Research Journal of Applied Sciences 9 (8): 466-473, 2014
ISSN: 1815-932X

The Necessity of Integrating Security as a QoS Parameter in Mobile Ad Hoc Networks

Ola M. Daoudeyeh and Rosilah Hassan
Faculty of Information Science and Technology,
University Kebangsaan Malaysia, 43600 Bangi,
Selangor Darul Ehsan, Malaysia

Abstract: Security and Quality of Services (QoS) are joined together in different ways: securing the QoS routing protocol from being interfered to prevent incorrect route choice, Quality of Security Services (QoSS) that concerns about securing the users applications and finally integrating security as QoS parameters thus beside the normal QoS the user can also request for a certain level of security. This study will look to the necessity of integrating security as a QoS parameter from additional point of view. Even though the QoS routing protocol chose the best route to achieve the requested QoS constraint yet the requested level of service is not achieved. This study claims that the reason behind that is the unsecured route where in the packet transmission phase security attacks can seriously harm the delay, throughput, packet delivery ratio or any other QoS requests. This study contribute and prove the need of adding security levels to the QoS routing table metrics as a second pair. The security level needed should be calculated on the QoS framework such a framework could be named as QoS++.

Key words: QoS, security, integrating security, ad hoc, MANETs

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are an infrastructure less networks where all the nodes in this network are free to move in any speed and any direction. This kind of networks gains more and more attention and the numbers of MANET's users are becoming larger and larger (Lu, 2008). A commonly used example of MANET's application is the battlefield environment (Witt and Turau, 2005; Conti and Giordano, 2007) where tanks use the air as the media to communicate. Earthquake rescue operations are another example of MANET applications since working in areas lack for infrastructure is one of MANET's main features, in addition to limited resources, free mobility and other characteristics (Hassan *et al*., 2010; Mohseni *et al*., 2010). MANET applications no more restricted to such kind of examples, it exceeded them to serve users in conference rooms or even in small workshops. Quality of Service (QoS) concerns about the users demanded level of service (Reddy *et al*., 2006). End users applications vary in their QoS constraints for example multimedia application users prefer to have the minimum jitter and/or minimum delay, other applications could request for a minimum bandwidth or other QoS. QoS frameworks and tools use a QoS routing protocols to find the best route that achieves the requested level of service (Kar *et al*., 2000; Ong, 2003; Sarma *et al*., 2008). Security also is a great issue in MANET, one of the main reasons is the absence of a centralized point or a network backbone.

Security and QoS in mobile ad hoc networks are discussed and joined together in different ways (Adibi and Agnew, 2008): securing the QoS routing protocol from being interfered to prevent incorrect or non-ultimate route choice, Quality of Security Services (QoSS) that concerns about securing the users applications (i.e., the level of application securing of spywares, malwares, viruses, etc.) and finally integrating security as QoS parameters (Duflos *et al*., 2005), thus beside the normal QoS constraints (delay, Jitter, bandwidth, etc.) the user can also request for a certain level of security. For example if the user needs to brows the net, normally the medium or even low level of security is enough since the connection does not include any sensitive information. But, this is not the case if he/she needs to access an online banking account where the highest level of security is demanded to avoid sensitive data reveal. Therefore, considering security as a QoS parameter gives the chance to choose the level required a reasonable reason of doing so is that having the highest

Corresponding Author: Ola M. Daoudeyeh, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600 Bangi, Selangor Darul Ehsan, Malaysia

level of security all the time and for all the connection sessions might be very costly in terms of money and network resources. Even that this approach is a new topic and is rarely discussed this study will look to the necessity of integrating security as a QoS parameter from additional point of view.

When a user needs to establish a session with certain level of service he/she choose the QoS constraint (maximum delay, maximum Jitter, Minimum Bandwidth, etc.) and the level required of this constraints. In the second step the routing protocol try to find the best route that can deliver the packets with the required QoS needs. After choosing the QoS route the packets start to flow from the source to the distention via the selected route (Fig. 1). The known security and QoS couplings are also illustrated in Fig. 1 where in step one, the QoS scan be found which as mentioned before concerned about the quality of the security provided to protect the user applications.

Step two, researchers can find security the newly added quality of service constraint where the user can ask for a cretin level of security as he needs. Just like any other QoS constraints.

Step three comes securing the QoS routing protocol, many security attacks target the route finding process and the routing table, therefore assuring that routing protocol is well protected prevent any faulty routing information and/or incorrect route selection.

Step four, when the packets starts to go through the route which claimed to achieve the requested QoS constraint they could go under attacks of un-behaved nodes in the route itself or by the neighboring nodes. Those attacks could cause in different problems such as increasing the delay, Jitter or eating up the bandwidth (Nichols and Lekkas, 2002; Sakarindr *et al*., 2005). Even though, there are plenty of protocols that have security in mind for this stage (packet delivery stage). But, they don't think about security for QoS benefit.

To make it more clear, let's say that the user or an application is running an online video, like most of the multimedia applications the most important thing is to have the minimum Jitter thus the user have to request a QoS with a minimum amount of Jitter. The process will go through the four steps mentioned earlier. And the packets start to be received through the selected QoS route till this point everything goes perfect, unless this route is under attack. Security attacks can be harmful in many ways but in general those attack cause in harming the QoS constraints in a way or another. As a result the user will not get the required service and the QoS framework and the QoS routing protocol fail to deliver the appropriate results.

The problem statement behind this work is that even though the QoS routing protocol find and chose the best route it could had to achieve the QoS constraints which is requested by the user or by one of the applications still the level of service requested is not achieved.

This study claims that the reason behind that is the unsecured route where in the packet transmission phase security attacks can seriously harm the delay, throughput, packet delivery ratio or any other QoS requests. This study prove the need of adding security levels to the QoS routing table metrics as a second pair for example each path have a weight of (delay time, security level) (Fig. 2). So, when the user asks for a cretin maximum delay time let say D the level of security needed should be calculated let say DS the routing protocol should find a route that satisfy the D delay value and at the same time satisfy the security level DS. The security level needed should be calculated on the QoS framework such a framework could be named as QoS++.

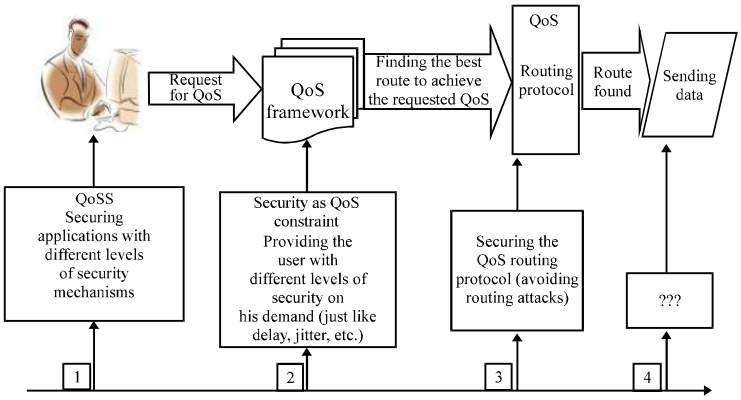

Fig. 1: Quality of Service (QoS) and security

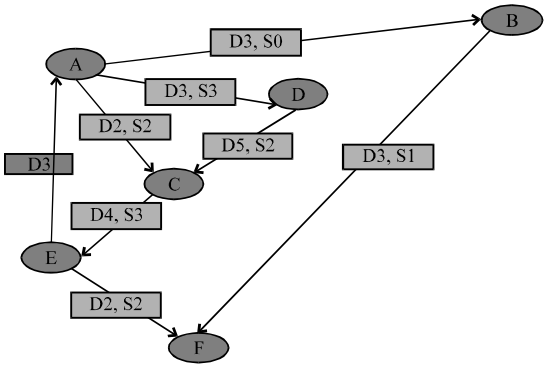

Fig. 2: Route weight with security added

QoS CONSTRAINTS AND SECURITY ATTACKS

In this study, researchers will discuss how security attacks affect the QoS main constraints. Since, delay and jitter is so related, researchers chose delay to represent both. In other hand, since the probability of packet loose directly affects the total throughput, researchers consider the total throughput and finally the essential constraints, bandwidth. Researchers will not consider the cost here as for the maximum of the knowledge there is no security attacks can directly affect the cost. Many researchers like by Mishra (2008), see that QoS and security is best treated as independent aspects even they have some dependences. Researchers gave how heavy computational of a Cryptography algorithm can increase the delay as an example of how QoS and security can affect each other. At this point, researchers will study the effect of being inside unsecure transmission environment on QoS constraints. Table 1 summarize the most known security attacks in MANETs and mark if they have influence on each of bandwidth, throughput or delay (Anantvalee and Wu, 2007; Xiao *et al*., 2007; Mohamad *et al*., 2009). The repudiation attack can be cover for many other attacks that can affect the three constraints, jamming for instance can consume the bandwidth, delay the packet transmission and may cause packet drooping if they exceeds the dedicated time to arrive which in turn minimize the throughput. Malicious code attacks can greatly maximize the delay namely the processing delay, trying to guarantee a minimum delay in presence of such attack will be difficult to achieve. At the same time, it can affect the throughput. In general, researchers can say that any significant delay can cause packet loose and decrease the total throughput. Both sessions hijacking and SYN flooding attacks, eat up the bandwidth by keep sending the RREQ and jamming the

Table 1: Security attacks and the main QoS constraints

Attacks	Bandwidth	Throughput	Delay
Repudiation attacks	✓	✓	✓
Malicious code attacks	-	✓	✓
Session hijacking	✓	✓	✓
Syn flooding	✓	✓	✓
Blackhole attack	-	✓	-
Rushing attack	✓	✓	✓
Neighbor attack	-	-	-
Jellyfish attacks	-	-	✓
Byzantine	-	✓	✓
Resource consumption attack	✓	-	✓
Wormhole attack	-	-	✓
Mac layer jamming	✓	-	✓
Eavesdropping	-	-	-
Interference and jamming	✓	✓	-
Denial of Service (DoS)	✓	✓	✓
Man in the middle attack	-	-	-
Impersonation attacks	-	-	-
Routing protocols attacks	✓	✓	✓

link. Due to that delay increase and packet loose probability is higher, blackhole attack mainly affects the throughput when the attacker intentionally drops the packets instead of delivering them. Rushing attack has the same effect as the SYN flooding. Jellyfish attack aims to increase the delay even it does not intentionally droop the packet delaying them may lead to that. The routing loops created by the Byzantine attack can affect the end to end delay, moreover the Byzantine affect the throughput due to packet drooping. In the resource consumption, attack the bandwidth might be affected during the attacker attempt to consume the victim's resources. A delay can be created due to this attack since the victim's CPU and other resources are not running with their normal capacity.

Wormhole attack mainly affects the throughput since the transmitted packets are not delivered to the intended receiver. Mac layer jamming can affect the bandwidth and delay. Interference attack can cause packet loose and bandwidth degradation, same do the denial of service attack in addition it can affect the delay as well. Routing protocols attacks (RREQ flooding, acknowledgment flooding, routing table overflow, routing loop, route broken message, etc.) normally lead to the three constraints harmful. Where, some other attacks like the Neighbor attack, Eavesdropping, Man in the middle and the impersonation attacks do not have a noticeable effect on bandwidth, throughput and delay.

Depending on Table 1, researchers can see that there is a tight relationship between security and QoS. Without applying the appropriate security mechanisms and preventing attacks assuring the QoS services and requirements will be difficult to achieve and unreliable. Therefore, QoS and security should be treated as a one compound area when dealing with the type and level of service provided to the user.

SIMULATION

The aim of this research is to test the effect of the security attacks on some of the QoS parameters. In order to decide if it is needed to integrate security with the QoS parameters. The simulation tests three different scenarios, in each scenario, the data transmission meant to be under attack of some un-behaved nodes where they try to perform certain level of attacks. The behavior of the network in terms of: end to end delay, throughput, packet delivery ratio and the nodes average energy consumption are tested.

GloMoSim: Global Mobile Information System Simulator (GloMoSim) is a heterogeneous network simulator that can easily simulate large networks with different connection capability (Zeng *et al*., 1998). GloMoSim lays on Parsec compiler which gives GloMoSim the advantage of using parallel discrete-event simulation that allows running the test on different CPU's at the same time (Meyer and Bagrodia, 1998). GloMoSim was chosen for the following reason:

- GloMoSim is a freeware simulation tool where researchers can download it online from http://pcl.cs.ucla.edu
- GloMoSim simulate the heterogeneous networks. Ad hoc, wireless and wired connectivity can be easily combined together in one network
- The AODV protocol is already implemented on the GloMoSim network layer hence only modifications are needed to this protocol
- GloMoSim have a built in statistics for each layer

Simulation environment: To reflect the more real alike ad hoc network appearance two connectivity scenarios are implemented. In the mobile nodes part the random topology is used. The nodes are randomly distributed on the simulation area. Other topologies like the bus topology where the nodes are in a liner way and the grid topology (Ruffino *et al*., 2006) where the nodes are placed in like a matrix can be considered as a special case of the random topology where the nature of mobile ad hoc goes more to be randomly distributed. The simulation test is placed on a 1500×1500 m area, the nodes move in random directions with 0-2 m sec^{-1} speed. The simulation time was sited to 10 min and each scenario was repeated 15 times. All the simulation parameters are configured in the Config (Fig. 3).

The simulation test based on three main scenarios with two sub scenarios for each. Where, the main scenarios are three different levels of security threats and the sub-scenarios are:

```
SIMULATION-TIME      10M
SEED                 2
TERRAIN-DIMENSIONS   (1500, 1500)
NUMBER-OF-NODES      50
NODE-PLACEMENT       RANDOM
MOBILITY RANDOM-WAYPOINT
MOBILITY-WP-PAUSE        20S
MOBILITY-WP-MIN-SPEED    0
MOBILITY-WP-MAX-SPEED    2
MOBILITY-POSITION-GRANULARITY 0.5
PROPAGATION-LIMIT       -111.0
PROPAGATION-PATHLOSS    TWO-RAY
NOISE-FIGURE     10.0
TEMPARATURE      290.0
RADIO-TYPE                RADIO-ACCNOISE
RADIO-FREQUENCY      2.4e9
RADIO-BANDWIDTH      2000000
RADIO-RX-TYPE             SNR-BOUNDED
RADIO-RX-SNR-THRESHOLD   10.0
RADIO-TX-POWER         15.0
RADIO-ANTENNA-GAIN   0.0
RADIO-RX-SENSITIVITY -91.0
RADIO-RX-THRESHOLD -81.0
################################
MAC-PROTOCOL         802.11
NETWORK-PROTOCOL     IP
NETWORK-OUTPUT-QUEUE-SIZE-PER-PRIORITY 100
################################
ROUTING-PROTOCOL     AODV
APP-CONFIG-FILE    ./app.conf
APPLICATION-STATISTICS          YES
TCP-STATISTICS                  YES
UDP-STATISTICS                  YES
ROUTING-STATISTICS              NO
NETWORK-LAYER-STATISTICS        NO
MAC-LAYER-STATISTICS            NO
RADIO-LAYER-STATISTICS          YES
CHANNEL-LAYER-STATISTICS        NO
MOBILITY-STATISTICS             NO
```

Fig. 3: Configuration file

- WAP ad hoc multi hop connection: the packets are traveling through the WAP to a mobile node that is out of the WAP range
- Pure ad hoc connection

SIMULATION METRICS

In this study, four simulation metrics are used for the performance measurement sake. Namely: delay, throughput, packet delivery ratio and energy consumption. Since, those metrics are more likely to be affected by security attacks.

End to end delay: Delay is an accumulative measurement of many delay sources. Process delay is the delay of packet processing before forwarding it to the next hop. DoS attacks can significantly increase the processing delay. Propagation delay is the time it takes the packet in the transmission media (i.e., the time needed for carrying the packet from the physical layer of the source node to the physical layer on the destination node). Therefore, the end to end delay is chosen to represent the entire delay in all stages.

Throughput: Throughput can be defined as the size of the packets flow in other words it's the average number of the transmitted packets. This metric is chosen since a lot of security attacks target the bandwidth like the jamming and poisoning threats which leads to throughput reduction.

Packet Delivery Ratio (PDR): Packet Delivery Ratio (PDR) is the percentage of the received packets by a cretin node out of the packet that already have been sent to it. PDR can reflect the network healthiness from the packet hijacking and black-hole attacks. The higher PDR the healthier is the connection.

Energy consumption: In ad hoc networks energy consumption is a very important issue that is due to the limited resources. DoS attacks and the power eating threats are some reasons of the dramatically nodes power consumption.

SCENARIOS IMPLEMENTATION

This research aims to study the effect of the security attacks on the QoS metrics, to derive the importance of integrating security along with other QoS parameters by studying the effect of several security attacks scenarios on those metrics. To do so researchers considered the Table 1 each threat gains one point for each check. As shown in Fig. 4 each security level (except level 0) generate one main scenario, these threat levels are determined based on the number of QoS metrics that they can affect.

Although, some threats are severe like the wormhole attack but in the Fig. 4 it is leveled as security threat of level 1. The reason behind this contradictory is that the leveling in this figure comes from the QoS parameters point of view and which threat affect them more, for example the Denial of Service attack is ranked as level 3 because its affect the bandwidth, throughput and delay at the same time. Where the wormhole attack is ranked as level 1 since it affects mainly the throughput. For the simulation purposes threats of level zero are neglected, level 1-3 are considered as three scenarios.

In each of which an attacker nodes are fortified with one or more attacks. Each scenario is tested onto a WAP ad hoc connection and again on a pure ad hoc connection. In the simulation test 12 nodes which are 25% of the mobile nodes number are used to launch attacks on the other nodes. In GloMoSim creating each node as a individually is very time consuming process and it significantly consume the memory too which make the simulation very slow, therefore one entity type is used to create all the simulation nodes. To differentiate the attacker nodes from other nodes researchers added a new variable: is attacker of type Boolean to the modified node structure is given:

```
Struct glomo_node_str {
   /* Common information about each node.*/
  /* This field represents the simulation id of the node.
     It is used only for simulation purposes and should not be used by the
protocol code at any layer. For the network address of the node use the next
field which is called nodeAddr.*/
  Unsigned      id;
  Node_ADDR   nodeAddr;  /* the network address of the node*/
  Unsigned short seed[3]; /* seed for random number generator*/
  Unsigned short initial seedValue[3]; /*First seed value for a node*/
 long  numNodes; /* number of nodes in the simulation*/
bool is attacker /*Added by me: to deffrenciate the
                 /* attacker nodes from other nodes.*/
                /* True means the node is attacker node*/
```

The creation of the nodes is done in the nodes.pc file where isattacker is set to TRUE for the first 12 nodes and FALSE to the rest of the nodes Fig. 4. The positioning of the simulation nodes is chosen to be random hence the modification is done only for the random node generator function. Creating random nodes with attackers is given below:

```
int DriverGenrateRandomNodes (GlomoNodePositionInfo*nodeData, int
nodeNum.
                                Glomo coordinates terrainDimensions,
                          unsigned short seed [3],
                          bool isattacker)
{
    int i;
    for (i = 0; i< nodeNum; i++)  {
       nodeData [i]. node addr = i;
       nodeData [i]. position.x = pc_erand(seed)*terrainDimensions.x;
       nodeData [i]. position.y = pc_erand(seed)*terrainDimensions.y;
     if (i<(nodeNum/4)-1)
       {nodeData[i]. isattacker = TRUE}
      else
        {nodeData[i]. isattacker = FALSE}
       }
      return i;
     }
```

Scenario 1: In this scenario, attacks of level one are implemented.

Black-hole: Researchers assumed that the attacker node is already engaged in the data forwarding. Researchers modified the data transmission function in the AODV file so that the attacker node will just ignore forwarding the packets to the next hop.

Wormhole: Two cooperative nodes are needed to implement this attack, one at each end, the first one should be enrolled in the packet route at the time it will receive the packet it will forward it to the node in the second end of the wormhole (the cooperative node) instead of sending it to the next hop in the route. Therefore, in the implementation the node equipped with the wormhole attack will send the entire received packet to its partner node regardless of what the next node in the route is.

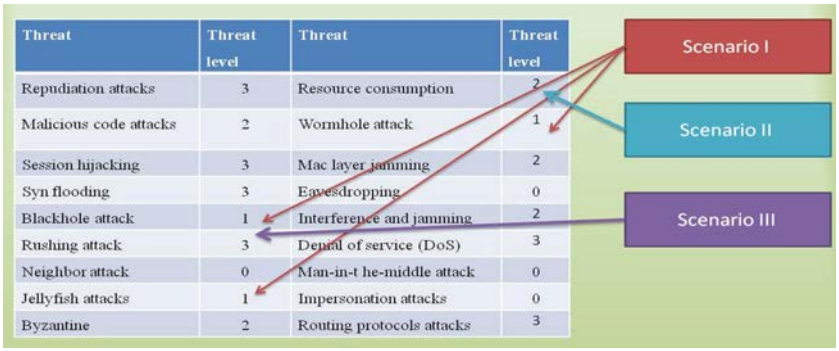

Fig. 4: Threat levels and the main three scenarios

Jellyfish: The nodes equipped with the jellyfish threat will hold the received packets for a while before resend them again to the next node. The holding time is implemented to be between 1-15 sec. Random function is used to assign the delay value in each test run.

Scenario 2: In this scenario, some attacks of level two are implemented. Byzantine and resource consumption attacks will represent this level in the simulation.

Scenario 3: In the last scenario, one attack of level three is implemented. Rushing attack will represent this level in the simulation. Since, the rushing attack is one of the most known denial of service attacks.

Like the resource consumption attack, the attacker node keep sending data packet over and over again in a fast rhythm but in the rushing attack the data packet is the same every time, so the victim node think that this is a duplicate packets and decide to ignore all the upcoming packets. At that time the victim node is forced to be in denial of service situation.

Byzantine: One way of implementing this kind of attacks is that the attacker node start to form a routing loop, therefore the attacker node is designed to resend the received packet back again to the sender. This was implemented by sitting The next Hop Address = Previous Hop Address in the packet header.

Resource consumption: Attacker node coded to send a data packet to the victim node every 5 sec, this action will consume the victim node resources (CPU and battery) but in this test, the concern is the power consumption or the battery draining.

RESULTS

This study evaluates the need of integrating security with the other QoS constraints and highlights the effect of security attacks on user's QoS requests. A simulation study using the GloMoSim simulator is performed for the HetMan architecture mainly in two scenarios of the heterogeneous ad hoc network combined with wireless access point, the second one is standalone MANET. Most commonly available threats on MANETs are grouped depending on their effect on the network metrics: delay, throughput and energy consumption. Each group represent different level of security threats where the threats that affect only one constraint goes to level one, those that affect two constraints goes to level 2 and level 3 contains threats that affect the three constraints. Each level considered as a different scenario and implemented with the two HetMan scenarios as a sub scenarios.

The results show that in an attack free network the pure MANET (i.e., scenario B) shows worse delay than scenario A where the average delay is about 0.28 sec in B and 0.21 sec in A. This means that the stand alone MANET have 35% more end to end delay time more than the heterogeneous MANET. Regarding throughput pure MANET also performed less than it's contradictory by 15%. For the packet delivery ratio pure MANET performed better than the WAP-MANET by 3%. Finally, pure MANET shows less energy consumption average where the WAP-MANET shows an increment in the power consumed by 25%, researchers refer the high energy consumption in scenario A to the dual mode where using two antennas consume more energy than using a single one. On the other hand running those scenarios under attack proved that packet delivery ratio and energy consumption are much vulnerable in the stand alone MANETs than the WAP-MANET. Delay was extremely affected by all the attacks levels and in both architecture scenarios. Where, throughput was affected with the same degree in most of the cases but the threat level did not have that large influence on the decrement of the throughput (i.e., the average of decrement for the two sub scenarios A and B was 38, 39, 45% under attack level 1-3, respectively).

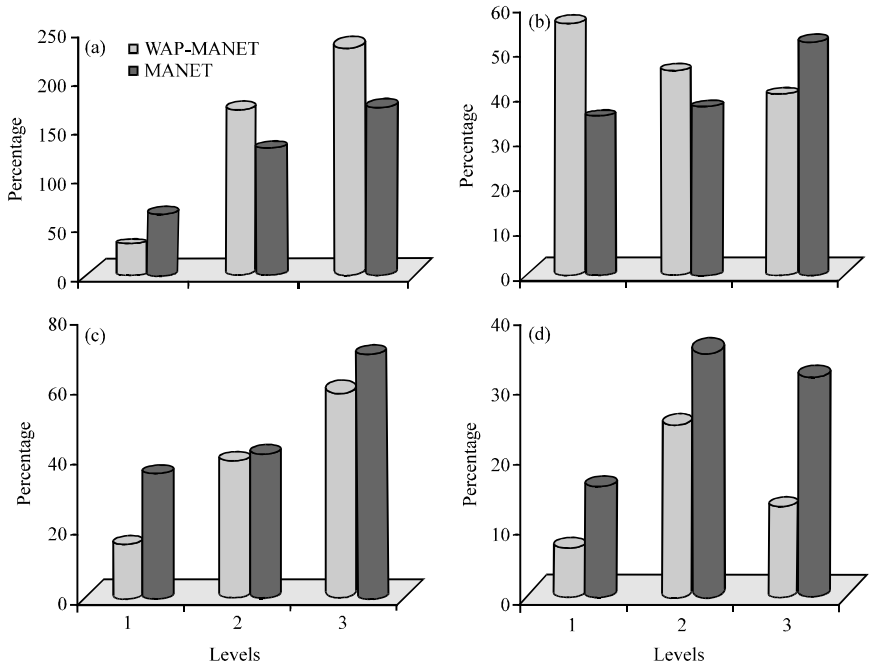

Fig. 5: Results; a) delay; b) decrement in throughput; c) packet delivery ratio and d) energy consumption

For the packet delivery ratio and delay the influence of the threat is covariant with the threat level since level two causes less PDR and more delay than those caused by level one. And in the same manner with level three and two. This was not the case about the energy consumption where level two had the highest average percentage of 25%, level one and level three have 8, 18%, respectively.

CONCLUSION

In this study, researchers conclude that threat attacks have a great influence on the QoS metrics, this situation leads to increase the user dissatisfaction. This study proves that it's not enough to find the route that it will achieve the QoS requested for. This route might be under attack of any level; these attacks most probably will affect the QoS constraints and make it unachievable. Hence, certain level of security should be integrated into the QoS routing to insure that the selected route is not only the best available route to achieve the required QoS but also have a level of assurance that no security attacks can affect this route and avert achieving its goals.

REFERENCES

Adibi, S. and G.B. Agnew, 2008. Security Measures for Mobile Ad-Hoc Network (MANETs). In: Handbook of Research on Wireless Security, Zhang, Y., J. Zheng and M. Ma (Eds.). IGI Global Inc., USA., ISBN-13: 9781599048994, pp: 500-514.

Anantvalee, T. and J. Wu, 2007. A Survey on Intrusion Detection in Mobile Ad Hoc Networks. In: Wireless Network Security, Xiao, Y., X. Shen and D.Z. Du (Eds.). Springer, New York, ISBN: 9780387331126, pp: 159-180.

Conti, M. and S. Giordano, 2007. Multihop ad hoc networking: The theory. IEEE Commun. Mag., 45: 78-86.

Duflos, S., V. Gay, B. Kervella and E. Horlait, 2005. Integration of security parameters in the service level specification to improve QoS management of secure distributed multimedia services. Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Volume 2, March 28-30, 2005, Taipei, Taiwan, pp: 145-148.

Hassan, R., R. Razali, S. Mohseni, O. Mohamad and Z. Ismail, 2010. Architecture of network management tools for heterogeneous system. Int. J. Comput. Sci. Inform. Secur., 3: 31-40.

Kar, S., P. Farjami and R. Chakravorty, 2000. Issues and architectures for better quality of service (QoS) from the Internet. Proceedings of the 6th National Conference on Pragmatics in China, June 26-28, 2000, Singapore, pp: 181-187.

Lu, B., 2008. Security in Mobile Ad Hoc Networks. In: Handbook of Research on Wireless Security, Zhang, Y., J. Zheng and M. Ma (Eds.). Information Science, USA., ISBN-13: 978-1599048994, pp: 413-430.

Meyer, R.A. and R. Bagrodia, 1998. PARSEC user manual. http://www.eecis.udel.edu/~cshen/861/notes/manual.pdf.

Mishra, A., 2008. Security and Quality of Service in Ad Hoc Wireless Networks. Cambridge University Press, UK., ISBN: 13-9781139470407.

Mohamad, O., R. Hassan, A. Patel and R. Razati, 2009. A review of security parameters in mobile ad hoc networks. Proceedings of the International Conference on Information and Communications Systems, December 20-22, 2009, Amman, Jordan.

Mohseni, S., R. Hassan, A. Patel and R. Razali, 2010. Comparative review study of reactive and proactive routing protocols in MANETs. Proceedings of the 4th IEEE International Conference on Digital Ecosystems and Technologies, April 13-16, 2010, Dubai, pp: 304-309.

Nichols, R.K. and P.C. Lekkas, 2002. Wireless Security: Models, Threats and Solutions. McGraw-Hill, New York, ISBN-13: 9780071380386, Pages: 657.

Ong, C.S., 2003. Quality of protection for multimedia applications in ubiquitous environment. Master's Thesis, Department of Computer Science, University of Illinois, Urbana.

Reddy, T.B., I. Karthigeyan, B.S. Manoj and C.S.R. Murthy, 2006. Quality of service provisioning in ad hoc wireless networks: A survey of issues and solutions. J. Ad Hoc Networks, 4: 83-124.

Ruffino, S., P. Stupar, T. Clausen and S. Singh, 2006. Connectivity scenarios for MANET. AUTOCONF Internet-Draft, July 5, 2006. http://tools.ietf.org/html/draft-ruffino-autoconf-conn-scenarios-00.

Sakarindr, P., N. Ansari, R. Rojas-Cessa and S. Papavassiliou, 2005. Security-enhanced quality of service (SQoS) design and architecture. Proceedings of the IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, April 18-19, 2005, Princeton, NJ., pp: 129-132.

Sarma, N., A. Singh and S. Nandi, 2008. A Strict Priority Based QoS-Aware MAC Protocol for Mobile Ad Hoc Networks. In: Distributed Computing and Internet Technology, Parashar, M., S.K. Aggarwal (Eds.). Springer, New York, NY., USA., ISBN: 9783540897361, pp: 121-132.

Witt, M. and V. Turau, 2005. BGR: Blind geographic routing for sensor networks. Proceedings of the 3rd International Workshop on Intelligent Solutions in Embedded Systems, May 20, 2005, Hamburg, Germany, pp: 51-61.

Xiao, Y., X. Shen and D.Z. Du, 2007. Wireless Network Security. Springer, New York, ISBN: 9780387331126, Pages: 432.

Zeng, X., R. Bagrodia and M. Gerla, 1998. GloMoSim: A library for parallel simulation of large-scale wireless networks. Proceedings of the 12th Workshop on Parallel and Distributed Simulation, May 26-29, 1998, Banff, Alta, Canada, USA., pp: 154-161.