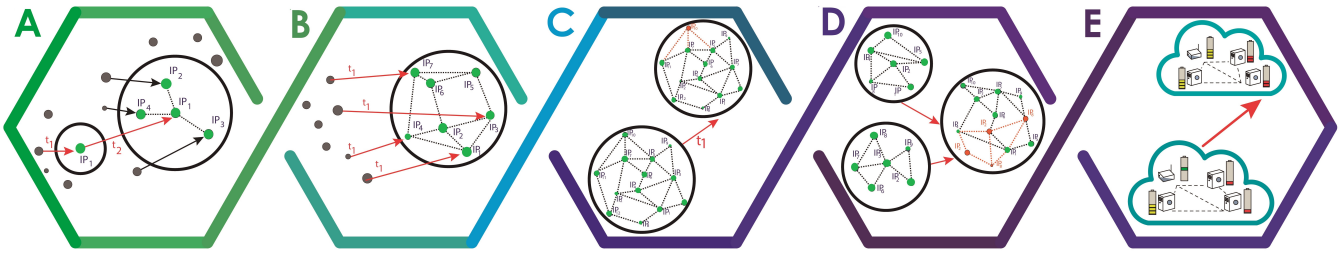

Figure 1. MANET dynamics. A) Independent initialization. B) Group initialization. C) MANET partition. D) MANETs migration. E) Mobile clouds. Gray dots represent inactive nodes. Green dots active nodes networked. Red dots active nodes with an address conflict. Red arrows denote time transitions.

Graceful Departure: it occurs when a node informs its neighbors about its departure from the network before leaving. The nodes store this event. Then, they respond with a confirmation liberating the node and its address.

Graceless Departure: a node can leave the network fortuitously, therefore it is required to detect these sudden departures. In this case, each node must store the address of its neighbors to inform the rest of the network if there is a lacking node (Refer to Figure 1c).

Migration of several MANETs: it is the unification of more than two networks into a new, bigger one, that can contain address conflicts (Figure 1d). In this scenario, an option is to use a duplicate address detection method (DAD). Each time a node selects a new tentative IP, the DAD determines the availability of this IP. Every node with a valid IP participates in this procedure. The uniqueness is verified through the broadcast of test messages and address conflict notifications (ACN). After n responses, if the node has not received an ACN, it assumes the IP. In MANET migrations a DAD could lead to an overflow of messages.

Mobile Clouds: a mobile cloud is a cooperative arrangement of dynamically connected nodes sharing opportunistically resources [8] (See Figure 1e). In this definition, Fitzek establishes that, among nodes, there is a social relationship that defines the willingness to cooperate and shape the way of cooperation that takes place in a cloud. It is *dynamic* because wireless channels are prone to temporal and spatial fluctuations, as well as, to changes in nodes. A *node* is any device with capabilities to connect to each other. The nodes are *connected* directly (peer to peer) or logically (through overlay networks). A *resource* is any shareable entity/means available in the system or embedded in the nodes that, according to the *opportunities* as they arise, are distributed to take a mutual advantage.

A. Address Allocation requirements in MANETs

In general terms, the requirements that have to fulfill an address allocation scheme in MANETs are [10]–[12]:

- Each node must obtain an address dynamically. The duplicate addresses have to be corrected in short lapses.
- The node permanence in a network is not guaranteed, in this sense, when a node leaves the network its address must be liberated, in such a way, other new nodes can use it. It means, periodical synchronization of the topology condition in the system.
- Only authorized nodes can belong to the network.
- It should minimize the amount of signaling required.

According to the requirements, the most convenient metrics for evaluating the performance of an addressing scheme in MANETs are [10], [12], [13]:

- *Dynamic address allocation:* The nodes have to obtain addresses without static or manually settings.
- *Overhead:* The amount of signaling required by the protocol to its operation.
- *Latency:* Average time needed to allocate an address to a requester node.
- *Sturdiness:* The scheme must adapt without inconvenient to the networks dynamic (failure tolerance, message losses, fluctuation in nodes lifetime, etc.).
- *Scalability:* The protocol performance cannot be degraded by increasing the network size.
- *Space address use:* The protocol has to assign the available address space uniformly because it is possible that limiting to only a portion the duplicity occurrences could be more frequent affecting the overall performance.

B. Schemes adapted to MANETs

Gateway Selection (ASLBGS): In the approach Adaptative Steady Load Balancing Gateway, once a functional MANET is established it looks for the best gateway connected to the Internet using path load balancing optimizing TTL and advertisement periodicity values through a genetic algorithm [14].

Prophet: this protocol follows a ”best effort” approach in which each node has autonomy to self-assign an IP in a predetermined range by randomly generating a number using an f(n) function. The function can take as a seed a random value. When a new node joins the network, it can take as seed an amount granted by another node. This mechanism has a low latency and a minimum overhead, however, the conflicts of duplicity, even in broad address ranges, can be a constant. As an alternative, this protocol can make use of a DAD mechanism, but it incurs in latency increments [13].

Virtual Address Space Mapping: in this mechanism a node assumes the role of an address authority that maintains static information of a certain number of nodes in the MANET,

storing a virtual space of addresses to assign to new nodes. The technique maps one point of the virtual space exactly to each new node. There are certain roles that at one point assume the nodes: Allocator, stores the address space, each space is disjointed between them, so there are no duplications. Initiator, intermediate node between Allocator and Requester that exchanges messages with them. The requester, node requesting an address. Normal, the remaining nodes available on the network [15]. The Requester makes a broadcast to its neighbors by looking for an Initiator that drives the request to the nearest Allocator. Allocator can designate other nodes to assume this same role and thus balance as MANET grows.

ManetConfig: in this mechanism, the nodes maintain an additional table that accommodates pending address requests. When a new node joins the network, it makes a broadcast of the requirement to its neighbors, in turn, they execute a query through the network requesting for an available address. It requires an ACK positive indicating address availability as well an ID to detect events such as partitions or migrations is related to the address provided. The protocol detects partitions by not receiving the ACK of all nodes; it deletes from the table stored in each node the occupied spaces of nodes that do not respond. When a migration occurs, the nodes exchange their used address lists in such a way that duplications can be detected. This scheme has a high tolerance to the loss of messages and the occurrence of network events. However, although in principle latency is low and overhead is reasonable, both metrics are susceptible as networks grows [16].

III. Machine-to-Machine communications and Bio-inspired models

The traditional networks were developed to transmit meaning information for human beings, where the high reliability, the interference resistance, and the high speeds are principal objectives in the design. These networks comprise several devices with significant computational resources that allow the implementation of architectures like TCP/IP. Due to the advent of IoT and the increase of appliances available to exchange information, the M2M communications occupy a fundamental role for the successful implementation of IoT by proposing a different paradigm in network architectures [1], [17], [18].

Devices capable of recording and transmitting information will be present in everyday appliances, and they will be produced in outstanding volumes [19], [20]. However, the primary function of each object will not change and consider that all these simple devices will be provided with computational resources (processor, memory, etc.) that allow implementing the entire stack of TCP/IP, would have an adverse impact on IoT expansion and IoT economic viability.

A. Key cost areas in Networks

Previously, the large-scale deployment of networking technologies has been intimately linked to economic factors. In networks, there are three main areas of increasing costs:

Hardware and Software: The portion of devices with sufficient computational and energy resources to support TCP/IP will be obscured by the large number of simple, resourceless sensors that have never been connected to the network. $Intel$ estimates that adding large-scale computing resources plus Wifi or Ethernet interfaces and additional heat sinks may involve an increase of up to 50 dollars in the final price of the devices [17]. On the other hand, opting for simple modulation interfaces, broadcast interfaces or simple reception technologies may suffice. In certain cases, these alternatives can be embedded in silicon integrated so the final cost could increase by only 1 dollar or less.

Surveillance and Management: Modifying networks to cope with growing traffic is utterly inefficient from an economic perspective. Although the payload is low in IPv6, in a context of millions of devices, it would correspond to a huge waste of bytes and especially to massive congestion in the network. There are thousands of producers of all types of applications, so it would be inefficient to expect a centralized entity to assign MAC addresses to all devices or to identify and audit a device in a constellation of trillions of nodes. Much of the information will be redundant and will only have ”local” meaning. In this scenario, to mitigate costs, one must appeal to the specialization of networks, individual autonomy, and localized effects.

Security: Contrary to the *Metcalf's* law, in the IoT to communicate several nodes on the ”edges” of networks without affinity or common context would provide zero utility-value and would represent an increase in costs and risks both of Failures as security. The greatest potentiality would be to increase the degree of intelligence and the capacities of the network without resorting to loading each node with such capabilities. Without the need for each node to have global reach and to lack in memory or other computational resources, devices would not be the target of unwanted infiltration [21].

There are no architectures of human communications networks that fit the size of the IoT avoing a massive waste of resources. Because of that, the approach must take into account bio-inspired systems such as social insect colonies, pollen propagation process or cellular communication where visual, auditory and chemical signals are emitted and interpreted by individuals in the ecosystem [17].

B. Bio-inspired models

Using mechanisms inspired by existing processes in nature has allowed us to obtain efective solutions for problems whose complexity increases according to the number of variables involved. In the IoT, it would be functional to apply principles from proccesses such as the following:

1) Pollen - Seeds Dispersion: : In spermatophytes, the flow of genetic information is carried out by the dispersion of pollen or seeds. Pollen holds a pair of cells containing the male genes of the plant that produces it; Additionally, it has a typical size and shape that differs from species to species and is usually microscopic. Pollen is dispersed by vectors like the wind or water currents or by interactions with insects reaching large areas and transporting pollen of various species [22].

From this process, it is possible to retrieve unusual characteristics applicable to M2M communications. Information signals (pollen) are characterized by being very light and mono-purpose, easy to carry by the vectors involved. The messages have the characteristic of being self-classified by type and content externally (in form and size). It is possible to conclude that the communication is receiver oriented, since the plants that receive the pollen are the ones that "decide" if they ignore the genetic message received or if they start pollination; This occurs without the need for some management or other external interaction. In this way, it is possible that similar groups of individuals end up exchanging information intentionally or accidentally. There is no retransmission mechanism simply because it is not necessary since the messages are so straightforward and easy to transmit that it is preferred to carry thousands of redundant information packets [17].

2) Ant's colony: : Ants possess limited cognitive abilities; however, they can collectively find the shortest path between food sources and the colony. Scout ants randomly walk around the settlement, if they discover a source of food they return directly to the nest releasing pheromones on the way. Ants that are nearby will be attracted and will tend to follow the same path, releasing more pheromones. If there are two or more options, a greater number of ants will travel in less time, so that the shorter road will become more attractive.

It is interesting to analyze that the ants use the environment as a means of communication by indirectly exchanging information between them, and it is the global state of the swarm that describes the work developed. The information is transferred only in a local scope, only those close agents will have access and will be involved in the process. The system is self-organizing, and its success arises from positive feedback. These are characteristics of a meta-heuristic, multi-agent, probabilistic system where incomplete or imperfect information accompanied by limited computational capabilities must optimize the solution to a problem [23], [24].

IV. Proposed model

To address the problem, we use the architecture described by $Intel$ in [17] composed of three functional levels or roles that nodes can assume in the network. The protocol uses the roles to designate different tasks and adjust to the MANETs dynamics, like in insect swarms. Defining, when and which node has to change its role, is a determining factor for the operation of this scheme. This mechanism leaves aside the error checking, routing, and high-level addressing in the end devices because it is not needed.

First level - Terminal devices: Characterized by lack of computational resources, they have very specific purposes in which they exchange small amounts of information that, according to the nature of the application, will have a certain degree of inherent redundancy. The devices can be grouped according to the type of application in such a way that, although they are in different terminal ecosystems, the information will be relevant only for those nodes interested in the data.

Second level - Propagation nodes: Characterized by having greater computational resources with which, apart from executing their particular purpose, they can assume the role of propagating vector of the information they receive. The information is transmitted to terminal nodes, to other propagators or to integrating nodes running basic rules. Additionally, they execute routines to gradually group the nodes according to affinities (external markers) and perform a proactive self-discovery of other propagators or integrators. They can also function as traditional gateways to TCP/IP; In this sense, you can group information from one or several terminal nodes and consolidate it into IPv6-like packets to send it to the Internet.

Third level - Integrating nodes: They have high computational resources which allow them to execute complex tasks. They perform the analysis of high-level information, extraction of patterns, control, and management of the Human-Machine interface. In practice, these nodes will have the IPv6 stack and will be devices available on the Internet; However, according to the demand, nodes that fulfill certain criteria can assume a role of a local integrating node in a MANET which would allow granting a greater level of "intelligence" to the network.

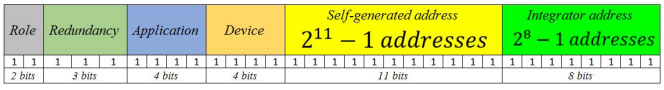

Figure 2. Proposed datagram. This structure was thought, in order to, reduce the amount of signaling required.

This scheme uses a datagram model (See Figure 2) that must be constructed to exchange information. The packets use external identifiers that allow to self-classify the message (Refer to Table I). In this way, 2 bits corresponds to the role that currently assumes the node, 4 bits to the nature of the application, 3 bits for the percentage of inherent redundancy of the information exchanged by the application, 4 bits to identify the type of device, 11 bits intended for a random number self-generated by the node and that would function as its address. This datagram lacks destination address field since the receiver will be the one who decides, according to external IDs, whether a message is relevant to him or not like in pollen/seed distribution. Also, the packet can contain 1 byte that allows identifying the propagator or integrator node associated to the terminal node.

The behavior of the model is described by the equations 1, 2 for address space available for terminal and propagator, 3 for the max number of nodes in the network with a single integrator and 4 for the minimum amount of nodes that should assume the propagator role:

$$AS_{terminal} = 2^{11+r+a+d} - 1 \quad (1)$$

$$AS_{propagator} = 2^{8+r+a+d} - 1 \quad (2)$$

$$Max(n) = [AS_{propagator} * AS_{integrator} * \gamma] \quad (3)$$

$$Min\#Prop(n) = \frac{\#Terminals}{AS_{propagator}} + [D(n)(r+a+d)] \quad (4)$$

Where:

r corresponds to the different redundancy levels.
a is the number of different applications.
d the number of different kinds of devices.
γ is a safety design factor.
$D(n)$ is the network density function.

The application ID comprises the main areas of industrial appliances in IoT. The type of devices takes into account the principal objects that could assume the Terminal role. Through the redundancy is possible to define network strategies in order to avoid processing unnecessary information.

Table I
EXTERNAL IDENTIFIERS.

Role	ID	Application	ID	Kind of Device	ID
Undefined	00	Other	0000	Other	0000
Terminal	01	IT Networks	0001	TAG	0001
Propagator	10	Surveillance	0010	Pump	0010
Integrator	11	Emergency Services	0011	Motor	0011
Redundancy	**ID**	Tracking	0100	Valve	0100
2%	000	Retail - Stores	0101	Alarm	0101
4%	001	Retail - Hospitality	0110	Sensor- Implants	0110
6%	010	Transport- Vehicular	0111	Environmental	0111
10%	011	Non-Vehicular	1000	Sensor- Security	1000
18%	100	Distribution	1001	Wearable	1001
31%	101	Resource-Automation	1010	Generators	1010
55%	110	Agricultural	1011	Actuators	1011
98%	111	Health-care	1100	Vehicle	1100
		Energy Management	1101	Lighting	1101
		Home automation	1110	Battery	1110
		Entertainment	1111	Fuel Cell	1111

The protocol is described by a finite state machine shown in Figure 3, that illustrates the different transitions that a node can suffer according to the network conditions and its own limitations. Any node that initiates its network functionalities will be sent to the 'INIT' state, in which it will consult neighboring nodes for the existence of one that is assuming the role of 'Propagator'. Depending on this response, and the computational resources available, the node will behave as Terminal or Propagator. In this way, the protocol supports group or independent initialization.

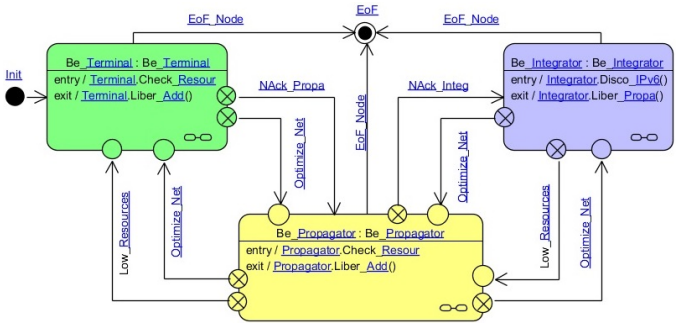

Figure 3. Protocol Finite States Machine. Colors represent the roles: green for "Terminal", yellow for "Propagator" and blue for "Integrator".

If there is any Propagator, the transition to the terminal node states is made. The node selects a propagator, self-allocates an address per the defined standard, requests authorization from the propagator to link to it, validates that its address is not repeated and then initiates the continuous sending of packets per the nature of the same. If a fault exists, either in the Terminal or in the Propagator, the protocol returns the operation to the initial state to select a new Propagator or that the node assumes the role of the same.

In case there are no Propagators, the node assumes this role if it has enough computational resources. It self-allocates a one-byte address and begins to be the axis of the organization of the nodes that wish to disseminate its information. In case there are nodes integrators, the Propagator is responsible for assembling IPv6 packets and sending them to the Integrator.

An integrating node would give the system a greater ability to "learn" since having the computing capacity could be able to extract patterns from different sub-nets, suggest reorganizations to the propagators and extrapolate information of value on the behavior of devices with similar features.

Under this protocol, the addresses only make sense in a local scope that corresponds to the one in which the propagating node has dominion. The load-balancing measures of the propagators themselves reduce the probability of duplicate addresses. The "leak" of terminal nodes has no impact on the system. At the moment in which a propagtor fails, the nearest propagator identifies the absence of said node, then it will assume all the load that had the previous one, and according to its resources will designate one or several new propagators.

V. MODEL VALIDATION

We implement the model in NS-3 and define three different scenarios, detailed in Table II, in order to validate the model.

Table II
SIMULATION SCENARIOS

Parameters	Scenario 1	Scenario 2	Scenario 3
Simulation Time	100 s	100 s	100 s
Nodes	50	80	100
Mobile Nodes	50%	40%	30%
Mobility Model	Randomwaypoint	GaussMarkov	GaussMarkov
Failure Nodes	3	5	8
Resources Distribution	Uniform	Exponential	Gamma
Traffic Model	Poisson	Self-similar	Self-similar

We run 281 replicates for each scenario and consolidate the results concerning two metrics: Uniform addressing space use (Figure 4) and Overhead vs Ipv6 (Figure 5).

The simulations shows that the protocol tend to assignate 37% more addresses than physical nodes in the network, this is a trade-off that the protocol must assume in order to tolarate the MANET dynamics. Acording to that the γ parameter of equation 3 must be at least 0.63 in physical implementations.

Concerning the Overhead, it is remarkable that when the traffic has the characteristics of M2M appliances the operational percentage range of our protocol is significative less in comparison with IPv6. The Median of the Overhead is 8 times

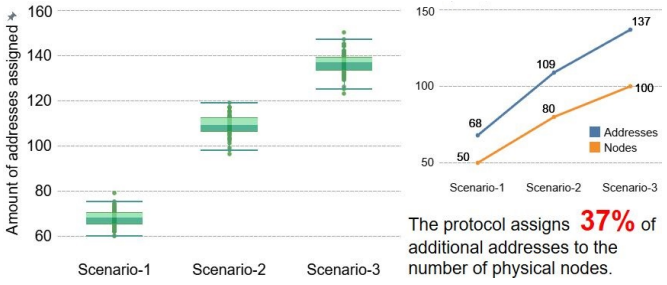

Figure 4. Results of Uniform Addressing Space Use

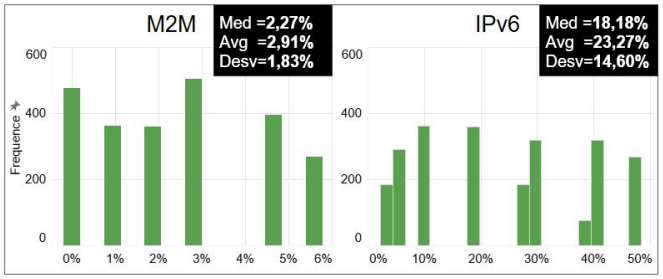

Figure 5. Results of %Overhead against IPv6

lower (2.27% vs 18.18%). In the long term, this represents a huge reduction in signaling for M2M traffic and thus a competitive advantage.

VI. Conclusions

The proposed model resorts to self-organization, understood as the collective capacity of "learning", to reorganize and balance the network in order to be more efficient in addressing and disseminating information packets as well as more robust against MANET dynamics.

Opting for mechanism inspired by fundamentals presented in nature processes for the message diffusion could lead into a more efficient option in economics terms and complexity.

Implementing the IPv6 stack, even in very resource-constrained devices, would result in an overhead on terminal devices, as well as, on network elements since they should support a significant amount of signaling traffic. In this sense, the proposed model would reduce in great magnitudes the overhead by adjusting more appropriately to the characteristics of the machine-to-machine communications.

Clustering nodes by affinities, employing low payload address allocation schemes and with only "local" meaning correspond to more efficient options for networks based on M2M communications.

The sensor networks is an ideal scenario for the application of this algorithm of address assignment, since it has the conditions for the existence of a highly interconnected environment, hoping to improve the process of establishing and maintaining the operation of the network.

References

[1] D. Minoli, *Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications*. Wiley, 2013.

[2] M. Cullinen, "Machine to machine technologies: Unlocking the potential of a $1 trillion industry, carbon war room research report," The Carbon War Room AT&T, Tech. Rep., february 2013.

[3] T. Truong-Huu, C. Tham, and D. Niyato, "A stochastic workload distribution approach for an ad hoc mobile cloud," in *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, Dec 2014, pp. 174–181.

[4] D. M. Shila, W. Shen, Y. Cheng, X. Tian, and a. X. S. Shen, "Amcloud: Toward a secure autonomic mobile ad hoc cloud computing system," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 74–81, April 2017.

[5] W.-Q. Xu and T.-J. Wu, "Tcp issues in mobile ad hoc networks: Challenges and solutions," *Journal of Computer Science and Technology*, vol. 21, no. 1, pp. 72–81, 2006.

[6] Y. Sun and E. M. Belding-Royer, "A study of dynamic addressing techniques in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 4, no. 3, pp. 315–329, 2004.

[7] S. Sarkar, T. Basavaraju, and C. Puttamadappa, *Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications, Second Edition*. CRC Press, 2013.

[8] F. H. Fitzek and M. D. Katz, *Mobile Clouds: Exploiting Distributed Resources in Wireless, Mobile and Social Networks*, 1st ed. Wiley Publishing, 2014.

[9] J. P. Ospina López and J. E. Ortiz Triviño, "Estimation of a growth factor to achieve scalable ad hoc networks," *Ingeniería y Universidad*, vol. 21, no. 1, pp. 49–70, 2017.

[10] V. Sachan, S. Srivastava, and P. Singh, "A survey on ip address assigment in a mobile ad hoc network," *International Journal of Computer Science and Information Technologies*, vol. 6, no. 3, pp. 2541–2544, 2015.

[11] M. Mohsin and R. Prakash, "Ip address assignment in a mobile ad hoc network," in *MILCOM 2002. Proceedings*, vol. 2, Oct 2002, pp. 856–861 vol.2.

[12] L. J. Garca Villalba, J. Garca Matesanz, A. L. Sandoval Orozco, and J. D. Mrquez Daz, "Auto-configuration protocols in mobile ad hoc networks," *Sensors*, vol. 11, no. 4, p. 3652, 2011.

[13] H. Zhou, L. M. Ni, and M. W. Mutka, "Prophet address allocation for large scale manets," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2, March 2003, pp. 1304–1311 vol.2.

[14] R. U. Zaman, A. Tayyaba, K. U. R. Khan, and A. V. Reddy, "Enhancement of load balanced gateway selection in integrated internet-manet using genetic algorithm," in *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Dec 2016, pp. 747–752.

[15] M. Taghiloo, M. Dehghan, J. Taghiloo, and M. Fazio, "New approach for address auto-configuration in manet based on virtual address space mapping (vasm)," in *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, April 2008, pp. 1–6.

[16] A. H. Network, S. Nesargi, and R. Prakash, "Manetconf: Configuration of hosts in a mobile," in ., 2002, pp. 1059–1068.

[17] F. daCosta, *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything*, 1st ed. Berkely, CA, USA: Apress, 2013.

[18] C. Anton-Haro and M. Dohler, *Machine-to-machine (M2M) Communications: Architecture, Performance and Applications*, ser. Woodhead Publishing Series in Electronic and Optical Materials. Elsevier Science, 2014.

[19] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, and D. Boyle, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Elsevier Science, 2014.

[20] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions." *Future Generation Comp. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[21] M. Alrowaily and Z. Lu, "Secure edge computing in iot systems: Review and case studies," in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, Oct 2018, pp. 440–444.

[22] R. Ennos, "Estimating the relative rates of pollen and seed migration among plant populations," *Heredity*, vol. 72, no. 3, pp. 250–259, 1994.

[23] F. Chan and M. Tiwari, *Swarm Intelligence: Focus on Ant and Particle Swarm Optimization*. I-Tech Education and Publishing, 2007.

[24] D. A. Vega, J. P. Ospina, J. F. Latorre, and J. E. Ortiz, "An adaptive trust model for achieving emergent cooperation in ad hoc networks," in *Current Trends in Semantic Web Technologies: Theory and Practice*. Springer, 2019, pp. 85–100.