Secure Routing for Supporting Ad-hoc Extreme Emergency Infrastructures

Emmanouil A. PANAOUSIS, Tipu Arvind RAMREKHA and Christos POLITIS
Wireless Multimedia and Networking Research Group
Kingston University London
KT1 2EE, United Kingdom
Tel: ++44(0)20 8417 7025, Fax: +44 (0)20 8417 2972
Email: {e.panaousis, a.ramrekha, c.politis}@kingston.ac.uk

***Abstract*—The importance of emergency services has lead to an indispensable need for lightweight technologies that will support emergency rescue missions. Due to their nature and the non-infrastructure characteristics Mobile Ad-hoc Networks (MANETs) are characterised as autonomous networks that have the potential to be exploited when wireless communications should be established in an ad-hoc manner in cases that traditional telecommunications infrastructures such as 3G have failed. A critical issue within the context of MANETs is the routing protocol that has to be followed by the nodes in order to set up communication "bridges" among each other. On the other hand, malicious entities may try to disrupt the conventional functionality of any routing protocol by (i) modifying routing information, (ii) fabricating false routing information and (iii) impersonating other nodes. In this paper we apply the IPSec protocol over well known routing protocols for MANETs and we evaluate their performance along with the lines of choosing an appropriate secure routing mechanism that can be applicable in emergency MANETs (eMANETs). These are MANETs that are established during an emergency scenario to provide communication links among the rescuers. To simulate the mobility of the rescuers during an emergency mission an appropriate mobility model has been utilised and acknowledged.**

***Index Terms*—MANETs, Routing, OLSR, AODV, DYMO, Security, IPSec, emergency**

1. Introduction

Mobile Ad-hoc Networks (MANETs) are wireless networks that do not include any centralised infrastructure. Each node of a MANET plays the role of a forwarder (or intermediate node) for packets originated by a source node and are propagating towards a destination node (Figure 1). The nature of the wireless medium and the fact that there is no centralised coordination point in MANETs have the potential to encourage malicious entities to launch different kind of attacks against the routing protocols. The latter are consistently constructed without any afore security mechanism. Consequently, any malicious node can exploit vulnerabilities and dramatically damage the proper routing functionality.

In this paper, we integrate the IPSec protocol [1], [2] into the well known MANET routing protocols OLSR (Optimised Link State Routing) [3], AODV (Ad-hoc On-demand Distance Vector) [4] and DYMO (Dynamic MANET On-demand Routing Protocol) [5]. To this end, we choose the appropriate IPSec mode and security schemes to provide *confidentiality*, *authentication* and *integrity* for the communication links. Our work has been done within the context of FP7 ICT-SEC PEACE[1] project which investigates the provisioning of day-to-day emergency communications in next generation all-IP networks. One scenario we examine is how to supply the policemen and firemen with an enhanced PDA or personal digital assistant. Within the context of the project, we aim at establishing VoIP communications among the aforementioned emergency rescuers. In this case, along with a QoS solution for the emerging communication, security mechanisms have to be developed to guarantee confidentiality, integrity and authentication. In any other circumstances where security mechanisms have not been applied in advance, adversaries have the potential to damage and totally disrupt the entire eMANET VoIP communication links.

2. Secure Routing

In this work we have applied the IPSec protocol to the most effective and well known routing protocols for MANETs namely the OLSR, AODV and DYMO. We have not examined the case of the DSR protocol for the following reasons. In the first instance, we have proven that among the reactive AODV and DSR protocols, the former is more effective for emergency scenarios in terms of packet end-to-end delay, packet jitter and total control load. Furthermore, in DSR each forwarding node modifies the RREQ messages by adding its own address. In this case end-to-end authentication can not be achieved by using IPSec. It is worth noting that DYMO [5] is a reactive multihop unicast routing protocol proposed similar to AODV. The main improvement that DYMO introduces compared to AODV, resides in the route maintenance operation. In the event that a data packet is received and cannot be forwarded due to broken or unknown routes, a Route Error (RERR) message is sent to the data packet originator to notify about the failure. The source node then deletes the route from its routing table and when an intermediate node receives a data packet for the same destination, it has to re-initiate route discovery.

The reasons that we have decided to secure the MANET routing protocols by using the IPSec protocol are summarised in the following. In fact, IPSec is one of the best security protocols and the most reliable and efficient secure network

[1] For more info visit: http://www.ict-peace.eu/.

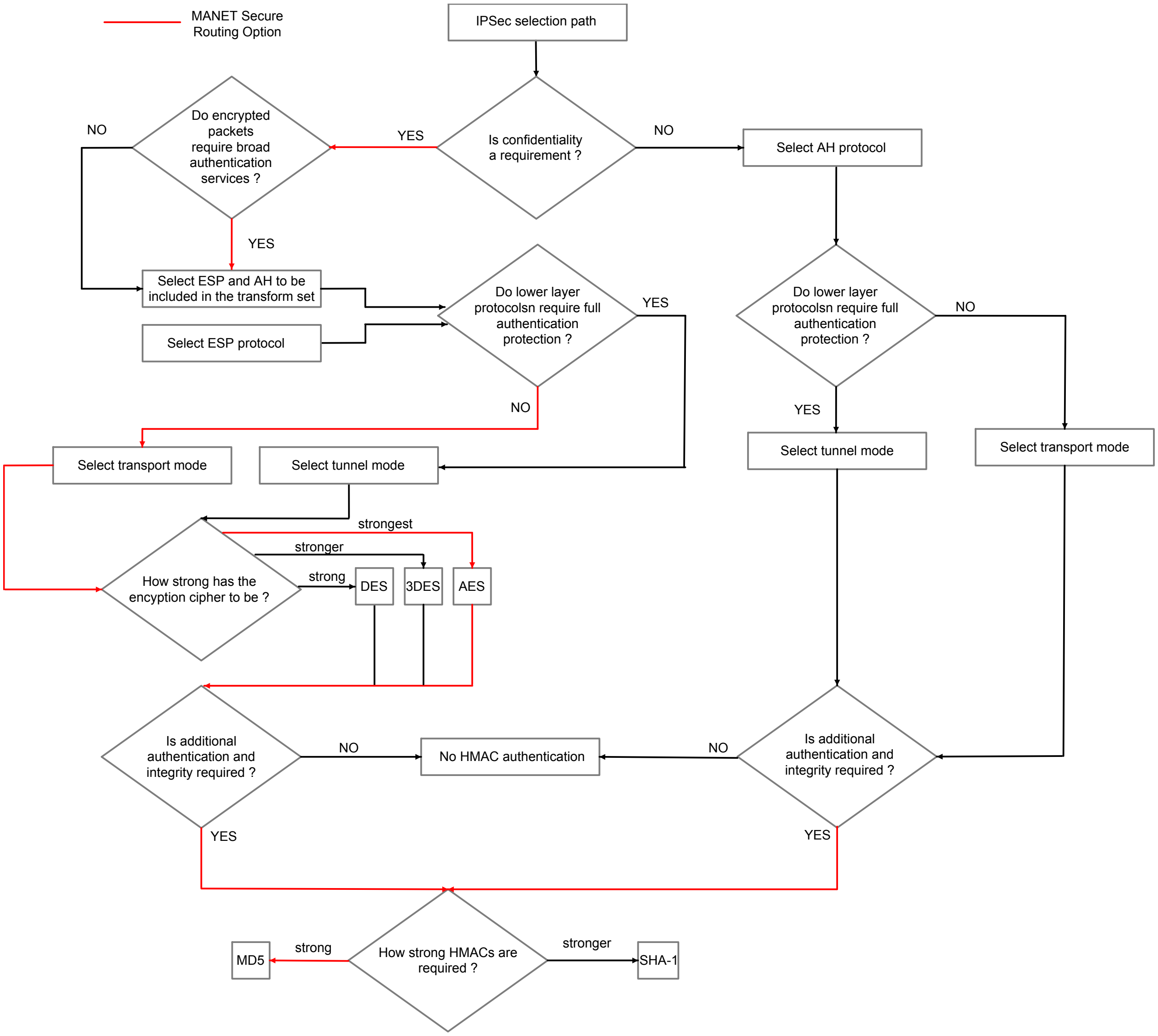
MANET Secure Routing Option
IPSec selection path
Is confidentiality a requirement ?
YES
NO
Select AH protocol
Do encrypted packets require broad authentication services ?
NO
YES
Select ESP and AH to be included in the transform set
Select ESP protocol
Do lower layer protocolsn require full authentication protection ?
YES
NO
Do lower layer protocolsn require full authentication protection ?
NO
YES
Select transport mode
Select tunnel mode
Select tunnel mode
Select transport mode
How strong has the encryption cipher to be ?
strongest
stronger
strong
DES
3DES
AES
Is additional authentication and integrity required ?
NO
No HMAC authentication
NO
Is additional authentication and integrity required ?
YES
YES
How strong HMACs are required ?
strong
MD5
stronger
SHA-1

Fig. 1: The different IPSec selection paths and our choice for securing the routing protocols.

layer protocol. The encryption provided by the IPSec defends the wireless communications from being hacked and confidential information to be revealed. Furthermore, if an adversary decided to hide its IP by pretending to be a legitimate node (IP spoofing), it will not succeed to authenticate itself in a wireless network that IPSec has been utilised due to the fact that the protocol provides a strong authentication scheme. In accordance with the concept of the integrity protection, in case the Integrity Check Value (ICV) of a packet is valid, it receives the appropriate treatment and the nodes decide the next hop node across the path to the destination. If any unauthenticated node changes any data in the IP datagram or updates the ICV, this node will be detected and the packet will be discarded.

For the purposes of the secure routing we have used the AH (Authentication Header) and ESP (Encapsulating Security Payload) protocols towards the establishment of eMANET communications that will guarantee integrity, authentication and confidentiality. The same hybrid approach has been followed by the authors in [2] where they present a possible solution for the protection of QoS signalling in military MANETs using AH and ESP. According to [2], we have chosen to use only the transport mode of the IPSec protocol in order to avoid high processing power overhead. Authentication and integrity are satisfied by the AH protocol that utilises the MD5 (Message Digest 5) hash algorithm along with a symmetric AES (Advanced Encryption Standard) key to produce an HMAC (Hash Message Authentication Code) called HMAC-MD5. We choose MD5 instead of SHA-1 (Secure Hash Algorithm-1) due to the power limitations of our devices (e.g. iPhones, PDAs) in addition to the fact that MD5 is strong enough to support our scenarios. For the ESP protocol we have used 128-bit symmetric keys because AES is the fastest and cryptographically strongest symmetric cryptographic algorithm. The aforementioned choices are illustrated in Figure 1 along with the different security options that IPSec has the potential to utilise and the hybrid mode we have chosen for the purposes of eMANETs.

3. Performance Evaluation

In this section we discuss the simulation results. Our goal is to evaluate the performance of each of the aforementioned MANET routing protocols during an emergency scenario assuming 20 nodes. It is worth mentioning here that MANET nodes of our simulation scenarios, use IEEE-802.11 wireless interfaces. To this end, we have used an obstacle-aware human mobility model (HUMO) [6] for eMANETs. Typical examples where the nodes of MANETs are human-operated are natural or man-made disasters, military activities or healthcare services. In these scenarios, obstacles are an integral part of the areas where such networks are deployed in order to facilitate communication among the firemen, policemen, paramedics, soldiers, etc. In the proposed mobility model, the nodes of the network move around the obstacles in a natural and realistic way. The obstacles are also taken into account in modelling the signal propagation.

The performance results of routing protocols under the extreme emergency scenario are illustrated in Figures 2, 3, 4 and 5. The average pause time of the nodes in the network is varied to investigate the effect of varying mobility on routing performance in such environments. We have firstly illustrated in Figure 2 the throughput which equals to the ratio of received by sent data packets and it is a critical Quality-of-Service metric given as: $throughput = \frac{\textit{average received data packets}}{\textit{average sent data packets}}$ against different pause time values or else different mobility levels for the different MANET routing protocols. We clearly notice that for higher node mobility scenarios or else lower average pause time that the throughput is higher for all the protocols. This is explained in [7] where authors prove that increased node mobility in MANETs increases the throughput of data transmission due to reduction of mutual transmission interference and exploitation of multiuser diversity through packet forwarding. For networks with pause time of less than 20 seconds[2], OLSR has higher throughput than AODV because it regularly updates its routes and detects regular route changes. Consequently, OLSR minimises data packet loss. However, in networks where the pause time is equal to or greater than 20 seconds, the route changes are less frequent. Instead, the regular route updates of OLSR induces more message overhead in the network and results in more transmission interference and lower throughput. DYMO throughput slightly outperforms the rest over the investigated mobility range. DYMO protocols uses a RERR packet to alert all the nodes in a route as soon as a route breakage is detected. The route is re-established so that packet loss is reduced compared to AODV. Also, its reactive nature implies that DYMO is more efficient than OLSR in high pause time networks where the route changes are less frequent and a reactive approach better suited.

In Figure 3, it can be observed that the total routing load of the routing protocol decreases when mobility decreases. In high mobility networks, the frequent route changes result in DYMO and AODV sending more reactive route discovery routing messages to obtain routes to destinations. DYMO uses additional RERR messages to explicitly alert participating nodes in a route about an unreachable route and therefore it uses more routing load than AODV. In low mobility scenarios where the route changes are less frequent, the difference between DYMO and AODV routing loads is reduced. However, OLSR uses a proactive approach and thus it utilises periodic routing messages without considering the rate of route changes. This is the reason for its high routing load compared to 'on-demand' routing approaches used by DYMO and AODV. However, the most important factor that indicates the high routing load of OLSR is the topology control (TC) messages as described in [3]. Finally, we can explain the decreasing routing load of OLSR as pause time increases considering that more stable links are available in low mobility networks allowing OLSR to make a better choice of MPR nodes. Thus, the flooding of TC messages in the network is reduced.

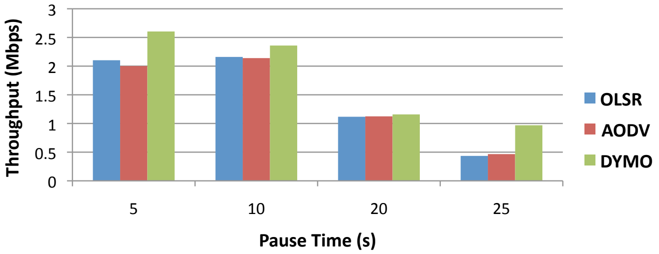

Fig. 2: The throughput for the different routing protocols.

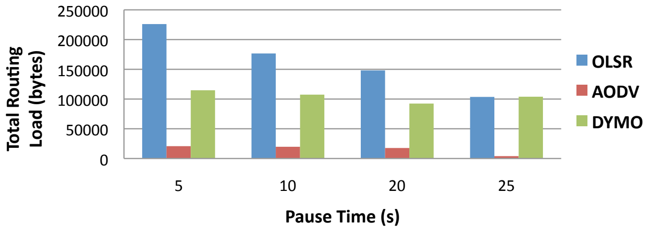

Fig. 3: The total routing load for the different routing protocols.

The average end-to-end packet delay results are shown in Figure 4. It can be deduced from the figure that the average packet delivery delay in the network decreases when the node pause time increases for all the routing protocols investigated. The average end-to-end delay value for packet delivery corresponds to the time required for finding a route to a destination plus the time required for a transmission to take place along such a route and is given by: *end-to-end delay = route discovery delay + transmission delay*. The route discovery delay is directly affected by mobility because any originator has to find valid routes in a corresponding frequency. On the other hand, the transmission delay depends on the routing load[3] because this affects the CSMA/CA link layer access protocols as we discuss in the following. In high mobility MANETs where route changes frequently, both AODV and DYMO have to rediscover valid routes to destination nodes thus increasing the average end-to-end delay as it is defined above. Additionally, DYMO introduces higher packet delivery

[2] when mobility is high.

[3] for a given data load. We send the same amount of data for the different scenarios.

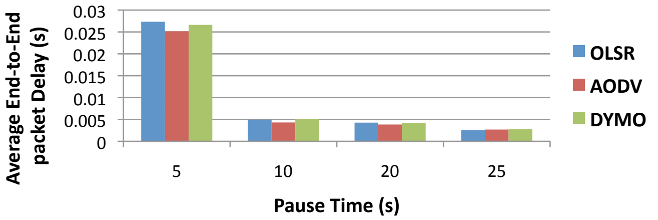

Fig. 4: The average end-to-end data packet delay for the different routing protocols.

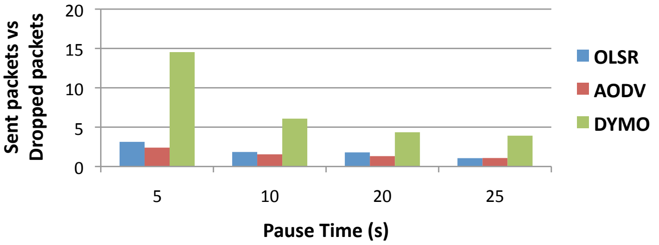

Fig. 5: The ratio of sent data packets vs dropped data packets for the different routing protocols.

delay than AODV as it has higher transmission delay. Figure 3 confirms this intuition by showing that DYMO introduces more routing load than AODV, due to RERR messages, in all pause time scenarios. It is also known that the CSMA/CA access protocol used in IEEE 802.11-enabled networks specifies that only one node among nodes sharing the same transmission space is allowed to transmit at a time. Therefore there is a higher average wait time in the case of DYMO where higher traffic is generated by RERRs reporting broken routes. Within the same context and due to the highest routing load of OLSR its transmission delay is the highest too.

Figure 5 depicts the ratio of the number of total packets[4] sent by each protocol against the total number of those packets that are dropped. This ratio corresponds to the reliability of the protocols in terms of how much actual and control information is received. The event of a packet drop occurs if established routes are broken during a transmission or if no routes can be established towards the intended recipient. DYMO has the highest number of packets sent to drop ratio implying that it is more reliable than OLSR and AODV. It uses the route error notification mechanism to quickly notify nodes of any route breakages so that new routes can be discovered and packet losses reduced. OLSR performs better than AODV because it regularly updates its route to discover these route breakages. Thus, it can use fresher routes to send packets as compared to AODV which discovers route breakage after a pre-defined route timeout interval. Additionally, when the average node pause time increases, the difference in the ratio value among the protocols is reduced because there are less route breakages. In addition, the ratio decreases for all the protocols as the network mobility decreases. As mentioned above, this is a result of mutual interference among concurrent transmission nodes that occur in static or networks consisting of nodes with low mobility as explained in [7].

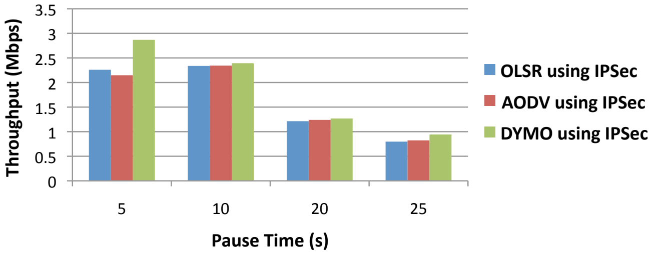

Fig. 6: The throughput for the different routing protocols using IPSec.

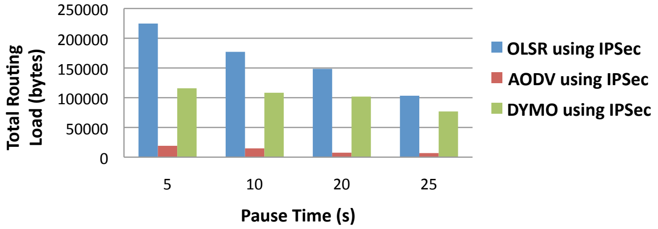

Fig. 7: The total routing load for the different routing protocols using IPSec.

The total number of operations required for MD5 processing per 512 bits block is 720 plus 24 operations for initialisation and termination. In order to compute the exact time of HMAC-MD5 operation for an input of packets n_k and for processor speed c_p the following equation is used: $t_{HMAC-MD5}(n_k,\ c_p) = [32+(2+744\cdot n_k)]/c_p$. To go a step further, the time overhead of AES is $T_{encryption} = 6,168$ and $T_{decryption} = 10,992$ processing cycles per packet assuming an 128-bit key length. Needless to say, IPSec packetisation and ciphering increase the size of the transmitted packets. In the transport mode, the space overhead of AH is equal to 24 whilst the size overhead of ESP is 10 bytes considering no authentication. Consequently, the total space overhead in the case of the utilised hybrid mode is (24+10) = 34 bytes. We have supposed that the emergency workers are equipped with PDAs with processing capability equal to 450 Millions of Instructions Per Second (MIPS) in order to compute the delay introduced in each device of HMAC-MD5 and AES encryption or decryption algorithms. From the two last equations, we have derived the time overhead per packet for each of HMAC-MD5 and AES algorithms. Namely, $t_{HMAC-MD5} = 1.68$ μsec/ packet, $t_{AES,encryption} = 13.7$ μsec/ packet, $t_{AES,decryption} = 24.4$ μsec/ packet.

To evaluate the performance of IPSec over the AODV, OLSR, DYMO we have illustrated the secure routing results in Figures 6, 7, 8, 9. As we were expecting, the trend for all the set of results is the same with the routing protocols performance evaluation graphs. We clearly see that the IPSec hybrid mode introduces time and space overhead as we have discussed in the previous section but it does not affect the main routing functionalities of the protocols. Whilst at the same time confidentiality, authentication and integrity are guaranteed. In Figure 6, throughput has been affected by the increased packet size introduced due to IPSec application. Although, the increased throughput results

[4] namely routing and data packets.

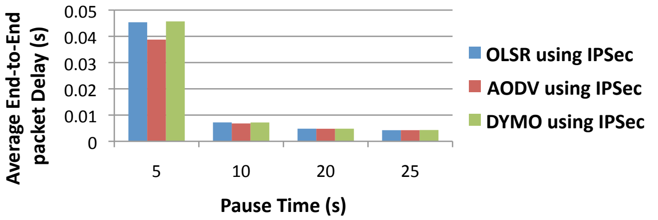

Fig. 8: The average end-to-end data packet delay for the different routing protocols using IPSec.

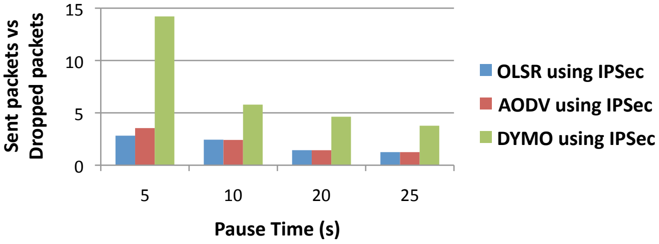

Fig. 9: The ratio of sent data packets vs dropped data packets for the different routing protocols using IPSec.

in higher energy consumption for the mobile devices which a inevitable characteristic introduced by any security solution. Routing load which is illustrated in terms of bytes (Figure 7) is also affected when security considerations are concerned due to space overhead of IPSec. Still the increment is negligible and that is what predicates the IPSec application efficient. In Figure 8, we observe that an increment of approximately 67% in the delay is noticeable. This happens due to the time overhead both ESP and AH protocols introduce to the communication links for each transmission. Although we have illustrated the ratio of total packets sent to total dropped packets against the different pause time values, we notice that there is no significant difference from the corresponding results taken without security considerations. This happens cause the IPSec does not prevent packet loss in any way and in this context intrusion detection mechanisms should be incorporated to the conventional secure routing protocols.

4. Summary and Future Work

In this paper, we have examined the case of secure routing within the context of emergency mobile ad-hoc networks. These are autonomous networks that can be deployed in emergency cases to establish communication among rescuers. To this end, we have taken advantage of the security strength of IPSec to provide confidentiality, authentication and integrity by using a hybrid mode appropriate for MANETs. In fact, we have used the transport mode of IPSec and we have applied the AES cryptographic algorithm along with the MD5 hashing function (AH and ESP security protocols). The afore choices have been based on the fact that lightweight devices require security implementations that are based on symmetric cryptographic algorithms such as the ones IPSec exploits. The performance evaluation shows that DYMO with or without using IPSec in overall is the best choice among all the examined MANET routing protocols due to the fact that RRER messages reduces the packet loss rate, increases the data throughput and packet delay jitter without introducing significantly higher routing load than the AODV and OLSR protocols.

Our plans for future work include but are not limited to guarantying security requirements, assuming that even if malicious nodes succeed to capture a node (node-capture attack), intrusion detection mechanisms such as the one proposed in [8] can be applied as a second wall of defence. In addition, we are planning to evaluate the performance of our innovative adaptive routing protocol for eMANETs proposed in [9] by using the proposed in this paper mode of IPSec. Finally, we intend to develop a testbed to evaluate the performance of different routing protocols along with the use of IPSec. In this way, we will be able to compare the results simulation results with the results taken in a real environment.

5. Acknowledgment

This work was undertaken in the context of the project ICT SEC-2007 PEACE (IP-based Emergency Applications and serviCes for nExt generation networks) with contract number 225654. The project has received research funding from the European 7^{th} Framework Programme.

References

[1] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol." *Internet Engineering Task Force*, no. 2401, Nov. 1998.

[2] A. Hegland and E. Winjum, "Securing qos signaling in ip-based military ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 42–48, November 2008.

[3] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)." *Internet Engineering Task Force*, no. 3626, Oct. 2003.

[4] C. e. a. Perkins, "Ad hoc on-demand distance vector (AODV) routing." *Internet Engineering Task Force*, no. 3561, Oct. 2003.

[5] I. Chakeres and C. Perkins, "Dynamic MANET on-demand (DYMO) routing." *Internet Engineering Task Force*, no. draft-ietf-manet-dymo-18.txt, Feb. 2010, work in progress.

[6] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "An obstacle-aware human mobility model for ad hoc networks," *Proc. 17^{th} IEEE/ACM MASCOTS Conference*, September 2009.

[7] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 4, pp. 477–486, 2002.

[8] E. A. Panaousis and C. Politis, "A game theoretic approach for securing aodv in emergency mobile ad hoc networks," *Proc. 34th IEEE Local Computer Networks Conference*, pp. 985–992, Zurich, Switzerland, October 2009.

[9] T. A. Ramrekha, E. A. Panaousis, G. P. Millar, and C. Politis, "ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations." *Internet Engineering Task Force*, no. draft-ramrekha-manet-cml-00.txt, Feb. 2010, work in progress.