International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 5, October 2018, pp. 3103~3111
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp3103-3111

User Selective Encryption Method for Securing MANETs

Amal Ahmad[1], Shereen Ismail[2]
[1]Department of Electrical/Computer and Communication Engineering, Al-Zaytoonah Private University of Jordan,Yordania
[2]Department of Computer Science and Engineering, American University of Ras Al Khaimah, United Arab Emirates

Article Info

Article history:

Received Dec 27, 2017
Revised Jun 13, 2018
Accepted Sep 10, 2018

Keyword:

Diffie–hellman
Key management
MANET
Selective encryption
Symmetric key algorithm

ABSTRACT

Security issue is getting important day by day. At present, there are a variety of methodologies to provide protection for data confidentiality. MANETs have lots of security challenges than traditional networks like infrastructure-less and self-organizing requirements. As the MANETs are dynamic networks that's make every transmission in such networks vulnerable to many attacks and improving security level becomes a main issue. This paper introduces a user selective encryption method by operating Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) and the Diffie-Hellman Key Exchange (DHKE) protocol for key management in order to improve MANET security. Through the Network Simulator-2 (NS-2), the we investigate the performance of the proposed method in terms of data transfer time and network throughput for different data sizes and different sender-to-receiver number of hops. The results show the superiority of AES over other encryption algorithms. Furthermore, the effectiveness of our proposed method is verified through comparing our results with those obtained from previous studies.

Corresponding Author:

Shereen Ismail,
Department of Computer Science and Engineering,
American University of Ras Al Khaimah,
American University of Ras Al Khaimah Road, Ras Al Khaimah, PO BOX: 10021, UAE.
Email: shereen.subhi@aurak.ac.ae

1. INTRODUCTION

In recent years, MANETs emerged as a major wireless networking technology. However, the security issues on MANET have become a major concern [1]. MANETs are vulnerable to attacks due to dynamic nature these vulnerabilities needs efficient solutions. Another challenge when it comes to MANET security is the key management issue. To avoid malicious nodes joining the networks, it is necessary to authenticate the nodes before joining in, on the other hand due to MANETs restricted energy and limited computational capability it is necessary to design a lightweight and storage efficient key management scheme [2-3].

Ahmad, at al. [1] analyzed of DES, 3DES and AES symmetric encryption algorithms in MANET was done using the NS-2 network simulator in terms of energy consumption, data transfer time, End-to-End delay time and throughput with varying sizes of data. Firstly, the network performance was simulated assuming the availability of the common key, and secondly, the network performance was simulated including the DH Key Exchange (DHKE) protocol in the key management phase. Based on these obtained simulation results the AES was the recommended encryption scheme.

Kushwaha et al. [4] presented a novel solution for data encryption in Mobile Ad hoc Networks based on Selective encryption to improve data security. The selective encryption algorithms was used to encrypt only certain portions of the messages, actually necessary messages were encrypted to provide the needed security and confidentiality level for the transmitted Messages. An extensive analysis were carried

out using fedora Operating System and NS 2.35 and the encryption part performed by using BLOWFISH symmetric key algorithm. In this study, the proposed method named Selective Significant Data Encryption (SSDE) was compared with full encryption and Toss-A-Coin method which is a selective Encryption method, in which the whole transmitted message divided into two groups and the group to be encrypted decided by tossing a coin. The performance of the methods evaluated based on the extensive set of experiments each experiment take 3000s simulation time. The results based on the encryption time showed the efficiency of SSDE over other methods.

Ren et al. [5] proposed a probabilistic selective encryption algorithm based on symmetric key that targets to gain extra uncertainty so that only trusted receiver can decrypt the ciphertext. An extensive set of simulation experiments were carried out based on NS-2 simulator, and simulation results showed that the technique of selective algorithms reduces the encryption time overhead and increases the efficiency of data encryption in wireless Ad hoc Networks.

Sangeetha and Sathappan in [6] improved an efficient Self Organized Gradient Boosting Key Authentication (SOGBKA) technique to improve the security of higher throughput data communication in MANETs. The SOGBKA includes three main processes which are; tree building, tree pruning and optimal node selection for performing secured data transmission in network, SOGBKA technique primarily creates Gradient Boosting tree based on mobile nodes in network and then creates self-organized key for each mobile node. Then, the SOGBKA technique computes trust values of mobile node based on the rate of data packet forwarded and dropped. Then, SOGBKA technique accomplishes tree pruning which leads to eliminate the mobile node with lower trust value. This process helps to reduce the data loss rate during transmission and increases the throughput rate. In the final process, SOGBKA chooses the best node through self-organized key authentication for transmitting the data with higher security to achieve a secure data transmission in MANETs. The performance of SOGBKA technique has been evaluated based on improving the throughput rate and reducing time taken for secured data delivery in MANETs. Based on these metrics, the authors recommended SOGBKA technique because of the competitive results when compared with the state-of-the-art techniques.

Arepalli et al. [7] proposed a novel method based on Elliptic Curve Group Diffie Hellman (ECGDH) to protect MANET against man in the middle attack in PUMA routing protocol which has the best multicast routing protocol compared to tree and mesh based multicast protocols. The proposed study compared PUMA routing protocol under normal situation, attack scenario, and protecting with ECGDH security using four parameters; throughput, packet delivery fraction, control overhead and total overhead with respect to number of nodes in a group. The results showed that ECGDH security mechanism provides better throughput in attack scenario, and the performance of packet delivery has been increased compared to man in the middle attack situation. Moreover, control overhead also has been increased using ECGDH security mechanism compared to legitimate and normal situations.

Krishnappa and Babu in [8] have discussed some of the unsolved security issues after abundant research work, and focused on the potential features of Swarm Intelligence (SI) and the associated techniques that can mitigate security issues. Based on SI, the authors have concluded that the majority of the previous researches used Ant Colony Optimization (ACO) or Particle Swarm Optimization (PSO) extensively. Elaborated discussion on SI with respect to trust management, authentication, and attack models are made with support of some of the recent studies have been done in same area. The authors have also concluded that the the contribution of swarm intelligence can produce an effective security method which can be improved by the integration with game theoretic concept of visualizing and discretizing mobile nodes.

Echchaachoui, A. et al [9] proposed a new method called OLSR-SDK capable of combining high security and high performance during routing in Ad-hoc networks. The authors have used an encryption method based on dynamic asymmetric cryptography and a clustering management key distribution, and applied this method in based on OLSR routing protocol. The proposed study focused on certain types of attacks, the authors selected two different attacks for simulation and testing; Black-Hole and DDOS. The obtained results have been compared with standard OLSR and showed that OLSR-SDK provided high security level, and greatly improved traffic performance (RDP 18% improvement and delay 19% improvement) against DDOS attack that directly target nodes. Under Black-Hole attack, the OLSR-SDK provided better transmission delays of 32% but did not improve packet delivery rate, causing a slight deterioration of 2%.

More proposed performance simulation studies for various symmetric key algorithms such as RC4, AES, Blowfish, RC2, DES, Skipjack and 3DES with varying parameters such as; data block size, and key size and different performance metrics like; encryption-decryption time, CPU process time, throughput and power consumption have been proposed in [10-17]. The rest of this paper is organized as follows; section 2 to 4, the system characteristics and simulation parameters, simulation environment, and simulation metrics and assumption are presented respectively. In Section 5, a detailed description for the proposed user selective

encryption method is illustrated, this section icludes the implementation procedure of the six offered cryptographic schemes built in NS-2 simulator. In section 6, the simulation scenarios and experimental results are discuused. Finally, this paper is concluded in section 7.

2. SYSTEM CHARACTERISTICS AND SIMULATION PARAMETERS

The proposed system and the simulation experiments have been conducted on NS-2. The network is configured to use AODV routing protocol using the command set val(rp) AODV. The Mac layer, data rate, transmission range, simulation area, simulation time, number of nodes and other details are set in Network Configuration File (NCF). The main network configuration parameters are summarized in Figure 1.

```
# Initialize some parameters

Mac/802_11 set dataRate_ 11Mb
Mac/802_11 set RTSThreshold_ 3000
set sim(end) 20.0
set val(chan)           Channel/WirelessChannel    ;
set val(prop)           Propagation/TwoRayGround   ;
set val(netif)          Phy/WirelessPhy            ;
set val(mac)            Mac/802_11                 ;
set val(ifq)            Queue/DropTail/PriQueue    ;
set val(ll)             LL                         ;
set val(ant)            Antenna/OmniAntenna        ;
set val(ifqlen)         50                         ;
set val(nn)             10                         ;
set val(rp)             AODV                       ;
```

Figure 1. Ad hoc NCF

3. SIMULATION ENVIRONMENT

We have run our simulation on a computer system with the specification described in Table 1. The performance evaluation for the proposed user selective encryption method has been carried out using NS-2 with the simulation parameters summarized in Table 2.

Table 1. System Configuration

Operating System	Redhat version 6.0.52 - Linux 2.2.x Kernel
Memory	2 GB
C++ Compiler	gcc version 4.3.0
TCL/TK version	8.4.11

Table 2. Simulation Parameters

Parameter	Value
Simulator	NS-2 (V- 2.29)
MAC Layer	802.11 datarate_ 11 MB
Simulation Time	200 sec
Simulation Area	2000 m * 2000 m
Transmission Range	250 m
Routing Protocol	AODV
Packet Size	1 KB

4. SIMULATION METRICS AND ASSUMPTIONS

In our simulation experiments, evaluating the performance of the implemented cryptographic schemes in Ad hoc network depends upon several factors:

a. Encryption schemes: three symmetric encryption algorithms DES, AES (128 key) and 3DES.
b. Number of hops: three main scenarios; a single hop, two hops and three hops between source and destination nodes.
c. Data file size: 2KB, 4KB, 8KB, 16KB, 32KB, 64KB, 128KB and 256KB.
d. Simulation modes: simulation mode 1 assuming the availability of the common key, and simulation mode 2 simulates the network behavior including the key management phase in the link sensing between the source and the destination nodes to ensure a reliable and secure key management.

5. DESCRIPTION OF THE PROPOSED SELECTIVE ENCRYPTION METHOD

In this paper, a user selective encryption method is proposed which hires the main three symmetric encryption algorithms: Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES) so the user is able to choose the suitable encryption algorithm according to MANET application and the security level required.

During the security establishment process, both source and destination nodes should select the required symmetric encryption algorithm by feeding NCF with the encryption type number as shown in Figure 2. The encryption type received from the NCF attached with the *encr* variable that presents the encryption type using the bind *("encr",&encr)* statement.

```
set mmapp1 [new Agent/sec]

$mmapp1 set addr $x0
$mmapp1 set dst  $x4
$mmapp1 set encr 4
$mmapp1 set key 11
#$mmapp1 set size_ 0
$mmapp1 set sender 1

set mmapp2 [new Agent/sec]

$mmapp2 set addr $x4
$mmapp2 set dst  $x0
$mmapp2 set encr 4
$mmapp2 set key 11
$mmapp2 set size_ 0
$mmapp2 set sender 0

$node_(0) attach $mmapp1 200
$node_(4) attach $mmapp1 200
```

Figure 2. Setting the encryption type in NCF

The cryptographic schemes that are implemented in the proposed selective encryption method are detailed in Table 3, which reflects the two adopted modes in our performance evaluation experiments; simulation mode 1 consider the availability of the common key that will be used in the selected encryption algorithm, and simulation mode 2 establish the key in a secure manner using the DH algorithm before the actual data encryption procedure has started.

Table 3. The Implemented Cryptographic Schemes

Encryption Type	Description
Encr 0	3DES
Encr 1	DES
Encr 2	AES
Encr 3	DES-DHKE
Encr 4	AES-DHKE
Encr 5	3DES-DHKE

Upon the reception of the encryption scheme, the data encryption is started and then the final encrypted packets are sent out from source using the function *void sec::snd_enc_pkt()* with particular lengths immediately to the destination node. The performance of the proposed method is examined and evaluated through conducting many network simulation experiments with the different implemented cryptographic schemes. For simulation environment, the following assumptions are taken:

a. Free space network with no multipath and/or fading
b. No noise affecting the network
c. 20 repetitions for each experiment

The performance metrics we use for the comparisons between the different schemes:

a. The data transfer time for varying data sizes (in sec)
b. The data transfer for varying number of hops (in sec)
c. The network throughput for varying data sizes (in KB/sec)
d. The network throughput for varying number of hops (in KB/sec)

6. SIMUALTION SCENARIOS AND RESULTS

This section discusses the performance results of the proposed user selective encryption method based on the selected metrics upon varying factors according to the following scenarios.

6.1. Scenario #1: Data Transfer Time for Varying Data Size

The data transfer time is considered the time starting from the encryption process of the first packet in a selected data file till the end of the last encrypted packet in the decryption process that have reached the destination node and calculated according to the following equations:

$$T_r = T_e + T_d + T_{EE} \quad (1)$$

$$T_e \cong T_d \cong \sum_1^{N_p} T_i \quad (2)$$

$$N_p = F_s/P_s \quad (3)$$

Where: T_r is the transfer time (in sec)
T_e is the encryption time (in sec)
T_d is the decryption time (in sec)
T_{EE} is the End-to-End delay time (in sec)
N_p is the number of packets in single data file
T_i is the time taken to encrypt a single packet (in sec)
F_s is the data file size
P_s is the single packet size

For the implemented encryption schemes in the proposed method, the transfer time results are shown in Table 4 for simulation mode 1 and Table 5 for simulation mode 2.

Table 4. Transfer Time Results-Simulation Mode 1

File Size (Kb)	Transfer Time (sec)		
	DES	AES	3DES
2	0.78	0.06	2.34
4	1.55	0.11	4.61
8	3.15	0.19	9.23
16	6.36	0.38	18.62
32	13.09	1.09	37.81
64	33.36	3.32	96.16
128	68.76	7.12	198.22
256	141.73	17.37	436.61

Table 5. Transfer Time Results-Simulation Mode 2

File Size (Kb)	Transfer Time (sec)		
	DES-DHKE	AES-DHKE	3DES-DHKE
2	1.76	1.04	3.32
4	2.53	1.09	5.6
8	4.13	1.17	10.21
16	7.34	1.36	19.6
32	14.07	2.07	38.79
64	34.34	4.3	97.14
128	69.74	8.09	199.19
256	142.71	18.35	437.59

These experimental results show that the AES transfer time is approximately 90% less than DES when running simulation mode 1. On the other hand, AES consumes approximately 25% transfer time less than DES for small data files and (57%-80%) less than DES for larger data files when applying the DHKE protocol in simulation mode 2. Another important observation is that the DHKE calculations will add approximately 28% time overhead to the overall transfer time results if we use a 2 Kbits prime number in the DHKE protocol. The relationship between raising the number of bits of the prime number used in DH and the calculations time overhead consumed by the algorithm as obtained from our experiments is shown Figure 3.

Figure 3. The number of prime number bits vs. DHKE calculations time overhead time results for the two simulation modes

6.2. Scenario #2: Data Transfer Time for Varying Number of Hops

Simulation experiments are conducted to study the effect of number of hops on data transfer time for the six implemented encryption schemes in the proposed user selective encryption method. In Figure 4, we can see three cases are tested for each implemented cryptographic scheme; a single hop, two hops and three hops in the path between source and destination nodes.

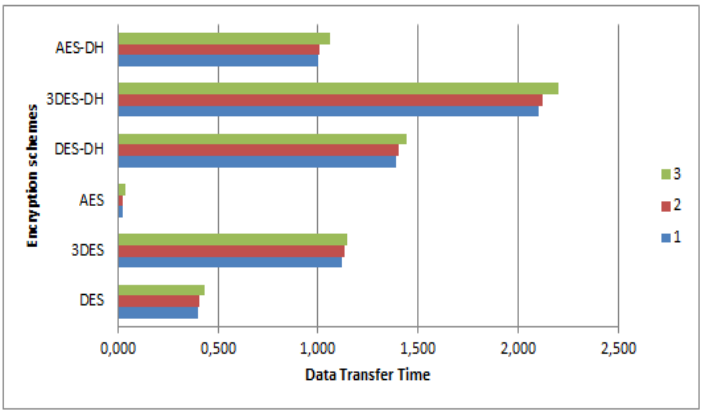

Figure 4. Data transfer time for varying number of hops

As we can notice from Figure 4, an advantage of using the AES encryption scheme is that it takes less data transfer time than DES and 3DES encryption schemes. This seems sensible compared with the conclusions in other studies such as [11] and [16] in which the authors ended their papers by concluding that AES is faster and more efficient than DES and 3DES encryption algorithms. In the proposed user selective encryption method, this is actually the case under the two adopted simulation modes.

6.3. Scenario #3: Network Throughput for Varying Data Size

Network throughput while running the implemented cryptographic schemes is calculated by normalizing the total encrypted file size in bytes by the data transfer time using the following formula:

$$Throughput = size\ of\ plain\ text\ /\ time\ consumed\ during\ encryption \quad (4)$$

For different data file sizes, throughput results are shown in Table 6 and Table 7 while running the two simulation modes.

Table 6. Throughput Results-simulation Mode 1

File Size (Kb)	Throughput (Kb/sec)		
	DES	AES	3DES
2	2.57	36.17	0.86
4	2.58	36.2	0.87
8	2.54	43.24	0.87
16	2.52	42.67	0.86
32	2.44	29.5	0.84
64	1.92	19.31	0.67
128	1.86	17.98	0.65
256	1.8	14.74	0.59

Table 7. Throughput Results-simulation Mode 2

File Size (Kb)	Throughput (Kb/sec)		
	DES-DHKE	AES-DHKE	3DES-DHKE
2	1.14	1.93	0.60
4	1.58	3.67	0.72
8	1.94	6.86	0.78
16	2.18	11.8	0.82
32	2.28	15.49	0.83
64	1.86	14.9	0.66
128	1.84	15.8	0.64
256	1.79	13.95	0.59

6.4. Scenario #4: Network Throughput for Varying Number of Hops

The Network Throughput that is measured with the three different senarios of hop count between source and destination are illustrated in Figure 5. Generally, it is clearly noticable that the AES has the superiority over the DES and 3DES algorithms in the two simulation modes for the conducted experiments but still the user has the ability to choose among the six implemented encryption schemes to secure his communication according to MANET application and the security level required.

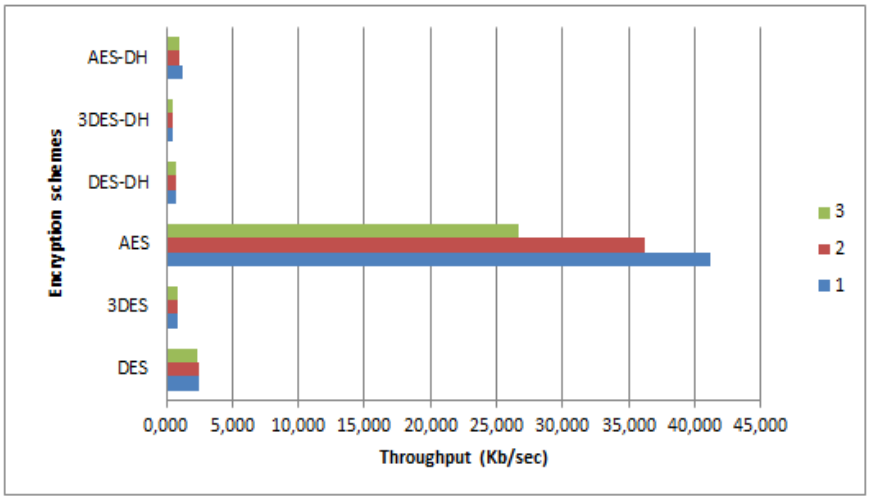

Figure 5: Network throughput for varying number of hops

Compared with the results obtained from Norouzi, et al. [17] and Elminaam, et al. [11], our results seem to be sensible. As far as throughput is concerned, AES produce highest throughput among the three implemented algorithms as shown in Figure 5. On the other hand, Elminaam, et al. in [11], the authors define throughput of a certain encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time which can consider as a good indicator for power consumption. In other words, the authors' study has ended with a very important observation which is; when the encryption time increases significantly the throughput will decrease as our results show in Figure 4 and Figure 5 for small to medium input data files.

7. CONCLUSION AND FUTURE WORK

In this paper, the performance of DES, 3DES and AES symmetric encryption algorithms have been evaluated under MANET environment. Moreover, we have applied a secure key management solution using the DHKE protocol. We offered the MANET user the ability to dynamically choose the preferred encryption scheme based on the security level required. Many simulation experiments have been conducted and eventually showed the superiority of AES algorithm over DES and 3DES for all performance metrics.

Security in Ad hoc networks is an important research topic. The suitability of the cryptographic solutions with Ad hoc limitations will always be challenging. Analyzing and evaluating the performance of other symmetric and Asymmetric ciphers and testing or proposing an effective and efficient key exchange methods using different network topologies assuming new nodes joining or leaving the network will be a valuable future work suggestions.

REFERENCES

[1] Ahmad A, Swidan A, Saifan R. COMPARATIVE ANALYSIS OF DIFFERENT ENCRYPTION TECHNIQUES IN MOBILE AD HOC NETWORKS (MANETS).
[2] Chen J, Wu J. A Survey on Applied Cryptography in Secure Mobile Ad Hoc Networks and Wireless Sensor Networks. Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice: From Principle to Practice. 2010 Feb 28:262.
[3] Du D, Xiong H. A dynamic key management scheme for MANETs. InCross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011 2011 Jul 26 (Vol. 1, pp. 779-783). IEEE.
[4] Kushwaha A, Sharma HR, Ambhaikar A. A Novel Selective Encryption Method for Securing Text Over Mobile Ad Hoc Network. Procedia Computer Science. 2016 Jan 1;79:16-23.
[5] Ren, Y., Boukerche, A., & Mokdad, L. (2011, March). Performance analysis of a selective encryption algorithm for wireless ad hoc networks. In Wireless Communications and Networking Conference (WCNC), 2011 IEEE (pp. 1038-1043). IEEE
[6] Sangeetha MS, Sathappan S. Self Organized Gradient Boosting Key Authentication for Secured Data Communication in Mobile Ad-hoc Network. International Journal of Applied Engineering Research. 2017;12(18):7823-32.
[7] Arepalli G, Erukula SB. Secure Multicast Routing Protocol in Manets Using Efficient ECGDH Algorithm. International Journal of Electrical and Computer Engineering. 2016 Aug 1;6(4):1857.
[8] Krishnappa PK, Babu BP. Investigating Open Issues in Swarm Intelligence for Mitigating Security Threats in MANET. International Journal of Electrical and Computer Engineering. 2015 Oct 1;5(5).
[9] Echchaachoui, A., Choukri, A., Habbani, A., & Elkoutbi, M. (2014, April). Asymmetric and dynamic encryption for routing security in MANETs. In Multimedia Computing and Systems (ICMCS), 2014 International Conference on (pp. 825-830). IEEE.
[10] Masram, R. Shahare, V. Abraham, J. and Moona, R. (2014), Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features. International Journal of Network Security & Its Applications, 6(4).
[11] Elminaam, D. S. Kader, H. M. A. and Hadhoud, M. M. (2009), Energy Efficiency of Encryption Schemes for Wireless Devices. International Journal of Computer Theory and Engineering, 1, 302-309.
[12] Singh, S. and Maini, R. (2011), Comparison of Data Encryption Algorithms. International Journal of Computer Science and Communication, 2(1), 125-127.
[13] Kumar, M. A. and Karthikeyan, S. (2012), Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. International Journal of Computer Network and Information Security (IJCNIS), 4(2), 22.
[14] Thakur, J. and Kumar, N. (2011), DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International journal of emerging technology and advanced engineering, 1(2), 6-12.
[15] Mandal, A. K. Parakash, C. and Tiwari, A. (2012), Performance Evaluation of Cryptographic Algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference, IEEE, 1-5.
[16] Elminaam, D. S. A. Abdual-Kader, H. M. and Hadhoud, M. M. (2010), Evaluating the Performance of Symmetric Encryption Algorithms. IJ Network Security, 10(3), 216-222.
[17] Norouzi, M. esmaeel Akbari, M. and Souri, A. (2012), Optimization of Security Performance in MANET. Journal of American Science, 8(6).

BIOGRAPHIES OF AUTHORS

Amal Ahmad Author is with Department of Electrical /Computer and Communication Engineering, Al-Zaytoonah Private University of Jordan, phone: 00962-6-4291511; fax: 00962-6-4291432; e-mail: Amal.q@zuj.edu.jo).

Shereen Ismail Author is with Department of Computer Science and Engineering, American University of Ras Al-Khaimah, Ras Al Khaimah, UAE, phone:00971-505373477 (e-mail: shereen.subhi@aurak.ac.ae).