Enhancing Security in Smart Cities using Dynamic Multipath Algorithm

Fatna El Mahdi, Mohammed Souidi, Halim Berradi, Ahmed Habbani

***Abstract*: The world of today is an ultimate connected world, where all types of physical devices and virtual objects can communicate in order to exchange information or provide services. Internet of Things (IoT) is one of the leading areas that make this worldwide connection possible, by integrating and enabling different solutions and communication technologies.**

Wireless mobile networks are increasing very fast and giving more perspectives in the telecommunication field. Nevertheless, some problems are still facing this development. The most important and mandatory issue, among them, is the security of the network. In this paper, we will introduce some related works about security concept for mobile networks and we present our solution that provides a new dynamic approach to find a variable number of multiple paths according to the neighborhood, the density and to the mobility of nodes in the network. In order to evaluate the impact of our solution on network performances, we implement our algorithm on one of the most known multipath protocols (MP-OLSR).

***Keywords*: Smart cities, Internet of Things, Dynamic Multipath, Security.**

I. INTRODUCTION

In the past, computers used to be connected to the internet by the only medium of wired networks, until the arrival of wireless technologies that changed this fact, and enabled computers to exchange information in wireless mode. By offering more flexibility and mobility to the inter-connected devices, this wireless technology opened the horizons for industrial researchers to explore more development paths into connecting all kinds of mobile and fixed devices such as cameras, sensors, vehicles, smartphones, computers, etc.

Mobile wireless networks are a cornerstone of IoT's success. Small objects that are generally limited in terms of computing capacity, memory and energy, ban be used in industrial, medical, agricultural and many other domains.

5G is the next generation of mobile networks. It is designed to optimize power consumption in order to be suitable for IoT (Internet of Things) and D2D (Device to device) implementation [1]. As in previous mobiles solutions, 5G will have to deal with various security challenges, especially in the case of sensitive communication areas such us Medical or military domains (Figure 1).

Many studies are investigating to enhance security of IoT systems and provide countermeasures against all types of attacks [2, 3]. Cryptography, as one of these countermeasures, is based on identity authentication of network elements and aims to insure integrity and confidentiality of the exchanged messages. This method consists on exchanging secret keys especially for symmetric cryptography when we use the same key. Swapping private keys in a self-organized system is sometimes a complicated task which makes this kind of solutions a bit hard to be implemented.

To overcome this problem, there are some research studies that suggest using Shamir secret sharing technique in order to share the encryption key [4, 5]. This technique consists on dividing the private key into n multiple parts, with a threshold k and sends each part in a path. Thus, no node can reveal the secret without knowing the complete parts or at least threshold number of secret shares (k parts) [6]. If a new node enters the network, it can obtain the secret parts with the help of polynomial interpolation method. However, in traditional cryptography, the trusted party keeps the secret key so there is a considerable probability for security attacks if one or more nodes with secret key can be compromised by the attacker.

Our proposal in this paper is to implement an approach to provide routes used to share the private keys used in the encryption process. Our approach will provide a dynamic and intelligent system in order to select a variable number n of multiple paths, with threshold k used to route different parts of shared key. The existing traditional solutions based on multipath, in IoT systems, deal with different networks with the same way, no matter how dense or mobile the network is. In fact, in such solutions, all the nodes will have a fix number of paths during the communication process. This is not optimal in term of performance especially in a dense network. This is a limitation that our contribution tries to solve by taking into consideration the mobility and density of nodes.

In fact, the random appearance and unplanned node mobility in mobile networks can hinder service continuity and make it extremely difficult or even impossible. It is therefore legitimate to consider the reliability of paths and provide backup routes as a main research field. In this context, that our new approach has been developed which is based on a dynamic algorithm to choose a multiple paths as needed, and which takes into account the link quality that constitute these multiple paths.

Revised Manuscript Received on June 15, 2020.

***** Correspondence Author

Fatna EL MAHDI*, ENSIAS, University of Mohammed V, Rabat, Morocco. Email: fatna.mahdi@um5s.net.ma

Mohammed SOUIDI, ENSIAS, University of Mohammed V, Rabat, Morocco. Email: souididoc@gmail.com

Halim BERRADI, ENSIAS, University of Mohammed V, Rabat, Morocco. Email: halimberradi@gmail.com

Ahmed HABBANI, ENSIAS, University of Mohammed V, Rabat, Morocco. Email: ahmed.habbani@um5.ac.ma

In this paper, a new multipath routing protocol based primarily on route reliability, mobility and network density will be presented, in order to determine and maintain routes that satisfy a considerable degree of reliability and stability.

This paper will be organized as follows; we will introduce the multipath specifications that make this concept importantly attractable. Next we will review some related works about multipath protocols evolution. Our contribution will come, based on this background, to introduce the dynamic multipath concept. So, we will explain the new algorithm that enables the selection of variable number of routes based on network density and disjoint degree. Afterwards, we will discuss the simulation results and finally conclude the paper.

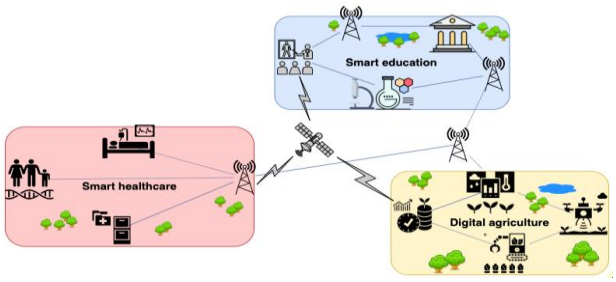


Figure 1: Example of communication in Smart environment

II. CONCEPT OF MULTIPATH

This section will be dedicated to introduce the concept of multipath, its specifications and different types of disjoint paths.

A. Multipath specification

The idea of multipath routing is old and based on connecting source and destination via multiple paths instead of single route. This concept is used in wired networks and in LAN/WLAN networks. Ad-hoc networks and IoT systems [7] also use this concept in order to benefit from its important advantages such as:

- **Automatic backup**: The main purpose of this concept is to offer one or multiple backup routes in order to prevent data loss in case of break in the principle route or node failure. Such automatic backup offers efficient and quick fault recovery in dynamic networks in order to guaranty the service continuity.
- **Load balancing**: This technique allows the resource usage sharing and balancing. Nodes power, memory and CPU usage can be optimized when the traffic is distributed across the network.
- **Road Aggregation**: Ad hoc networks are by nature resource constrained systems. This technique allows to aggregate many routes simultaneously in order to optimize the resource usage and reach the network requirement especially in term of bandwidth.

B. Disjoint Paths

The notion of disjoint roads is one of the most important parameters in the efficiency and reliability of multipath protocols. In fact, the selection of disjoint routes increases the effective bandwidth between two pairs of nodes, distributes the resources better, reduces congestion in the network and reduces the probability of packet loss. In addition, the disjointed routes also increase the reliability of the communication, since the presence of an interruption at a disjointed road in no way affects the other route. For this reason, a lot of research has studied the concept of disjointed paths as [8, 9]. Two types of disjointed roads are defined: node disjoint and link disjointed paths. Node disjoint paths have no nodes in common except the source and the destination (Figure 2). On the other hand, link disjoint paths have no common link (Figure 3). Note that a link disjoint paths may have nodes in common. It is clear that, case of link disjoint paths, the independence of roads in case of link failures is better guaranteed. But, one can guarantee both the independence of nodes and links at the same time by selection node disjoint paths.

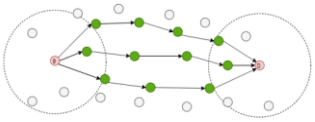


Figure 2: Node disjoint path

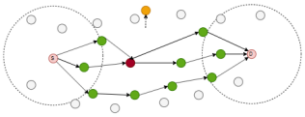


Figure 3: Link disjoint path

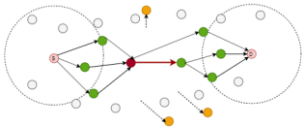


Figure 4: Not link disjoint

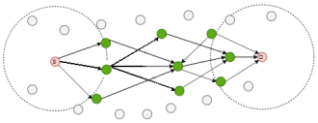
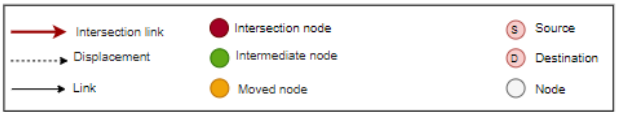


Figure 5: Fail-safe path



III. RELATED WORK

As a case study, we will implement our approach on Multipath Optimized Link State Routing protocol (MP-OLSR) RFC 8218 which is a development of routing protocol OLSR that aims to provide aggregate bandwidth, load balancing and fault-tolerance. This version of OLSR, provides a fixed number of three routes between source and destination in MANET. With same process as OLSR RFC 3626, MP-OLSR exchanges control messages periodically in order to learn the whole network topology [10]. Multipath Dijkstra algorithm uses this topology information to get the multiple paths where the packets will be routed [11]. By adjusting distinct cost functions using this algorithm, we can get node-distinct routes and path-distinct routes as well. By a routing mechanism based on intermediate nodes, the packets are forwarded through the network [12]. Yi et al. in [13], tried to enhance data transmission performance in TCP by taking into consideration the node's reliability in the process of route selecting in multipath. Simulations showed that the use of multipath offers better throughput and network protection compared with single path version.

The same authors concluded in [14] that RREQ messages increase in the process of route discovery in multipath reactive protocol, resulting the generation of more overhead.

OLSR and MP-OLSR use Hop count as a default link metric. This choice is based on the shortest path between source and destination, and characterized by its simplicity and implementation adaptation. The principle of hop count is not about the distance between source and destination, but about the minimum number of hops. However, this approach does not take into consideration the important parameters such as reliability, packet loss, throughput, and latency. Chan et al. showed in [15] that even if we minimize the number of hops in a given route, the throughput will not be necessarily maximized.

D Couto et al. in [16] proposed metric which is called ETX (Expected Transmission Count), it is based on evaluating loss ratio to calculate the path quality and choose the link from source to destination with the high packet delivery ratio compared with other possible paths.

In [17, 18] Zaidi et al. implemented ETX in DSDV, and concluded that the use of this metric has a significant impact on network throughput. Liu et al. in [19] also compared ETX in OLSRv2 with hop count and found that the advantage of using ETX is considerable when the routes are long and traffic is high. However, when routes are short and traffic low, the difference with hop count is not remarkable.

IV. SYSTEM MODEL

Our contribution addressed the weaknesses of the previous work, in order to propose a generic approach able to automatically detect the evolution of the parameters and to adapt to the changes of the topology, in order to make the right decision and choose the appropriate number of paths.

Before starting the description of our algorithm, we will first explain the notion of degree of disjunction. It should be noted that the selection of node disjoint paths is much more difficult than those with disjoint links. However, the choice of disjointed route type can be provided by the route selection algorithm according to the route discovery results.

According to our new dynamic multipath protocol, we have been interested more in node disjoint paths, but we will also manage all the possible cases in order to choose the number of paths n variable, and the threshold k according to the neighborhood of the source and the destination, and take into account also the case where we have nodes in common, for that one will use the notion of degree of disjunction defined by the following formula:

$$\text{DisjunctionDegree}(P_1, P_2) = \frac{\min(Nt^{P_1}, Nt^{P_2}) - Nc}{\min(Nt^{P_1}, Nt^{P_2})} * 100 \quad (1)$$

- Nt^{P_i}: Total node number of route P_i excluding source and destination
- N_c: Number of common nodes between road (P_1, P_2)

As an examples shown in figure 6 the disjunction degree equal to 100%, in figure 7 the disjunction degree equal to 50%, but in figure 8 the disjunction degree equal to 0%.

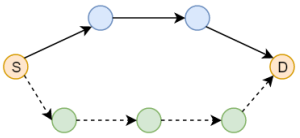


Figure 6: 100 disjoint path

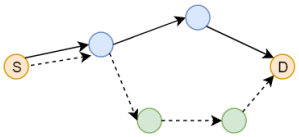


Figure 7: 50% disjoint paths

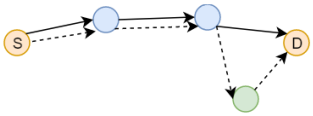


Figure 8. 0% disjoint paths

We suppose that the aim of selecting variables (n, k) (number of paths, threshold) is the use of a security method which consists on dividing the private key into multiple parts and sharing it with the communicating nodes in threshold cryptography. Thus, no node can reveal the secret without knowing the complete parts or at least threshold number of secret shares. If a new node enters the network, it can obtain the secret parts with the help of polynomial interpolation method, so in order to guarantee:

- **Confidentiality** we must have k > max (visited),
- **Availability** we must have n - k ≥ max (visited),

With max (visited) is maximum number of intersections between paths.

The following algorithm explain our approach to find variable n and k, the same algorithm is schematically presented in figure 9.

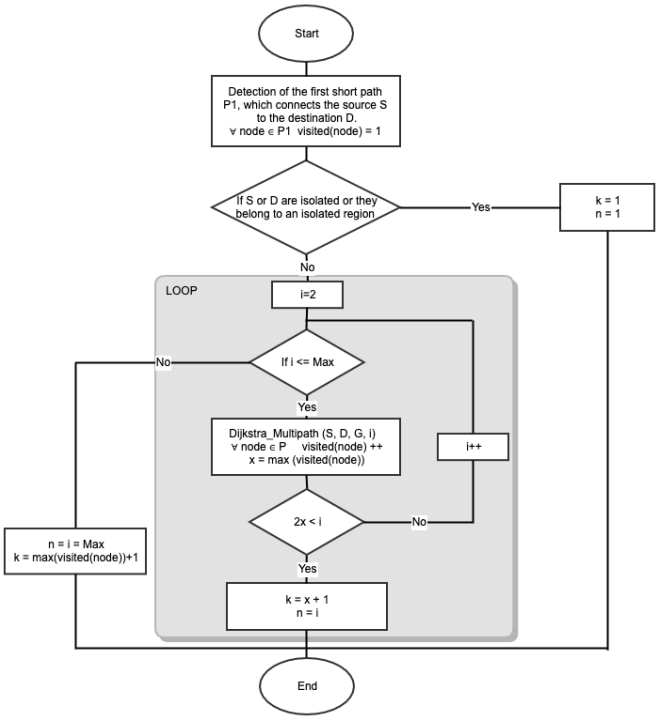


Figure 9: The proposed dynamic multipath algorithm

V. RESULTS AND DISCUSSION

In this section, we present the comparison between the standard versions of the MPOLSR and our proposed protocol D-MPOLSR.

In addition, we made several simulations with variable number nodes.

The comparison between standard MPOLSR and D-MPOLSR can be evaluated using the NS2 simulator. In each simulation, we change the number of nodes in order to study the density effect in mobile environment, when using both MPOLSR and D-MPOLSR protocols.

For all simulations in this chapter we will use the following parameters as shown in table I.

Table I: Parameters Value in simulations comparing MPOLSR / D-MPOLSR.

Parameter	Appearance
Routing Protocol	MPOLSR, D-MPOLSR
Number of Nodes	10, 20, 30, 40, 50, 60, 70, 80, 90 and 100 nodes
Environment Area	1500 meter x 1500 meter
MAC protocol	IEEE 802.11
Transport Layer	User Datagram Protocol (UDP)

As shown in figure 10 packer delivery ratio is better in a high network density. We observe also that the impact of the new algorithm makes a slight increase of PDR. This is justified by the fact that in D-MPOLSR there is more chance to find paths to deliver packets from source to destination.

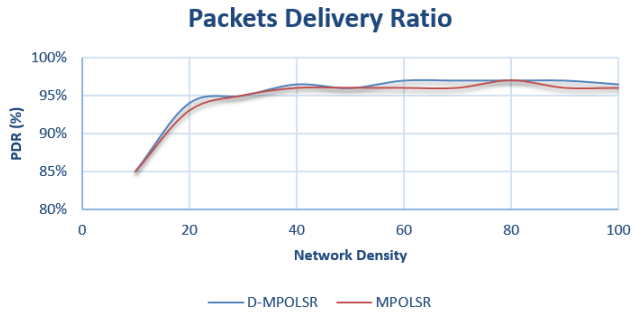


Figure 10: The evolution of PDR

In this figure 11, we analyze the average delay evolution according to network density in two simulations: MPOLSR, and D-MPOSR. As we can see, in low density network, the average delay is nearly the same for all protocols. As the density becomes higher, we observe that the end-to-end delay increases when our algorithm is implemented. This can be justified by the fact that each node performs extra processing to select paths, and calculate n and k. In addition, the paths selected using our algorithm maybe longer than those selected using standard multipath protocol, which may also generate more delay.

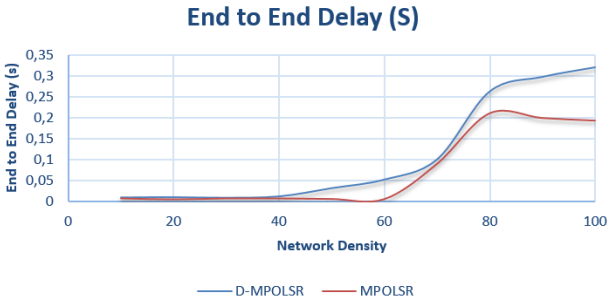


Figure 11: The evolution of the Delay

The throughput is the ratio of received packets and sent packets. It is the number of packets successfully transmitted to their destination, and it can be evaluated in packets per second or bits/sec. For a better networking quality, a high throughput is required.

We observe in figure 12 that the throughput for D-MPOLSR is better than MPOLSR, and this value increases with the network density.

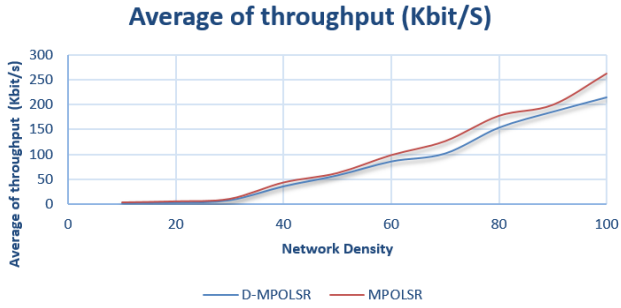


Figure 12: The evolution of the Throughput

Algorithm: Dynamic Multipath Algorithm

Initial

S: source, D: destination. Let V be a set (finite or infinite) and E a part of $V \times V$ (i.e., a relation on V). The graph $G = (V, E)$ is the pair data (V, E). The elements of V are called the vertices or nodes of G. The elements of E are called the arcs or edges of G. If V is finite, we will speak of finite graph. NT all the nodes that exist in the topology. P_i the i^{th} path found. Max is the maximum of paths. $n \leftarrow 0$ and $k \leftarrow 0$

Begin

Step 1:

The source will perform the Dijkstra algorithm to find the shortest path to the destination.
It will assign the value 1 to the visited attribute of all the nodes that make up this shortest path

Step 2:

- **If** the source or destination is isolated or belongs to an isolated region **then**

  $n \leftarrow 1$

  $k \leftarrow 1$

  break;
- **Else**

Step 3:

- **For** $i = 2 ; i =< Max ; i++$

  $Dijkstramultipath(S, D, G, i)$ is used to find i possible paths,

  increment each time the visited value of the intermediate nodes visited

  $x = max(visited)$

  If $2x < i$ **then**

  $n \leftarrow i$

  $k \leftarrow x + 1$

  break;

  Else

  continue;

  End if
- **End for**
- **If** $i > Max$ and $n = 0$ and $k = 0$ **then**

  $n \leftarrow Max$

  $k \leftarrow max(visited) + 1$

  break;
- **End if**

END

VI. CONCLUSION

Mobile networks are vulnerable to many security threats that challenge their availability, confidentiality, integrity and privacy. IoT technology is not an exception and could also be impacted by these known threats, especially the DoD and IoT implementation. In the present article, we have introduced the multipath concept. Then we have also presented a detailed literature study of multipath approach, with some proposed protocols based on this concept. We have proposed a new approach to make the number of selected routes in multipath protocols variable according to network density among other factors. This approach allows us to define the variable number of paths "n" and a threshold called "k" that will be used in the security solutions in future works.

To evaluate performance and robustness of our dynamic multipath solution, we have conducted some simulation scenarios. The obtained results show that our solution provides globally good performances, security and reliability in MANETs. We plan to use this new protocol to improve our defensive system against malicious nodes in future research works.

REFERENCES

1. D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," IEEE Access, vol. 6, pp. 4850-4874, 2017.
2. A. Khan, J. Abdullah, N. Khan, A. Julahi, and S. Tarmizi, "Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks," International Journal of Computer Science and Network Security (IJCSNS), vol. 17, pp. 357-365, 2017.
3. B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," Journal of Network and Computer Applications, vol. 131, pp. 66-74, 2019.
4. L. Goubin and A. Martinelli, "Protecting AES with Shamir's secret sharing scheme," in International Workshop on Cryptographic Hardware and Embedded Systems, 2011, pp. 79-94.
5. W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks," Wireless Networks, vol. 15, pp. 279-294, 2009.
6. F. El Mahdi, A. Habbani, Z. Kartit, and B. Bouamoud, "Optimized Scheme to Secure IoT Systems Based on Sharing Secret in Multipath Protocol," Wireless Communications and Mobile Computing, vol. 2020, 2020.
7. K. Witrisal, P. Meissner, E. Leitinger, Y. Shen, C. Gustafson, F. Tufvesson, et al., "High-accuracy localization for assisted living: 5G systems will turn multipath channels from foe to friend," IEEE Signal Processing Magazine, vol. 33, pp. 59-70, 2016.
8. S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240), 2001, pp. 3201-3205.
9. P. Papadimitratos, Z. J. Haas, and E. G. Sirer, "Path set selection in mobile ad hoc networks," in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002, pp. 1-11.
10. J. Yi and B. Parrein, "Multipath Extension for the Optimized Link State Routing Protocol Version 2 (OLSRv2)," 2017.
11. F. El Mahdi, B. Bouamoud, and A. Habbani, "Analyzing security in Smart cities networking and implementing link quality metric," in 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), 2019, pp. 1-8.
12. M. Souidi, A. Habbani, H. Berradi, and F. El Mahdi, "Geographic forwarding rules to reduce broadcast redundancy in mobile ad hoc wireless networks," Personal and Ubiquitous Computing, vol. 23, pp. 765-775, 2019.
13. J. Yi, E. Cizeron, S. Hamma, and B. Parrein, "Simulation and performance analysis of MP-OLSR for mobile ad hoc networks," in 2008 IEEE Wireless Communications and Networking Conference, 2008, pp. 2235-2240.
14. J. Yi, A. Adnane, S. David, and B. Parrein, "Multipath optimized link state routing for mobile ad hoc networks," Ad hoc networks, vol. 9, pp. 28-47, 2011.
15. L.-W. Chen, W. Chu, Y.-C. Tseng, and J.-J. Wu, "Route throughput analysis with spectral reuse for multi-rate mobile ad hoc networks," Journal of information science and engineering, vol. 25, pp. 1593-1604, 2009.
16. D. S. J. De Couto, "High-throughput routing for multi-hop wireless networks," Massachusetts Institute of Technology, 2004.
17. Z. Zaidi, T. Y. Tan, and Y. Cheng, "ETX could result in lower throughput," in 2009 Proceedings of 18th International Conference on Computer Communications and Networks, 2009, pp. 1-6.
18. F. E. Mahdi, A. Habbani, N. Mouchfiq, and B. Essaid, "Study of security in MANETs and evaluation of network performance using ETX metric," in Proceedings of the 2017 International Conference on Smart Digital Environment, 2017, pp. 220-228.
19. N. Liu and W. K. Seah, "Performance evaluation of routing metrics for community wireless mesh networks," in 2011 Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2011, pp. 556-561.

AUTHORS PROFILE

Fatna EL MAHDI was born in Rechida, Morocco, in 1990. Received her engineering degree in 2013 from National High School for Computer Science and Systems Analysis (ENSIAS) in Agdal, Rabat, Morocco.

Her current research interest is security of routing protocols in mobile ad-hoc networks. She is currently PhD students at the same school (ENSIAS) Mohammed V University, within Smart Systems Laboratory (SSL).

Mohammed SOUIDI received his engineering degree in 2009 from the National School of Computer Science and System Analysis (ENSIAS) in Rabat. He worked as Information Technology project engineer in Morocco Telecom.

His current interest is the optimization of the routing protocols in mobile Ad Hoc networks. He is currently PhD student at ENSIAS whithin the team Smart Systems Laboratory.

Halim Berradi received the state engineer degree from the ENSAT attached to ABDMALEK ESSADI, Tangier, in 2012. He is currently pursuing the Ph.D. degree with the Laboratory of Smart Systems (SSL), at the National School of Computer Science and Systems Analysis (ENSIAS) attached to Mohammed V University, Rabat, Morocco. Her research interests include the security of smart cities and systems based on new technologies.

Ahmed Habbani full professor of Higher Education at the National School of Computer Science and Systems Analysis (ENSIAS) attached Mohammed V University, Rabat, Morocco. He received his Ph.D. degree in Applied Sciences in laboratories: LEC (Laboratory of Electronics and Communications) of the EMI (Mohammedia School of Engineers) attached to the University Mohamed V Rabat, and LISIF (Laboratory of Instruments and Systems of Ile de France) of the Pierre et Marie Curie University, FRANCE.

His research interests include Modeling, development and implementation of : Mobile Intelligent Digital System; Routing Protocol (information collected to provide security, mobility, multipath and GPS rental);Smart grid ;Smart wireless sensors networks.