Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2022.00034

Research Article

SSEA for PSN: A novel secure technique of communication through IOT devices

Sadika KHOUNI[1,*], Hamimi CHEMALI[2]

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

ARTICLE INFO

Article history
Received: 28 October 2020
Accepted: 02 June 2021

Key words:
Internet of Things; Wireless Sensor Network; Pocket Switched Network; Delay Tolerant Network; Epidemic; Ad-hoc Network

ABSTRACT

Simple Epidemic Algorithm (SEA) is a social protocol used in the Pocket Switched Network (PSN) technology. SEA infects an entire population. We have defined a Secure Simple Epidemic Algorithm (SSEA) for PSN where a security condition controls the traffic. SSEA doesn't infect a global population. As the Internet Of Things (IOT) is with no specific definition, we have proposed a new model of IOT. In this latter, PSN that uses the developed SSEA guarantees the exchange of information. To best understand, we have defined a small model with four communities and an "EXTERNAL". Nodes traveling between communities have different security degrees. The security degree reflects the number of communities to which the node belongs and defines the security condition of SSEA. The exchange of information relies on the cooperative nodes. Supplying help and extra services in time and space identify the cooperation. In the best case, SSEA infects nodes with high security degrees and reduces the network communication cost.

Cite this article as: Khouni S, Chemali H. SSEA for PSN: A novel secure technique of communication through IOT devices. Sigma J Eng Nat Sci 2022;40(2):300–309.

INTRODUCTION

British technology pioneer Kevin Ashton was the first to use the popular term Internet Of Things (IOT) in 1999. It is a network of objects connected to the Internet Network via sensors [1]. Each one has an Internet Protocol (IP) address [2-3]. Later on, several definitions have appeared. In [4], it is a philosophy with neither single nor universal description. In [5-6], IOT is a compilation of all existing communication technologies inter-reacting with Internet Networks. So, more problems appear when the number of objects goes high. The major problem is how to secure information, how to give an IP address to all objects [1], and how to maintain a link between them when an internet connection was loosed. For complete coverage of the monitoring system, it needs extra activities [7]. All searchers are working to find a new alternative link of communication in IOT.

Social network based protocol routing is one of many protocols routing used in PSN [8]. Simple Epidemic Algorithm (SEA) [9-10] is used in the social network based

*Corresponding author.
*E-mail address: sadika2009@gmail.com

This paper was recommended for publication in revised form by Regional Editor N. Özlem Ünverdi

Published by Yıldız Technical University Press, İstanbul, Turkey

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.

Going from the proposition that IOT is with no universal description, the new in this paper is the definition of the newly 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.

The following items define the model:

- The topology of the model: The environment is divided into communities and an "EXTERNAL". Each community is a small local IOT network. "EXTERNAL" is an external IOT network. Inside communities, every node (person) behaves as a local network device. In "EXTERNAL", it should keep this identity and will be a social ad-hoc network member too.
- The Security degree *d* parameter: In this model, "Human" and "Object" have a common relation as to belong to the same family or to belong to the same factory or institution. Being in the same place at the same time during several periods can be a relation. Therefore, every node may belong to more than one community. This multi membership defines the security degree *d* parameter. So, each node must have a vector identity (which includes *d*).
- The PSN Technology: In "EXTERNAL", when a node lost an Internet connection, it switches to keep a link with its community via other nodes. This technique of communication defines the Pocket Switched Network (PSN) technology. So, PSN deals and supports all types of IOT items in absence of the internet connections. It is one of the technologies used to discover and to add new objects to existing IOT.
- The Cooperation of nodes: Since PSN is based on the movement of the persons to deliver information; it relies on their cooperation to establish links. 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 2, we present the proposed IOT Model, in where the topology of the model is detailed; and the security degree *d* is defined. In Section 3, we describe PSN Technology and show how we have developed SSEA for PSN to establish secure communication between nodes. In Section 4, we present the scenario of communication using PSN. In Section 5, first, we compared SSEA to SEA for a different case of nodes number and values of security *d* parameter to prove the benefit of the model; after, we compare SSEA with related work to show its performance. In Section 5, we write the conclusions.

THE PROPOSED IOT MODEL

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.

The Security Degree

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

$$d = \frac{k}{N} \tag{1}$$

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. Figure 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.

PSN TECHNOLOGY

PSN derives from the Delay Tolerant Network technology (DTN). In DTN, radio disconnects between devices present the major recurring problem [11-12]. DTN uses intelligent equipment to deliver information [13], whereas PSN uses only persons (mobile phones). It works without any help and any specific structure.

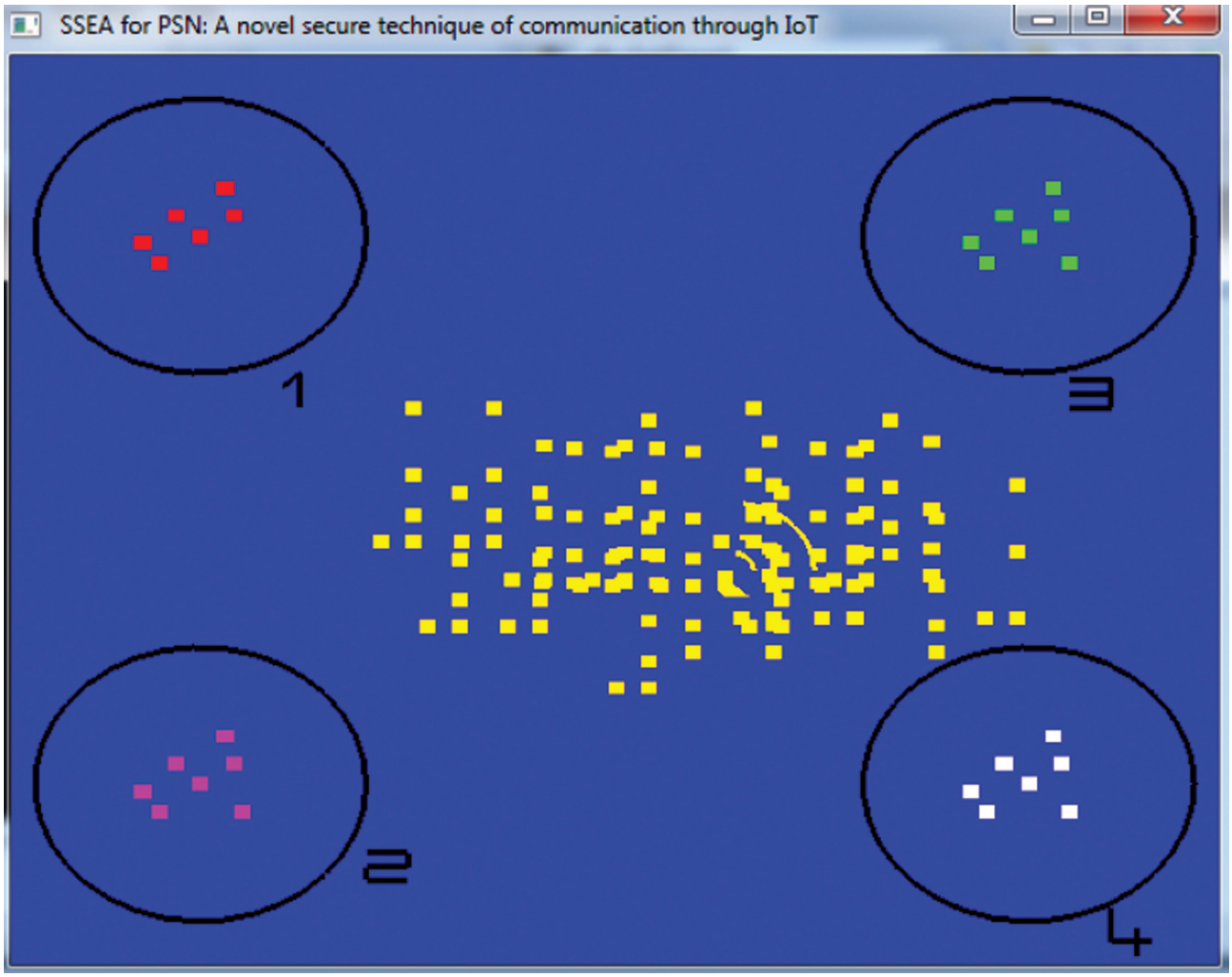


Figure 1. The Topology of the Proposed IOT Model.

In PSN, the transmission is as Store-Carry-Forward (SCF) pattern [8]. The mobile phone is to store messages. The movement of the persons is to carry it. Short-range radio links [14-15] were to forward it. Ultrasound [16-17], Bluetooth, and WIFI [18-19] are part. The trouble in the mixed network results from interoperability between nodes [20-21]. Authors in [22-23] propose solutions to this problem.

There are several routings explored in PSN; social network-based protocol routing is the more popular one [8].

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)[24-25]. It is a better technique to build a link in Ad Hoc Networks [26], Vanet [27], and DTN [28]. The Epidemic Algorithm can, in the end, infect an entire population.

First, let defines the Simple Epidemic Algorithm SEA [9-10]:

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 [10].

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.

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

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 $(n_d - k)(1 - 1/(n_d - 1))^k$). 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_dE_{cost}.

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".

Figure 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.

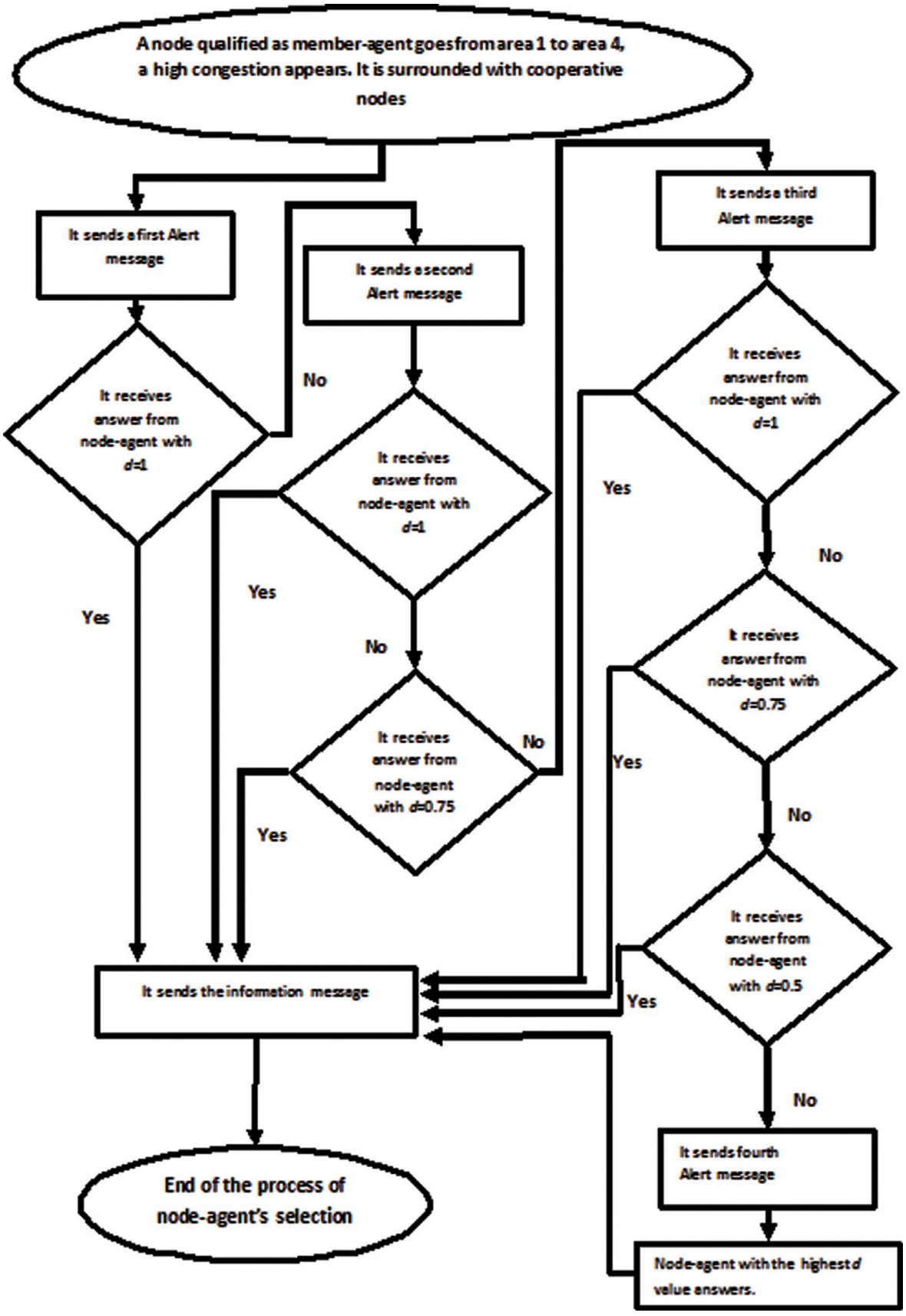


Figure 2. Searching of node-agent flowchart.

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 Figure 2 will be repeated to find the second node-agent and so on.

RESULTS AND DISCUSSION

First, we have compared SSEA with SEA. Then, we have compared SSEA with GOSSIP to prove the performance of the method.

The Comparison of Sea with SSEA

SEA and SSEA are simulated for the same population (n = 100 nodes) under Matlab. The initial value of *k* is 1 (the node which desired to spread information through secure nodes). The simulation is in rounds. We have considered that t_1 (already defined in Section 2 and added to the round) is 0.005 of the round of simulation.

First, we have considered that the member-agent was surrounded by cooperatives nodes with the same security degree *d*. Figure 3 represents the newly affected nodes. As seen, all graphs are very close and seem to be one graph; these dues to the much reduced shift time between the graphs (t_1=0.005 of the round of simulation). In Figure 4, which represents the total infected nodes, we can see the shift between the graphs. For d = 1, the graph of SSEA has shifted by step de t_1. Similarly, for d=0.75, 0.5, and 0.25, it has shifted $2t_1$, $3t_1$ and $4t_1$ respectively. The cost of communication was to drop the same for SEA and SSEA.

In the second state, the member-agent was surrounded by nodes with different security degrees *d*. Figure 5 ((A)-(B)), Figure 6 ((A)-(B)) and Table1 show that for a total number of 100 nodes, eight situations of communication for SSEA were predicted:

For d=1:

Situation1: From 100 nodes, only 10 were cooperatives.

Situation2: From 100 nodes, only 15 were cooperatives.

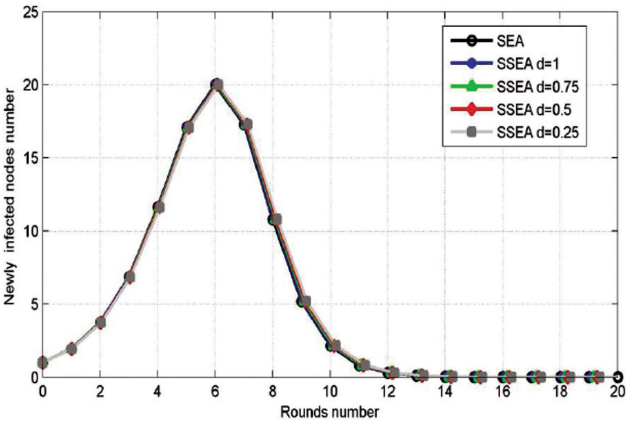


Figure 3. Newly infected nodes in SSEA for different *d* values.

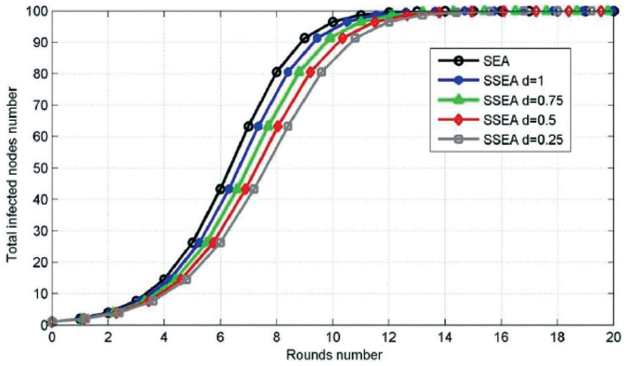
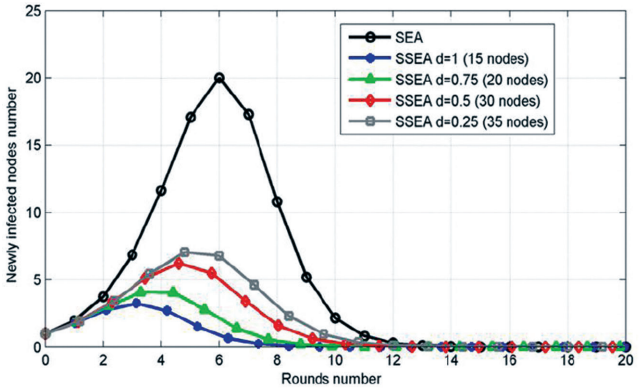
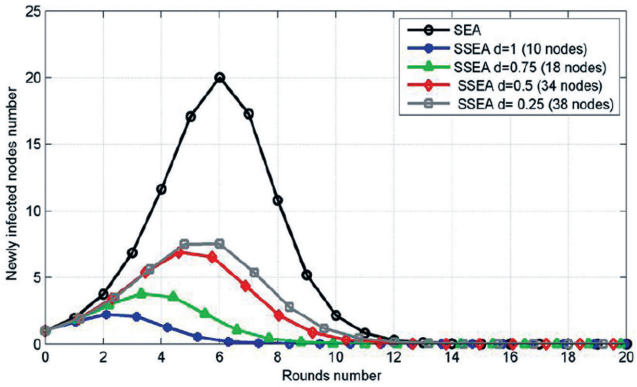


Figure 4. Total infected nodes in SSEA for different *d* values.



(A)



(B)

Figure 5. Newly infected nodes in SSEA for selection of nodes with specific *d* values.

For d=0.75:

Situation3: From 100 nodes, only 18 were cooperatives.

Situation4: From 100 nodes, only 20 were cooperatives.

For d=0.5:

Situation5: From 100 nodes, only 30 nodes were cooperatives.

Situation6: From 100 nodes, only 34 nodes were cooperatives.

And for d=0.25:

Situation7: From 100 nodes, only 35 nodes were cooperatives.

Situation8: From 100 nodes, only 38 nodes were cooperatives.

In all situations, the member-agent communicates only with cooperatives nodes.

As observed in Figure 5, Figure 6, and Table1, the time elapsed for d=1 is less than the other values of d: 6 rounds for situation1 and 7 for situation2.

For d= 0.75: the time elapsed is 8 for situation3 and 9 for situation4.

For d= 0. 5: the time elapsed is 10 for the situation5 and 11 rounds for situation6.

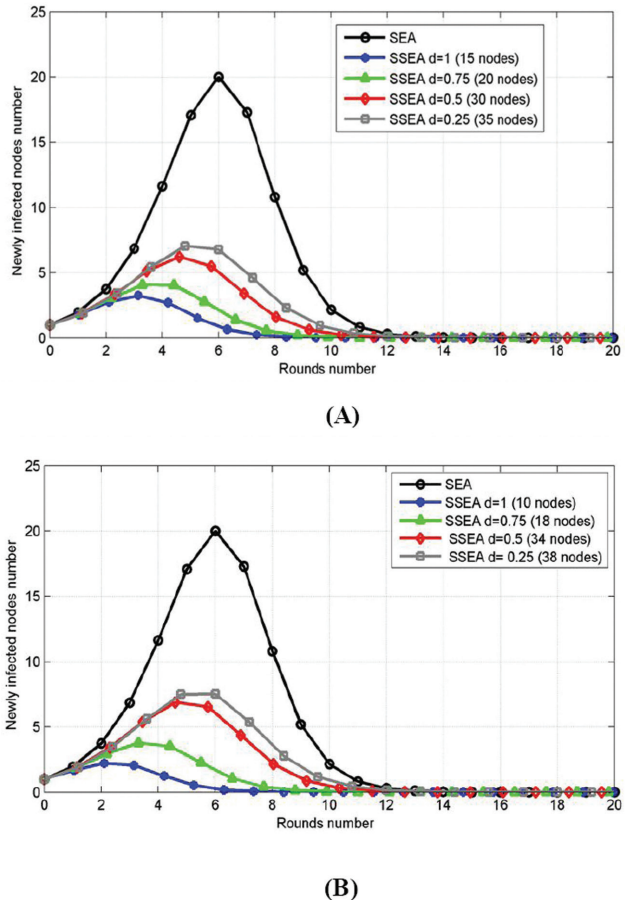


Figure 6. Total infected nodes in SSEA for selection of nodes with specific d values.

For d= 0.25: the time elapsed is 11 rounds for situation7 and 12 for situation8.

From table1, we can see that the least time is for d =1, then for d=0.75, after for d=0.5, and finally for d=0.25.

The last colon of Table 1 shows that the energy cost defined in section 3 is reduced only to the selected nodes.

The time necessary to infect 100 nodes in SEA is estimated to 14 rounds, and the energy cost is $100E_{cost}$ (Figure 6, Table1).

So, a comparison of the different situations of SSEA with SEA for 100 nodes shows that SSEA is best for high d values. SSEA reduces the time of infection and energy consumption. More, SSEA secures information when d is high.

The Comparison of SSEA with Gossip[10]

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 [10] (Table 2), we have calculated the rounds needed to spread information in SSEA for different cases of the number of nodes for different security degrees (Table3, Table4, Table5, Table6).

For each d value, we have envisaged three rates of the total number of nodes N considered in gossip [10]: 1/8, 1/4, and 1/3.

Table 1. Performance of variable total number of nodes using SSEA

		Times Rounds	The energy cost
Total nodes / ***d*=**	100 nodes (without considering d)	14	$100E_{cost}$
1	10 nodes	6	$10E_{cost}$
	15 nodes	7	$15E_{cost}$
0.75	18 nodes	8	$18E_{cost}$
	20 nodes	9	$20E_{cost}$
0.5	30 nodes	10	$30E_{cost}$
	34 nodes	11	$34E_{cost}$
0.25	35 nodes	11	$35E_{cost}$
	38 nodes	12	$100E_{cost}$

Table 2. Performance of variable total number of nodes using gossip, through which each time an informed nodes would choose 1 neighboring nodes [10]

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

Table 3. Performance comparison between SSEA (d = 1) and gossip [10]

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

Table 4. Performance comparison between SSEA (d = 0.75) and gossip [10]

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

Table 5. Performance comparison between SSEA (d = 0.5) and gossip [10]

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	12	13
513	16	12	15	16

Table 6. Performance comparison between SSEA (d = 0.25) and gossip [10]

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	12	13
513	16	12	15	16

We can observe in Table1 for d=1 that the best time is for rate 1/8, and more rate is high, time converges to gossip [10].

In Table4 for d=0.75, Table5 for d=0.5 and Table6 for d=0.25, we can see the same remark that in Table3.

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 [10].

So, as proved in the comparison with SEA, and the comparison with gossip [10], SSEA, reduces the energy consumption to the selected nodes, and the number of rounds to infect nodes.

Finally, we can confirm that SSEA is beneficial in terms of reduction of time and energy consumption, so the cost of communication is reduced.

CONCLUSIONS

This research has introduced a new IOT model. It is a particular Wireless Sensor Network (WSN). 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. The cooperation of near nodes was to set up communication. The popularity and reputation of nodes measured the privacy of messages. This latter was defined by the security degree, which reflected the number of communities to which the node belonged.

To more see the benefits of this model, we have developed SSEA for PSN. SSEA is a SEA on which we have added a security degree as a condition to spread information. In SSEA, the link is gotten only between selected nodes. The comparison with the related works shows the benefit of SSEA to reduce energy consumption and communication time.

Like all communication methods, this method presents some disadvantages. The first one is the break of a link when nodes are absent [8; 17]. Since our method focus on high congestion areas, this problem is eliminated. The second one is a long time need to respond because of the no cooperation of nodes that says nodes are not available or available with low battery or low charge. This problem isn't permanent; the node is tracking for cooperative nodes. It delays the communication but doesn't drop it. The third one is the reduction of communication security when all nodes are with low security degrees.

Other hands, our method gives serious advantages: it works without a specific structure and specific technology [8]. When no internet connection is available, this method based on cognitive identification is a well to get a link between nodes [8; 17]. Thanks to select a reduced nodes numbers with high security degrees, this method offers a low cost of communication with more secure links. All networking technologies can be used [17-19]: Wifi, Bluetooth, Ultrasound.....

So, for the future, when all wireless networks will gather to make sure permanent links, this method based on PSN will be the leader of this new technology of networking. So, this way of networking may combine an original concurrent to the Internet Network.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES

[1] Karen R, Scott E, Lyman C. The internet of things: an overview. Reston, VA: Internet Society; 2019.

[2] Crabtree A, Tolmie P. A day in the life of things in the home. Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing; 2016:1736–1748. [CrossRef]

[3] Oliveira CC, Oliveira DC, Gonçalves JC, Kuniwake JT. Pratical introduction to internet of things: practice using Arduino and Node.js. Proceedings of the 22nd Brazilian Symposium on Multimedia and the Web; 2016:17–18. [CrossRef]

[4] Stout WMS, Urias VE. Challenges to securing the internet of things. Proceedings of the International Carnahan IEEE Conference on Security Technology; 2016:1–8. [CrossRef]

[5] Ruiz M, Álvarez E, Serrano A, García E. The Convergence between wireless sensor networks and the internet of things, challenges and perspectives: a survey. IEEE Lat Am Trans 2016;14:4249–4254. [CrossRef]

[6] Lingel J. The poetics of socio-technical space: evaluating the internet of things through craft. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems; 2016:815–826. [CrossRef]

[7] Shemshadi A, Sheng QZ, Qin Y. ThingSeek: A crawler and search engine for the internet of things. Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval; 2016:1149–1152. [CrossRef]

[8] Sarkar RR, Rasul K, Chakrabarty A. Survey on routing in pocket switched network. Wirel Sens Netw 2015;7:113–128. [CrossRef]

[9] Genç Z, Özkasap Ö. Peer-to-peer epidemic algorithms for reliable multicasting in ad hoc networks. Int J Electronics Commun Eng 2007;1:575–579.

[10] Yang R. Analysing the efficiency and robustness of gossip in different propagation processes with simulations. Journal of Physics: Conference Series 2020;1486:032001. [CrossRef]

[11] Dong W, Li C, Miao Z. Joint link state and forwarding quality: a novel geographic opportunistic routing in VANETs. Proceedings of the International Conference on Computer, Information and Telecommunication System; 2016:1–5. [CrossRef]

[12] Minea M, Claudia SM, Stăncel IN, Viviana LM. Combined opportunistic vehicular/cellular networking for cooperative driving assistance in highway scenarios. Proceedings of the International Conference on Applied and Theoretical Electricity; 2016:1–6. [CrossRef]

[13] Seguí J, Jennings E. Delay tolerant networking – bundle protocol simulation. Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology; 2006:235–240. [CrossRef]

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

[15] Priyantha NB. The cricket indoor location system. PhD Thesis. Boston: University of Cambrige, MIT; 2005.

[16] Priyantha NB, Chakraborty A, Balakrishnan H. The Cricket location-support system. Proceedings of the 6th annual international conference on Mobile computing and networking; 2000: 32–43. [CrossRef]

[17] Amah TE, Kamat M, Abu Bakar K, Moreira W, Oliveira-Jr A, Batista MA. Spatial locality in pocket switched networks. Proceedings of the 17th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks; 2016:1–5. [CrossRef]

[18] Bromberg YD, Grace P, Réveillère L. Starlink: runtime interoperability between heterogeneous middleware protocols. Proceedings of the 31st IEEE International Conference on Distributed Computing Systems; 2011:446–455. [CrossRef]

[19] Emruli B. Ubiquitous cognitive computing: a vector symbolic approach. PhD Thesis. Luleå, Sweden: Luleå University of Technology; 2014.

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

[21] Stusek M, Masek P, Kovac D, Ometov A, Hosek J, Kröpfl F, et al. Remote management of intelligent devices: Using TR-069 Protocol in IoT. Proceedings of the 39th IEEE International Conference on Telecommunications and Signal Processing; 2016:74–78. [CrossRef]

[22] Simatic J, Cherkaoui A, Bastos RP, Fesquet L. New asynchronous protocols for enhancing area and throughput in bundled-data pipelines. Proceedings of the 39th IEEE International Conference on Telecommunications and Signal Processing; 2016:1–6. [CrossRef]

[23] Burleigh S. Delay-tolerant electronic commerce. Proceedings of the IEEE International Conference on Wireless Communications & Signal Processing; 2015: 1–4. [CrossRef]

[24] Shashidhar N, Kari C, Verma, R. The efficacy of epidemic algorithms on detecting node replicas in wireless sensor networks. J Sens Actuator Netw 2015;4:378–409. [CrossRef]

[25] Ganesan D, Krishnamachari B, Woo A, Culler D, Estrin, D, Wicker S. An empirical study of epidemic algorithms in large scale multihop wireless networks. Technical Report IRB-TR-02-003, Intel Research; 2002.

[26] Vahdat A, Becker D. Epidemic routing for partially-connected ad hoc networks. Technical Report CS-2000-06, Department of Computer Science. Durham, USA: Duke University; 2000.

[27] Spadaccino P, Cuomo F, Baiocchi A. Epidemic and timer-based message dissemination in VANETs: A performance comparison. Electronics 2020;9:595. [CrossRef]

[28] Rango F, Amelio S, Fazio P. Epidemic strategies in delay tolerant networks from an energetic point of view: Main issues and performance evaluation. J Netw 2015;10. [CrossRef]