International Journal of Grid Computing & Applications (IJGCA) Vol.6, No.1/2, June 2015

IMPACT ANALYSIS OF BLACK HOLE ATTACKS ON MOBILE AD HOC NETWORKS PERFORMANCE

Mohamed Elboukhari[1], Mostafa Azizi[1] and Abdelmalek Azizi[2,3]

[1]Department of Applied Engineering, ESTO, Oujda, Morocco

[2]Departement Mathematics & Computer Science, FSO, Oujda, Morocco

[3]Academy Hassan II of Sciences & Technology, Rabat, Morocco

ABSTRACT

A Mobile Ad hoc Network (MANET) is a collection of mobile stations with wireless interfaces which form a temporary network without using any central administration. MANETs are more vulnerable to attacks because they have some specific characteristics as complexity of wireless communication and lack of infrastructure. Hence security is an important requirement in mobile ad hoc networks. One of the attacks against network integrity in MANETs is the Black Hole Attack. In this type of attack all data packets are absorbed by malicious node, hence data loss occurs. In this paper we investigated the impacts of Black Hole attacks on the network performance. We have simulated black hole attacks using Network Simulator 2 (NS-2) and have measured the packet loss in the network without and with a black hole attacks. Also, we measured the packet loss when the number of black hole attacks increases.

KEYWORDS

Network Security, Mobile Ad Hoc Networks, MANETs, Black Hole Attack, AODV Protocol.

1. INTRODUCTION

Wireless network is the network of mobile computer nodes that are not physically wired. The main advantage of such network is communicating with rest of the world while being mobile. The disadvantages are their limited bandwidth, processing capabilities, memory and open medium. Two types of wireless network are wireless mobile ad hoc network (MANET) and fixed backbone wireless system. MANET is a group of stations which do not use a fixed a predefined infrastructure. Thus the functioning of ad hoc networks is dependent on co-operation and the trust between nodes. Computer stations aid each other in forwarding information about the network topology and hence have the responsibility of keeping the network connected.

in these type of networks each station also operates as a router and forwards data packets to the correct destination once a route is determined [1]. To maintain this connectivity stations employ routing protocols such as AODV [2] or DSR [3].

MANETs are vulnerable to several attacks and black hole attack is one of these. In this attack, a malicious station that drops all packets makes employment of the security problems of the on demand route discovery protocols like AODV. The malicious station will pretend to possess the shortest and freshest route to the destination station by manipulating the control packet [4] to attract other station to transmit their information through its station. In the route discovery mechanism of AODV, intermediate stations are responsible to seek a fresh path to the destination station, transmitting discovery packets to their neighbour stations. Malicious stations abuse this mechanism and they immediately respond to the source node with false information as they have a fresh enough path to the destination. So source station transmits its information packets via this malicious station supposing it is a true path. Also, black hole behaviour may be due to a damaged node dropping packets unintentionally. The end result of the existing of black hole stations is the loss of packets.

In our paper, we have implemented black hole attacks simulation in MANETs and have studied their influence on the network performance. We elaborated our simulations using NS-2 (Network Simulator version 2) [5]. Having elaborated a new routing protocol that simulates the black hole attacks using NS-2, we have implemented tests to analyse the network performance without and with black holes attacks. As expected, the packet delivery ratio in the network is deteriorated considerably in the presence of black hole behaviour. We concluded also that this ratio is dramatically decreased with the increase of the black hole nodes.

The paper is organized as follows: section 2 presents the MANET applications and characteristics. In section 3 we present MANET vulnerabilities and attacks. Description of black attack in AODV protocol is developed in section 4. Network simulations results are illustrated and discussed in section 5. We conclude the paper in section 6.

2. MANET CHARACTERISTICS AND APPLICATIONS

MANET possesses specific characteristics:

Autonomous and infrastructure less*:* MANET is a self-organized network, independent of any existing infrastructure and centralized network administration. Each node operates as a router and acts in distributed manner.

Multi-hop routing*:* Because there is no dedicated router in the network, since every station acts as a router and helps in forwarding data packets to the final destination station. So, information sharing among mobile nodes is made available.

Dynamic network topology: Because MANET stations change their position randomly in the network, the MANET topology changes dynamically.

Variation on link and node capabilities: Every participating station is equipped with several kinds of radio devices making the possibility of receiving and transmission capabilities. They all act on multiple frequency bands. Asymmetric links may be established due to this heterogeneity in the radio capabilities.

Energy-constrained operation: The processing capabilities of station are limited due to the batteries carried by mobile stations.

Scalability: A several of MANET applications can involve bulky networks with plenty of stations. Scalability is primordial and crucial to the flourishing operation of MANET.
There are several applications of MANETs. Some of them are described below.

Military Networks: The digital military fields need consistent communication in different ways. Most stations are implemented in moving military vehicles that can share data among them.

Sensor Networks: Sensor Network is a collection of a large number of stations named sensors, that sense a signal and send it to special destination node.

Automotive Applications: Automotive networks are extensively discussed nowadays. Vehicles can be configured to exchange messages on the road with traffic lights and with each other establishing MANETs of different sizes. This network will give drivers data about traffic congestions, the road conditions, and accident-ahead warnings which help in optimizing the traffic conditions.

Emergency services: MANETs are broadly being employed in rescue operations (floods, earthquakes, etc.).

3. MANET VULNERABILITIES AND ATTACKS

We define vulnerability as a weakness in security system. Mobile ad hoc network is more vulnerable than wired network. Some of the vulnerabilities of MANET are as follows:

Lack of centralized management: MANET does not possess a centralized monitor server. The absence of management makes the sensing of attacks very difficult; it is not simple to observe the traffic in a highly dynamic.

Resource availability: Resource availability is a big issue in MANET. To secure communication in such dynamic environment leads to the elaboration of different security schemes.

Scalability: Due to mobility of nodes, scale of ad-hoc network varying all the time. Hence scalability is a major issue concerning security. Security mechanism should be capable of managing a large network as well as small ones.

Cooperativeness: Usually routing algorithm for MANETs assumes that nodes are cooperative and non-malicious. As a result an attacker can become an essential routing agent and perturb network functionalities.

Dynamic topology: Changeable nodes membership and dynamic topology may disturb the trust relationship among nodes. Also the trust may be disturbed if some nodes are detected as compromised. This dynamic behaviour could be better protected with adaptive and distributed security mechanisms.

Limited power supply: The MANET stations require considering limited power supply that will be the source of several threats. A station for example can behave in a selfish way and does not forward packets.

Bandwidth constraint: Low capacity links exists in MANET that is susceptible to interference effects, external noise and signal attenuation.

Adversary inside the Network: The mobile nodes within the MANET can freely leave and join the network. Also the nodes within network may behave maliciously. This is a hard task to detect that the behaviour of the node is malicious. This attack hence is highly dangerous compared to the external attack. These nodes are named compromised nodes.

No predefined Boundary: In MANETs we cannot precisely define a network physical boundary. An attacker can come in the wireless medium range of a station it will be capable to exchange messages with that station. The attacks include Eavesdropping impersonation, replay, tempering and Denial of Service (DoS) attack.

Securing MANET is a more challenging task. Understanding attacks is the first step to develop a good security schemes. Security of communication in mobile ad hoc network is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to attacks than wired network. There are several attacks which present threats to MANET:

Denial of Service attack: The goal of this attack is to attack the availability of a station.

Impersonation: If the authentication process is not properly elaborated, an attacker can act as a genuine station and observe the network traffic. It can also transmit fake data packets, and obtain access to some critical data.

Eavesdropping: This attack operates passively. The node simply monitors the confidential information. This information can be later exploited by the malicious node. The secret information like location, private key, public key, password etc. can be fetched by eavesdropper.

Routing Attacks: The attacker makes routing services a target; it is an important service in MANETs.

Black hole Attack: An attacker in this type attack publishes a zero metric for all destination stations causing all stations around it to route data packets through it. A malicious node transmits fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops (absorbs) all packets that it receives instead of normally forwarding those packets. An attacker listen the requests of other nodes in a flooding based protocol.

Wormhole Attack: In a wormhole attack, an attacker captures packets at one point, tunnels them to another point, and then replays them into the network from that point. Routing services can be disrupted when routing control message are tunnelled. Wormhole attack is the tunnel between two colluding attacks.

Replay Attack: An attacker that elaborates a replay attack resend the valid information repeatedly to inject the MANET routing traffic that has been received previously. This attack targets generally the freshness of routes.

Jamming: An attacker in this attack initially observes wireless medium to specify frequency at which destination station is receiving packet (signal) from sender station. It then transmits packet on that frequency, hence that error free receptor is hindered.

Man-in-the- middle attack: An attacker sites between the receiver and sender, and monitors any information being exchanged between two stations. in some cases, Attacker may impersonate the sender or the sender.

Gray-hole attack: Gray hole attack is implemented in two phases. In the first phase the station advertise itself as possessing a valid route to a destination, while in second phase, stations drops intercepted data with a certain probability.

4. BLACK HOLE ATTACKS IN AODV PROTOCOL

MANET routing protocols are divided into three main classifications:

Table driven (proactive) protocols manage routing information between all the stations in the network. each station elaborate its own routing table that can be employed to seek out a path to a destination and data routing is stored. Whenever there is any modification in the network topology, update has to be made in the entire network [6]. Some of the table driven protocols are: Cluster Gateway switch routing protocol (CGSR), Destination sequenced Distance vector routing (DSDV), Optimized Link State Routing protocol (OLSR),Wireless routing protocol (WRP) and Fish eye State Routing protocol (FSR).

In On-demand or Reactive routing protocols routes are elaborated as and when required. When a node wants to send data to any other station, it first initiates route discovery method to discover the path to that destination station. Many kinds of on demand driven protocols have been designed such as: Dynamic Source routing protocol (DSR), temporally ordered routing algorithm (TORA), Associativity Based routing (ABR) and Ad hoc On Demand Distance Vector (AODV). Hybrid routing protocols employ both the previous types. Some different types of Hybrid routing protocols are: Distributed dynamic routing (DDR), Zone-based hierarchical link state (ZHLS) and Zone routing protocol (ZRP).

In this paper we are concentrated in analysing the effect of black hole attack on MANETs employing AODV.

AODV (Ad hoc On-Demand Distance Vector) [2] is a reactive routing protocol composed of two modules:

Route discovery module: To send data to a given station D, the source station S consults its routing table. If it finds an entry towards this station D, it employs it, else it begins a route discovery process (see Fig. 1), which consists in flooding, by the source station S, a route request (RREQ) packet towards neighbours. When RREQ packet obtained an intermediate station, this last consults it routing table to seek a fresh route (if the route sequence number is larger than that of RREQ) towards the needed destination in RREQ packet. If such a route is found, a route reply (RREP) packet is sent through the pre-established reverse route towards the source station S. If the intermediate station does not find a fresh route, it updated its routing table and sends RREQ to the neighbours. This process is reiterated until RREQ is receiving by the destination node D. The destination node D transmits RREP to S by using the pre-established reverse route.

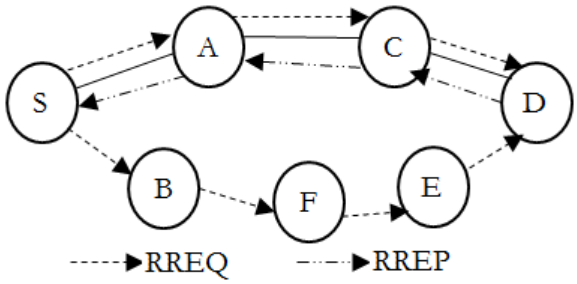

Figure 1. Route discovery mechanism of AODV protocol

Route maintenance module: AODV employs Hello messages to maintain the connectivity between nodes. Each station periodically sends a Hello packet to the neighbours and waits Hello packets on behalf of the neighbours. If Hello packets are communicated in the two directions, a symmetrical link between stations is always maintained in case of no link interrupt happened. The broken link may be repaired locally by the station upstream, else a route error (RERR) packet is sent to the source S. This last can began again, if necessary, the route discovery procedure.
MANETs are vulnerable to different attacks. General attack types are the threats against MAC, Physical, and network layer that are the most essential layers. Attacks on the network layer aims two goals: Not forwarding the data packets or modifying some attributes of routing packets. A basic attack that an adversary node can execute is to stop forwarding the data packets. As a consequence, when the attacker station is chosen as a route, it denies the data exchange to take place.

MANET that employs the AODV, a black hole station pretends to possess a fresh enough routes to all destinations needed by all the stations and drops the network traffic. When a source station floods the RREQ packet for any destination node, the black hole station immediately responds with an RREP packet that contains the highest sequence number and this packet is supposed as if

it is originating from the destination or from a station that possesses a fresh enough route to the destination station.

The source station ignores the RREP packet captured from other stations and begins to send the information packets over malicious station. An adversary node takes all the routes towards itself. It does not accept forwarding any packet anywhere. This attack is named a black hole as it swallows all objects; data packets [7].

In Fig. 2, source station S wishes to send information packets to a destination station D in MANETs. Node M is an attacker node which acts as a black hole node. The malicious node replies with false reply RREP having higher modified sequence number. So, information communication lunches from S through M instead of D.

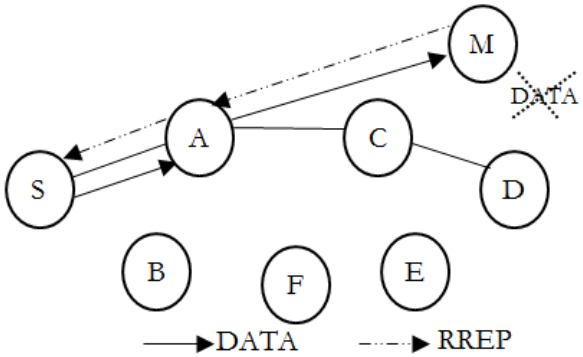

Figure 2. Black hole attack process

5. SIMULATIONS RESULTS

To understand the effects of black holes we simulated the MANET scenarios with and without a black hole nodes present in the network. To accomplish that, we introduced a new protocol which we called bAODV (blackholeAODV) into the NS-2. Nodes which behave as black hole adopts this protocol and acts exactly like black hole node as described in this article.

To study this protocol we used two scenarios of a small network. In the first simulation of our first scenario we did not have employed any black hole station and in the second simulation of this scenario we have added two black hole stations. We have then compared the results of the two simulations.

We have employed 25 stations in our tests and UDP connections are implemented between even and odd numbered stations. In this simulation the even numbered stations are the transmitting stations and odd numbered stations are the receiving stations. For example station 0 is sending to Node 1, Node 2 to Node 3, Node 4 to Node 5 and Node 6 to Node 7, etc. stations 18 to 24 are employed as black hole stations during the simulations as required. Hence, we could calculate the transmitting and received packets between any two stations. We could also count the number of packets dropped at each station including the black hole stations. This mechanism is used as a CBR (Constant Bit Rate) connection pattern of the network.

Table 1. Simulations parameters

Parameters	Value
Simulator	NS-2.34
Data packet size	512 byte
Simulation time	500 secondes
Environnement size	750×750
Number of Nodes	25
Pause time	1s
Observation parameteres	PDR (Packet Delivery Ratio)
Number of malicious nodes	1 to 7
Traffic Type	CBR
Maximum Mobilty	20 m/s
Mobility Model	Randow Waypoint [9]
Routing Protocols	AODV, bAODV

In the two scenarios, every single station is positioned at different coordinates and lunches different movements. Node movements and positions are randomly generated. For each scenario, stations change its position from a random point to a random destination point with a randomly speed. Simulation time is fixed to 500 seconds and the CBR connections lunch at the first second of the simulation and lasts for 450 seconds.

In our scenarios CBR parameters are enabled to have packet sizes of 512 bytes, and rates of 10 kbits/sec. The parameters which are set for experiments on network simulator NS-2 are described in the table 1.

For the performance analysis of the new protocol bAODV, a regular well-behaved AODV network is used as a reference. The experimental results are being elaborated under NS-2 Simulator. Also, our scenarios are tested in NAM [8] for better understanding of the nodes movement and behaviour (see Figure 3).

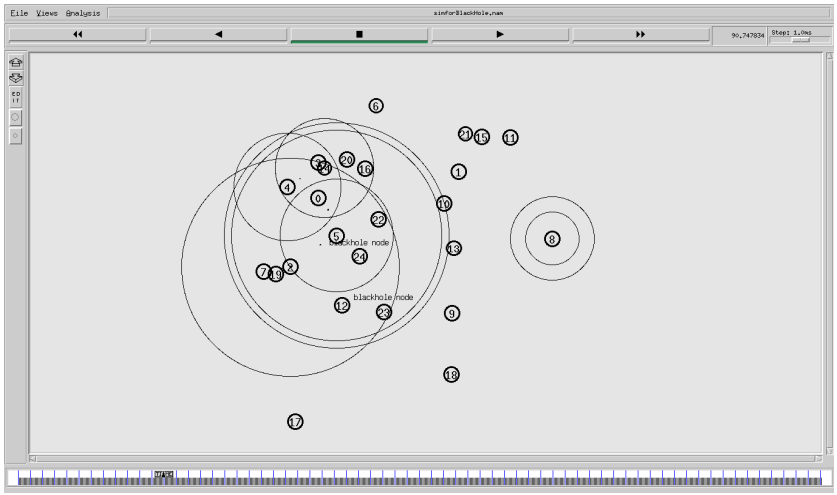

Figure 3. Simulation in NAM with two black hole nodes (node 23 and 24)

AODV and the proposed bAODV are simulated in same settings of parameters and scenarios. Experiments are run on different number of black hole nodes. Simulation provides more interest

on the network performance evaluation in term of packet delivery ratio (or packets loss) and normalized routing load where the number of block hole stations is varying.

The metric adopted to evaluate the performance is the Packet Delivery Ratio (PDR). PDR is the ratio between the number of packets originated and sent by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination. The packet loss ratio is defined as 1-PDR.

Table 2. Packet loss percentages in the network in the absence of black hole nodes

Path	packets sent	packets received	packets drepped	% of packets lost
Node 0 - Node 1	1093	1078	0,00	1,37
Node 2 – Node 3	1061	1008	0,00	4,99
Node 4 - Node 5	1100	1067	0,00	3,00
Node 6 - Node 7	1100	1085	0,00	1,36
Node 8 - Node 9	1109	1081	0,00	2,52
Node 10 - Node 11	1091	1075	0,00	1,46
Node 12 - Node 13	1116	1070	0,00	4,12
Node 14 - Node 15	1121	1024	0,00	8,65
Node 16 - Node 17	1043	954	0,00	8,53
Total	9834	9442	0,00	3,98

During the first scenario we performed two simulations. Every node is operating in cooperation with each other. The packet loss in MANET without any black hole stations is shown in Table 2. In the second simulation of the first scenario, we introduced two malicious nodes that carry out the black hole attacks in the network. In this case, nodes 23 and 24 act as a black hole stations. We measure the number of packets transmitted by the source and received by the destination station. Also we calculate how of the packets that could not obtain the destination stations are dropped in the black hole stations. These are presented in Table 3.

We give a comparison to the results of these two simulations to analyse the network behaviours. The simulation results describes that the packet loss with a black hole stations increases beyond that absorbed by the black hole stations. This we supposed to be due to the congestion augmentation in the routes through the black hole nodes.

The table III shows that the packet loss ratio decreases when there is the malicious nodes in the network. For example, in the total, the amount of packet loss ratio is 0.03 if the black hole attacks are absent. But due to event of the black hole attacks the amount of packet loss ratio increases to 0.16; some of the packets are absorbs by the black hole stations. Also, we remark from the table II that in the absence of malicious nodes there is no dropped packets. On the other hand, in the presence of black holes nodes we note that in total 82.63% of packets lost at the balck hole nodes.

Table 3: Packet loss percentages in the network in the presence of black hole nodes

Path	packets sent	packets received	packets dropped	% of packets lost	% of packets lost at the black hole nodes
0 - 1	1089	1013	67	6,97	88.15
2 - 3	1037	920	77	11,28	65.81
4 - 5	1084	875	192	19,28	91.86
6 - 7	1114	966	117	13,28	79.05
8 - 9	1156	1074	4	7,09	4.87
10 - 11	1089	986	86	9,45	83.49
12 - 13	1089	944	127	13,31	87.58
14 - 15	1056	702	299	33,52	84.46
16 - 17	1087	726	349	33,21	96.67
Total	9801	8206	1318	16,27	82.63

In the second scenario, we take 25 nodes in which nodes 0 -17 are simples nodes and 18-24 can be simple nodes or malicious nodes. The parameters in this scenario are the same as those noted in table I. Also, we adopted the same CBR connection and mobility model pattern. In this scenario, we implement a simulation to study the impact of the increase of number of black hole nodes on the PDR in the network.

Normal nodes use AODV protocol. These nodes become black hole nodes when they use bAODV protocol. So, we vary in the simulation the number of black hole nodes and we measure the ratio of PDR resulted. Table IV illustrates the results obtained of our tests. This table shows the following result: as the number of black hole nodes increases, PDR decreases dramatically. This is due the effect of malicious nodes which drop packets and by the way they do not cooperate with other nodes.

Table 4: The effect of the number of malicious node on PDR

Number of milicious nodes	0	1	2	3	4	5	6	7
% PDR	97	92	80	78	71	67	66	59

From the results of our tests presented in this table, we remark that in the absence of black hole nodes the PDR is 0.97 but when the number of black hole nodes increased to 7 the ratio of PDR becomes 0.59. This is a big decrease in packets lost in the network.

6. CONCLUSIONS

In this study we have investigated the effects of black hole nodes in ad hoc networks. We elaborate an AODV protocol that simulates the behaviour of a black hole using NS-2 simulator and we simulated scenarios each describing different MANETs with 25 stations. We add black hole stations in our simulations in the first scenario and we have provided a performance comparison of the networks without and with black hole stations. We also tested a network with black holes in the second scenario to study the effect of black hole behavior. We studied in this scenario the effect of the increase of the black hole attacks on PDR in the network.

The results demonstrate that the presence of black hole stations increases the packet loss considerably. The network experienced 16.27% packet loss on average due to the insertion of two

black hole nodes in MANET. This loss is partially (82.63%) due to packets absorbs in the black hole stations and partially due to congestion in MANET over the paths through the black hole stations.

Another result which we have elaborated is concerned with the augmentation of the number of black hole stations in MANET. Our results show that when the number of black hole stations augments, the ratios of PDR decrease dramatically. As a consequence, the packet loss increases respectively.

As a conclusion, in black hole attacks all traffics are forwarded to specific stations or from the malicious stations causing damage to the MANETs and statins as described in the result of the simulations. The detection of black hole attack in MANETs is still considered to be a challenging task.

Acknowledgements

The authors would like to thank EL MALLOUKI NASRINE for its support and help to finish this work.

REFERENCES

[1] Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[2] . Perkins, E. B. Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," RFC: 3561, Nokia Research Center, 2003

[3] D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[4] Mahmood, R.A., Khan, A.I.: A Survey on Detecting Black Hole Attack in AODVbased Mobile Ad Hoc Networks. In: International Symposium on High Capacity Optical Networks and Enabling Technologies (2007)

[5] http://www.isi.edu/nsnam/ns/

[6] M. Abolhasan, T. Wysocki, E. Dutkiewicz, ― A Review of Routing Protocols for Mobile Ad- Hoc Networks, Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[7] N.H.Mistry, D.C.Jinwals, M.A.Zaveri;" Prevention of Blackhole Attack in MANETs". In Proceedings of EPWIE- 2009, Gujarat, India, pp 89-94, July 2009.

[8] http://www.isi.edu/nsnam/nam/

[9] Deepak Dembla, Dr.Yogesh Chaba,"Modeling and Analysis of an intelligent AODV Routing Protocol based on Route Request Retransmission Strategy in MANETs", International Journal of Computer Applications (0975-8887) Volume 30-No.11 pp 6-13, September-2011

Authors

Mohamed elboukhari received the DESA (diploma of high study) degree in numerical analysis, computer science and treatment of signal in 2005 from the University of Science, Oujda, Morocco. He is currently an assistant professor, department of Applied Engineering, ESTO, university Mohamed First, Oujda, Morocco. His research interests include cryptography, quantum cryptography and wireless network security, Mobile Ad Hoc Networks (MANETS).

Mostafa azizi received the diploma of engineer in automatic and computer industry in 1993 from school Mohammadia of engineers, Rabat, Morocco and he received the Ph. D in computer science in 2001 from the university Montreal, Canada. He is currently professor at university of Mohamed first, Oujda, Morocco. His main interests include aspect of real time, embedded system, security and communication and management of the computer systems in relation with process industry.

Abdelmalek azizi received the Ph. D in theory of numbers in 1993 from university Laval, Canada. He is professor at department of mathematics in university Mohamed First, Oujda, Morocco. He is interesting in history of mathematics in Morocco and in the application of the theory of number in cryptography.