All Sciences Proceedings

1st International Conference on Pioneer and Innovative Studies

June 5-7, 2023 : Konya, Turkey

ICPIS

All Sciences Proceedings
http://as-proceeding.com/

https://as-proceeding.com/index.php/icpis

Alternative technique of messaging through a new configuration of IOT devices

Sadika KHOUNI[1,*], Hamimi CHEMALI[1] and Nora KERKAR[1]

[1] *Ferhat Abbas University, Faculty of Technology, Department of Electronic, Sétif, Algeria*

[*] *sadika2009@gmail.com*

Abstract – A new strategy for configuring Internet Of Things (IOT) nodes based on the Pocket Switched Network (PSN) under high congestion infrastructure is developed to present a new communication alternative relying on a subset of cooperative nodes supplying help, free contribution and extra services in time and space. Two parameters ‘‘node-agent’’ and ‘‘security degree’’ are initially defined to compute resulting network performance. The developed model comprising 5 regions (4 communities and an ‘‘EXTERNAL’’) built in C++ has proved that communication can be established under even weak ‘‘defined cooperation’’. To validate this New IOT developed technique and analyze its performance, we have implemented this mechanism of transmitting information on exploring a ‘‘Secure Simple Epidemic Algorithm’’ (SSEA), in where propagating of information is under control of an added secure condition to the basic Simple Epidemic Algorithm (SEA).The response time is optimized in the case of high security degree and large number of selected nodes.

Keywords – Internet of Things, Wireless Sensor Network, Pocket Switched Network, Delay Tolerant Network, Epidemic, Ad-Hoc Network.

I. INTRODUCTION

Simple Epidemic Algorithm (SEA) [1-2] is used in the social network based protocol routing to keep a link between nodes. We have defined the Secure Simple Epidemic Algorithm (SSEA). The latter is SEA, for which the spread of information is in a security condition (security degree *d*). In SSEA, the selected candidate should have a high *d* value. In this paper we have defined a new IOT model that uses the newly developed SSEA for PSN as a technique of communication. This new IOT model preserves communication's link when an Internet connection is lost. PSN is based on the movement of the persons to deliver information, so it relies on their cooperation to establish links. In this paper we will process communication between persons (mobile phones). The following items define the cooperation of each node: battery level, charge, and availability. An available node with a high battery level and a high charge will be an excellent cooperative node.

The main body of this paper is organized as follows: In Section II, we present the proposed IOT Model, in where the topology of the model is detailed; and the security degree *d* is defined. In Section III, we describe PSN Technology and show how we have developed SSEA for PSN to establish secure communication between nodes. In Section IV, we present the scenario of communication using PSN. In Section V, we compare SSEA with related work to show its performance. In Section VI, we write the conclusions.

II. THE PROPOSED IOT MODEL

A. *THE TOPOLOGY OF THE PROPOSED MODEL*

As the first approach, let consider N static

Areas. Each area defines a community. An area's outside defines "EXTERNAL".

Each node may belong to more than one community. Inside the community, it is a local

network member. Once in "EXTERNAL", each node is a social ad-hoc network member.

In "EXTERNAL", for each node, we have defined the parameter *d* as the security degree that reflects the number of communities to which it belongs and its Trustworthiness. In the absence of an internet connection, every node desiring to communicate with its community sends messages via other nodes. This technique is named the PSN technology. Each node searches about nodes with high *d* values (Trustworthy nodes) to secure the transmission. Considering nodes cooperative, so "EXTERNAL" is an IOT network linking the different local IOT networks defined inside each community.

B.THE SECURITY DEGREE

To give a cognitive identity to node, we have defined and introduced the parameter *d* as shown in equation (1).

$$d = \frac{k}{N} \qquad (1)$$

Where *k* is the number of communities that node belongs to, and *N* the total community number. The possible values of *d* are *N values.*

So, each node has a specific *d* added to the identity vector. Node with high *d* is a popular node and a more secure one to transmit information.

To study the efficiency of the proposed model and to get measurement, we have fixed the number of communities. Fig. 1 shows an example model of 5 regions: 4 communities (community 1, 2, 3, and 4) and an "EXTERNAL". Every community has limited size and members. The four plotted communities are circles, and we have affected the colors red, green, pink, and white respectively to the first community, the second one, the third, and the fourth. When nodes are in "EXTERNAL", the color affected is yellow. For this example (refer to equation 1), we have four security degrees *d*: 1, 0.75, 0.5, and 0.25 when node belongs respectively to 4 communities, 3, 2, and 1 community.

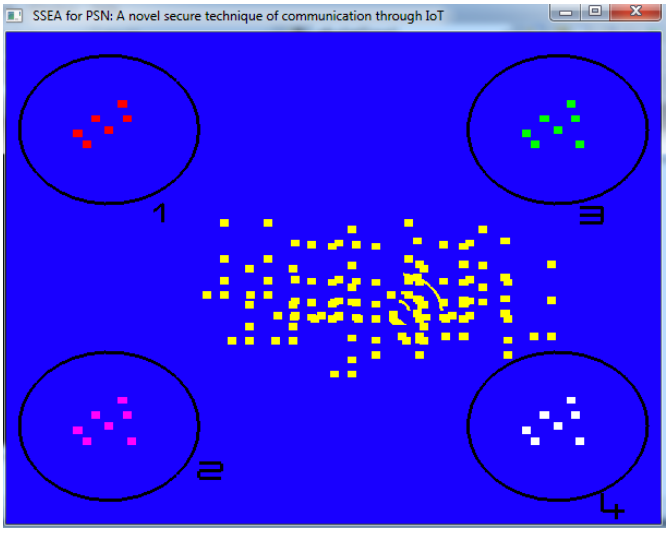

Fig. 1 The Topology of the Proposed IOT Model.

III. PSN TECHNOLOGY

PSN derives from the Delay Tolerant Network technology (DTN). In DTN, radio disconnects between devices present the major recurring problem [3-4]. DTN uses intelligent equipment to deliver information [5], whereas PSN uses only persons (mobile phones). It works without any help and any specific structure.

In PSN, the transmission is as Store-Carry-Forward (SCF) pattern [6]. The mobile phone is to store messages. The movement of the persons is to carry it. Short-range radio links [7-8] were to forward it. Ultrasound [9-10], Bluetooth, and WIFI [11-12] are part. The trouble in the mixed network results from interoperability between nodes [13-14]. Authors in [15-16] propose solutions to this problem.

There are several routings explored in PSN; social network-based protocol routing is the more popular one [6].

The Epidemic Algorithm is one of the algorithms used in the social network based protocol routing. It is used in various Wireless Sensor Networks (WSN) [17-18]. It is a better technique to build a link in Ad Hoc Networks [19], Vanet [20], and DTN [21]. The Epidemic Algorithm can, in the end, infect an entire population.

First, let defines the Simple Epidemic Algorithm SEA [1-2]:

For a fixed size population *n*, *k* nodes are already infected. The infection appears in rounds. The probability that a particular susceptible (uninfected) node is then infected in a round if *k* nodes are already infected is shown in equation (2).

$$P_{inf}(k,n) = 1 - (1 - 1/(n-1))^k \quad (2)$$

The time complexity is O (log *N*), also after $log_{0.75}\frac{n}{2}$ rounds, every node is infected [2]. To prove the efficiency of our proposed IOT model, we have developed the Secure Simple Epidemic Algorithm (SSEA).

- DESCRIPTION OF SSEA

As defined in section 2, *d* reflects the number of communities to which node belongs. The utility of *d* appears when nodes are in "EXTERNAL" without an internet link. So each node is a member of the social ad-hoc network, and it is supposed cooperative. For this situation, we have developed SSEA in where the infection is relative to the security degree *d*. The objective is to infect only the nodes with a high security degree to secure the communication. In this state, SSEA reduces the number of infected nodes, so the energy consumption is reduced. The system of equations (3) shows the probability that a particular susceptible (uninfected) node with *d* value is then infected in a round if *k* nodes with *d* value are already infected.

$$P_{d,inf}(k,n) = \begin{cases} 1 - (1 - 1/(n_d - 1))^k, & n_d < n \\ P_{inf}(k,n), & n_d = n \end{cases} \quad (3)$$

As seen for equation (2) defined by two values, *n*, and *k*, SEA infects an entire population with no condition; whereas, the three values, *n*, *k*, and *d*, define the conditional probability given by the system of equations (3). The security degree *d* controls the infection in SSEA. This latter affects only the nodes desired. That is the first difference between equation (2) and the system of equations (3). The second one is that equation (2) is defined for a global population of *n* nodes, while the system of equations (3) is defined for a population of nodes with a specific *d* value. A particular case appears when all nodes have the same *d* value, so the system of equations (3) will be equation (2).

To select nodes with a specific security degree, the expected number of newly infected nodes will be $(n_d - k)(1 - (1 - 1/(n_d - 1))^k)$. In the end, n_d nodes will be infected with the same security degree *d*.

For *n* nodes, and considering the cost communication as homogeneous, E_{cost} is the energy cost between two nodes. The energy cost of the network in SEA is nE_{cost}. In SSEA, the communication is between n_d selected nodes, so the energy cost is $n_d E_{cost}$.

IV. THE SCENARIO OF COMMUNICATION

To explain the working of our defined model, we have built a virtual scenario of the node-agent's discovery under C++ using the OpenGL library (a library used in diverse areas of computer graphics and exploitable across several platforms). We have defined a member-agent to discern it among other nodes. The procedure carries out the following tasks:

- ✓ A member-agent leaves the first community and travels toward another.
- ✓ It sends a periodic message (hello message) to check and decide its presence inside the community.
- ✓ Leaving its first community and before reaching the targeted one, member-agent belongs to a medium named "EXTERNAL".

Once in "EXTERNAL", and when strong congestion appears, member-agent without the link of communication cannot reach the targeted community to which it must deliver information. So, PSN was to govern the communication network: Member-agent generates an alert message to its environment to get other links or alternatives that would offer a solution. This situation requests the cooperation of nodes. It generates an alert message in a defined period and waits for an answer. This message includes a vector identity comprising the communities it belongs to. A candidate node will reply with an acceptance message comprising its vector identity. If more than one node responds, member-agent calculates their security degrees *d* (reflects the privacy of a message). It delivers messages to the node owning the highest one to get

a more secure link. So, this node behaves as a node-agent. The following timers t_1, $2t_1$, $3t_1$, and $4t_1$ were predefined to find node-agent with d=1, 0.75, 0.5, and 0.25 respectively.

Remember that every timer is the time that separates a time of sending an alert message and receiving an answer. Let's recall that cooperation is a sign of accepting or refusing the transport of messages. To model cooperation cases, we have implemented a different number of nodes (considered cooperatives) in the region defined as "EXTERNAL"

Fig. 2 describes the flowchart procedure to find the first node-agent.

At the first time, we considered that a member-agent is going from area1 to area4. Once in "EXTERNAL" high congestion appears and no internet link is available. In this situation, node-agent switches to process the PSN technique to send information to area4. We suggest that the member-agent is surrounded by cooperatives nodes, and each cooperative node belongs to one community (d=0.25) at least. Four situations are considered:

- First situation

Member-agent sends an alert message, and when it receives answers, it gives the information to the first responding candidate with d=1. If there are no candidates with d=1, it passes to the second situation.

- Second situation

It sends a second alert message, and when it receives answers, it sends the information to the first responding candidate with d=1. If there are no candidates with d=1, it sends the information to the first responding candidate with d=0.75. If there are no candidates with d=0.75, it passes to the third situation.

- Third situation

It sends a third alert message, and when it receives answers, it sends the information to the first responding candidate with d=1. If there are no candidates with d=1, it sends the information to the first responding candidate with d=0.75. If there are no candidates with d=0.75, it sends the information to the first responding candidate with d=0.5. If there are no candidates with d=0. 5, it passes to the fourth situation.

- Fourth situation

It sends a fourth alert message, and when it receives answers, it sends the information to the first responding candidate with the highest d value.

If this first node-agent can't finish this task, the process of Fig. 2 will be repeated to find the second node-agent and so on.

V. RESULTS AND DISCUSSION

- THE COMPARISON OF SSEA WITH GOSSIP[2]

As defined in our IOT model, the node spread information only to the nodes with high security degree. To give a comparison between SSEA and gossip [2] (Table1), we have calculated the rounds needed to spread information in SSEA for different cases of the number of nodes for different security degrees (Table2, Table3, Table4, Table5).

Table1. Performance of variable total number of nodes using gossip, through which each time an informed nodes would choose 1 neighboring nodes [2]

Total nodes N	Times Rounds
65	11
129	13
257	15
513	16

For each d value, we have envisaged three rates of the total number of nodes N considered in gossip [2]: 1/8, 1/4, and 1/3.

We can observe in Table2 for d=1 that the best time is for rate 1/8, and more rate is high, time converges to gossip [2].

In Table3 for d=0.75, Table4 for d=0.5 and Table5 for d=0.25, we can see the same remark that in Table4.

For the different states of security degrees values d, the best time is for d= 1. In all cases, the number of rounds for SSEA is less than in gossip [2].

So, as proved in this comparison with gossip [2], SSEA, reduces the number of rounds to infect nodes.

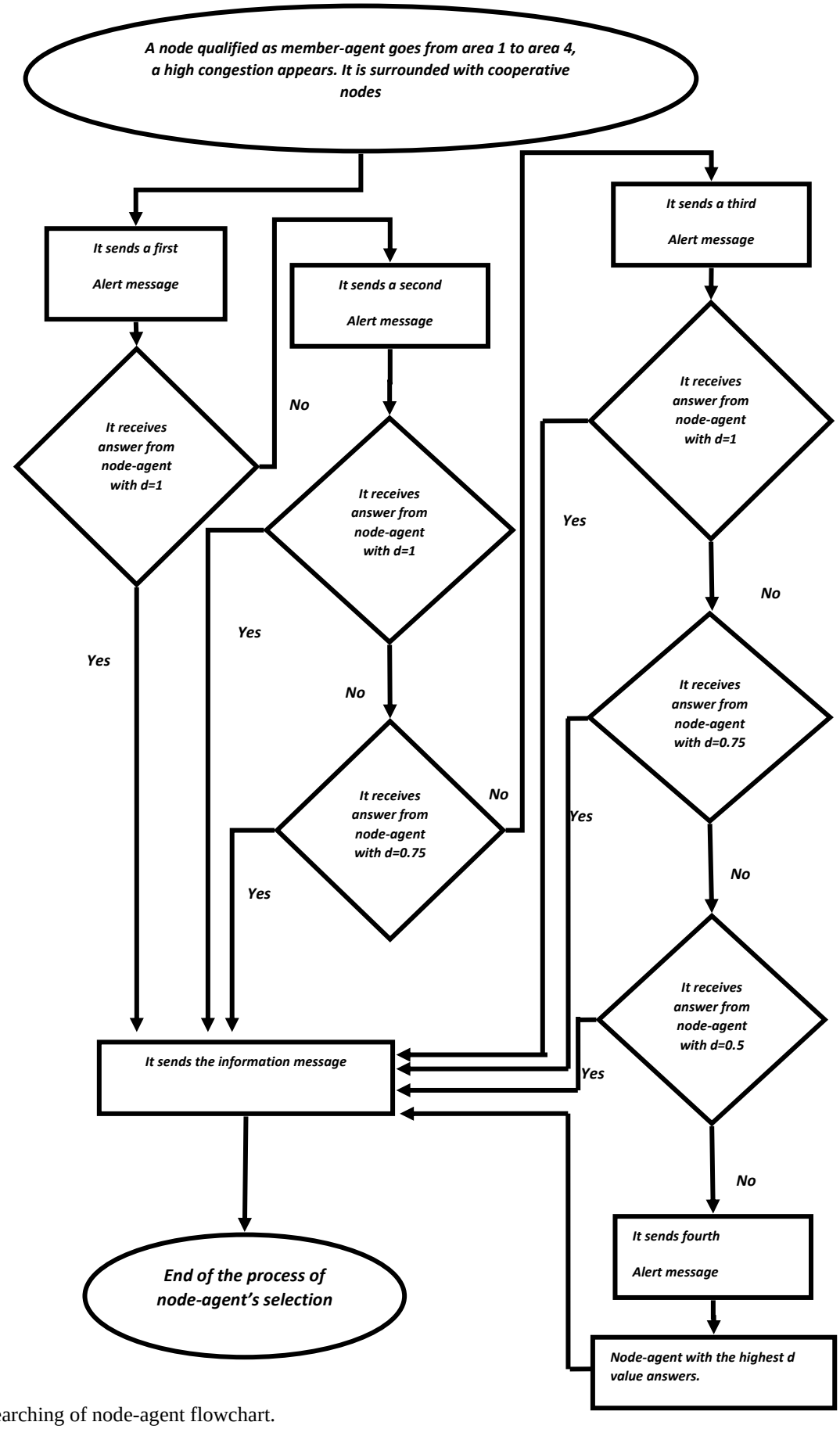

Fig.2 Searching of node-agent flowchart.

Table2. Performance comparison between SSEA (d =1) and gossip [2]

Total nodes N	Times Rounds [10]	Times Rounds (SSEA) d =1		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	12	13
513	16	12	15	16

Table3. Performance comparison between SSEA (d =0.75) and gossip [2]

Total nodes N	Times Rounds [10]	Times Rounds (SSEA) d =0.75		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	12	13
513	16	12	15	16

Table4. Performance comparison between SSEA (d =0.5) and gossip [2]

Total nodes N	Times Rounds [10]	Times Rounds (SSEA) d =0. 5		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	13	14
513	16	13	15	16

Table5. Performance comparison between SSEA (d =0.25) and gossip [2]

Total nodes N	Times Rounds [10]	Times Rounds (SSEA) d =0.25		
		$\frac{N}{8}$	$\frac{N}{4}$	$\frac{N}{3}$
65	11	5	8	9
129	13	8	10	11
257	15	10	13	14
513	16	13	15	16

The following figures (Fig3 - Fig.6) summarize the previous tables. It can well be seen that SSEA is better than Gossip (Ruiqi Yang) for the different cases considered.

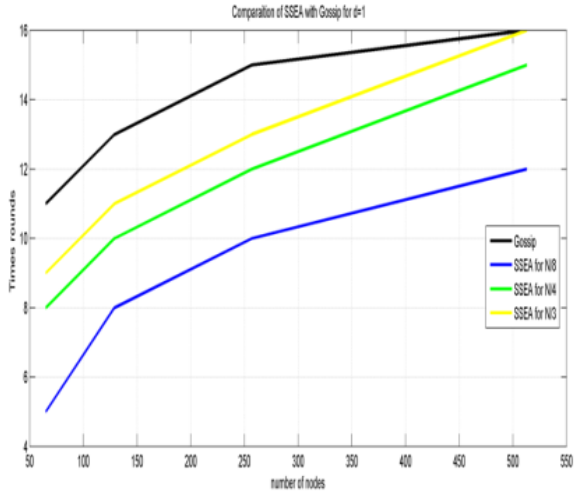

Fig.3 Performance comparison between SSEA (d =1) and gossip [2]

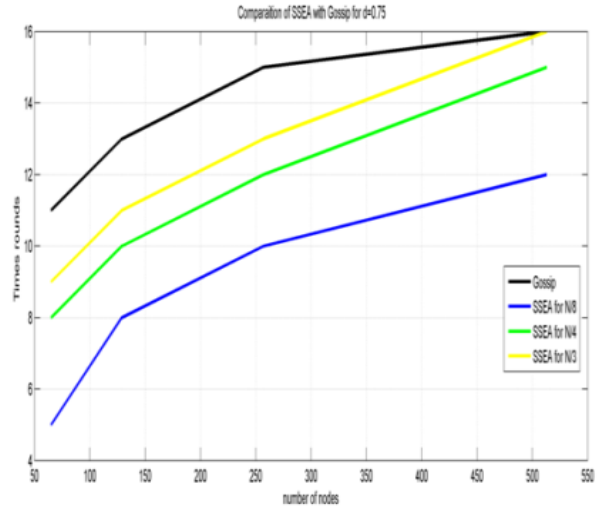

Fig.4 Performance comparison between SSEA (d =0.75) and gossip [2]

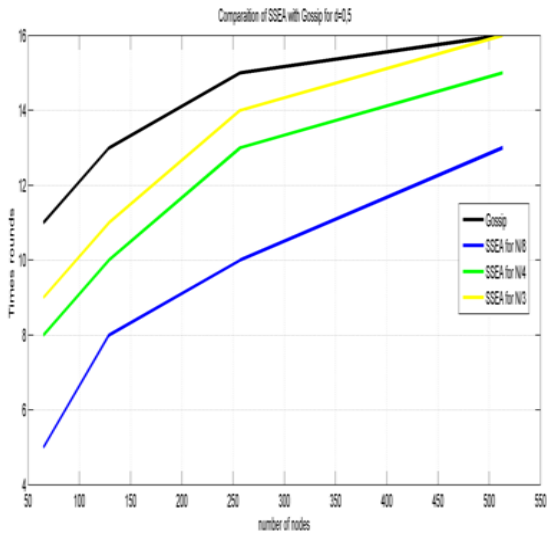

Fig.5 Performance comparison between SSEA (d =0.5) and gossip [2]

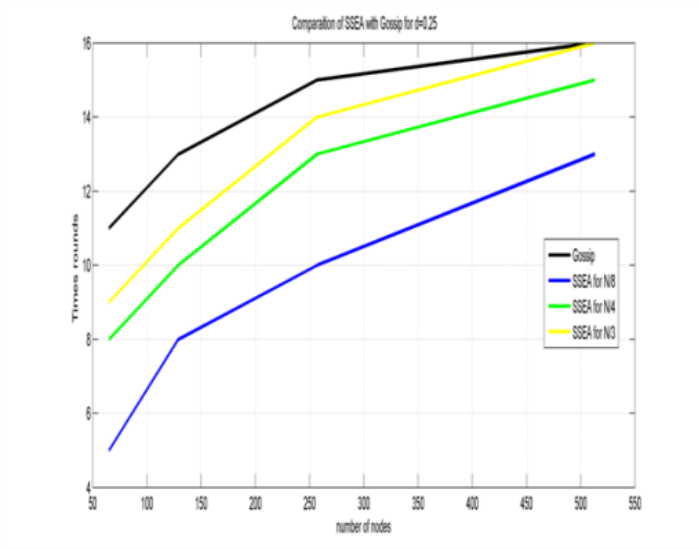

Fig.6 Performance comparison between SSEA (d =0.25) and gossip [2]

VI. CONCLUSION

This research has introduced a new IOT model. In this model, nodes (persons) travel between a set of communities and an "EXTERNAL". The efficiency of this definition is when the node was with no link.

It used the PSN technique to send messages. For PSN we have developed SSEA. SSEA is a SEA on which we have added a security degree as a condition to spread information. Security degree reflects the number of communities to which the node belongs. It defines the privacy of messages measured by the popularity and reputation of nodes.

The cooperation of near nodes was to set up communication. Our method gives serious advantages: it works without a specific structure and specific technology. When no internet connection is available, this method based on cognitive identification is a well to get a link between nodes.

REFERENCES

[1] Genç Z, Özkasap Ö, (2007) Peer-to-Peer Epidemic Algorithms for Reliable Multicasting in Ad Hoc Networks, International Journal of Electronics and Communication Engineering, 1(3), 575-579.

[2] Yang R, (2020) Analysing the efficiency and robustness of gossip in different propagation processes with simulations, Journal of Physics: Conference Series, 1486, 032001.

[3] Dong W, Li C, Miao Z, (2016) Joint Link State and Forwarding Quality: A Novel Geographic Opportunistic Routing in VANETs, In Proceedings of the International Conference on Computer, Information and Telecommunication Systems Kunmingg 1-5.

[4] Minea M, Claudia SM, Stăncel IN, Viviana LM, (2016) Combined Opportunistic Vehicular/Cellular Networking for Cooperative Driving Assistance in Highway Scenarios, In Proceedings of the International Conference on Applied and Theoretical Electricity 1-6.

[5] Seguí J, Jennings E, (2006) Delay Tolerant Networking – Bundle Protocol Simulation, In Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology 235-240.

[6] Sarkar RR, Rasul K, Chakrabarty A, (2015) Survey on Routing in Pocket Switched Network, Wireless Sensor Network, **7(**9), 113-128.

[7] Papaj J, Dobos L, Palitefka R, (2014) Candidate node selection based on trust for cognitive communication of mobile terminals in hybrid MANET-DTN, In Proceedings of the 5th IEEE Conference on Cognitive Infocommunications 61-66.

[8] Priyantha NB, (2005) The Cricket Indoor Location System, PhD Thesis, University of Cambrige, Boston, MIT, USA.

[9] Priyantha NB, Chakraborty A, Balakrishnan H. (2000) The Cricket Location-Support System, In Proceedings of the 6th annual international conference on Mobile computing and networking, 32-43.

[10] Amah TE, Kamat M, Abu Bakar K, Moreira W, Oliveira-Jr A, Batista MA, (2016) Spatial Locality in Pocket Switched Networks, In Proceedings of the 17th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks 1-5.

[11] Bromberg YD, Grace P, Réveillère L, (2011) Starlink: runtime interoperability between heterogeneous middleware protocols, In Proceedings of the 31st IEEE International Conference on Distributed Computing Systems 446-455.

[12] Emruli B, (2014) Ubiquitous Cognitive Computing: A Vector Symbolic Approach, PhD Thesis, Luleå University of Technology, Luleå, Sweden.

[13] Raveneau P, Rivano H, (2015) Tests Scenario on DTN for IoT; III Urbanet collaboration, Technical Report RT-0465, Inria-Research Centre, Grenoble,Rhone-Alpes, France.

[14] Stusek M, Masek P, Kovac D, Ometov A, Hosek J, Kröpfl F, Andreev S, (2016) Remote Management of Intelligent Devices: Using TR-069 Protocol in IoT, In Proceedings of the 39th IEEE International Conference on Telecommunications and Signal Processing 74-78.

[15] Simatic J, Cherkaoui A, Bastos RP, Fesquet L, (2016) New Asynchronous Protocols for Enhancing Area and Throughput in Bundled-Data Pipelines, In Proceedings of the 39th IEEE International Conference on Telecommunications and Signal Processing 1-6.

[16] Burleigh S, (2015) Delay-Tolerant Electronic Commerce, In Proceedings of the IEEE International Conference on Wireless Communications & Signal Processing 1-4.
[17] Shashidhar N, Kari C, Verma, R, (2015) The Efficacy of Epidemic Algorithms on Detecting Node Replicas in Wireless Sensor Networks, Journal of Sensor and Actuator Networks, 4(4), 378-409.
[18] Ganesan D, Krishnamachari B, Woo A, Culler D, Estrin, D and Wicker S, (2002) An Empirical Study of Epidemic Algorithms in Large Scale Multihop Wireless Networks, Technical Report IRB-TR-02-003, Intel Research.
[19] Vahdat A, Becker D, (2000) Epidemic routing for partially-connected ad hoc networks; Technical Report CS-2000-06, Department of Computer Science, Duke University, Durham, USA.
[20] Spadaccino P, Cuomo F, Baiocchi A, (2020) Epidemic and Timer-Based Message Dissemination in VANETs: A Performance Comparison, Electronics, 9, 595.
[21] Rango F, Amelio S, Fazio P, (2015) Epidemic Strategies in Delay Tolerant Networks from an Energetic Point of View: Main Issues and Performance Evaluation, Journal of Networks, 10,1.