Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications

Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis
Wireless Multimedia & Networking (WMN) Research Group
Kingston University London
KT1 2EE London, United Kingdom
{e.panaousis, l.nazaryan, c.politis}@kingston.ac.uk

ABSTRACT

The nature of Mobile Ad hoc NETworks (MANETs) makes them suitable to be utilized in the context of an extreme emergency for all rescue teams. We use the term emergency MANETs (eMANETs) in order to describe Next Generation Networks (NGNs) which are deployed in emergency cases such as forest fires and terrorist attacks. Secure routing in MANETs is critical. Due to the absence of a central authority, intermediate nodes act as routers forwarding packets across a multihop path. A well known attack against the conventional operation of routing protocols such as the Ad hoc On-demand Distance Vector (AODV) routing protocol, is the wormhole attack. Secure routing in eMANETs is critical due to the fact that secure multimedia communications should be established among the devices of the recovery workers.

In this paper we propose a novel routing mechanism called AODV-Wormhole Attack Detection Reaction AODV-WADR to defend eMANETs against wormhole attacks. Our simulations are carried out using the network simulator ns-2 and they show that AODV-WADR does not introduce high overhead, reducing significantly the amount of packet loss caused by malicious wormhole nodes. These are critical requirements for eMANETs where lightweight security mechanisms should be applied and malicious activities should be circumvented.

Keywords

Ad hoc networking, security, emergency, routing

1. INTRODUCTION

A MANET is a network of wireless mobile nodes such as PDAs, laptops and mobile phones which are self-organizing in dynamic network topologies. Their difference compared to the traditional mobile wireless networks is that they do not rely on any fixed infrastructure. In fact, mobile nodes rely on each other to keep the connectivity of the MANET. This characteristic makes them a useful and unique feasible solution for communication services in extreme emergency situations where the fast and effective deployment of a network infrastructure is impossible.

We use the term eMANETs in order to describe MANETs which are deployed in an extreme emergency case. Even if there are no other communication links as a consequence of disasters, wireless terminals such as PDAs and laptops could connect to each other and set up an eMANET to provide secure multimedia communications for extreme emergency services. In these cases, eMANETs consist of mobile nodes of workers such as firemen or policemen who collaborate to accomplish their mission. People and vehicles in extreme emergency cases can be internetworked in areas without preexisting communication infrastructure or when the use of such infrastructure requires wireless support. Security in MANETs is more challenging than in wired networks due to broadcast nature of the wireless medium and the frequent topology changes. Furthermore, due to numerous constraints such as lack of infrastructure, dynamic topology, and lack of pre-established trust relationships between nodes, most of the proposed routing protocols for MANETs are vulnerable to a number of disruptive threats which are presented extensively in [1].

In addition, in MANETs nodes cooperatively form the network by agreeing to certain routing messages according to well known routing protocols such as AODV [2] or OLSR [3]. It is worth mentioning that mobility makes the problem of detecting intruders harder. In this paper we examine the wormhole attack which takes place when two geographically separated adversaries create a tunnel called *wormhole tunnel*, as we show in figure 1. Consequently, aim of the attackers is to create a man-in-the-middle attack[1] or to destroy the proper operation of the AODV in an eMANET, by advertising shorter routes to a destination. The tunnel is created either using a wired link or by having a long range high bandwidth wireless link operating at a different frequency band.

Our proposed mechanism secures AODV against potential wormhole attacks. The mechanism is a part of the PEACE[2] Security Platform (PSP) proposed in [4]. We show that in the case where malicious nodes have launched a worm-

Mobimedia'09, September 7-9, 2009, London, UK.

[1] they can drop packets, listen to confidential information or change the transferred data packets.

[2] EU-FP7 PEACE project is a partly funded EU project. PEACE investigates the provisioning of day-to-day emergency communications in next generation all-IP networks. For more info visit: http://www.ict-peace.eu/.

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292

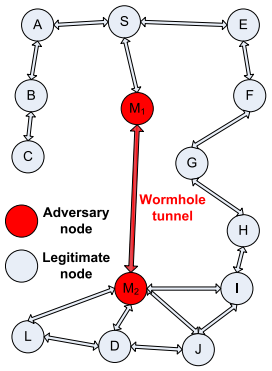

Figure 1: An example of wormhole attack in a MANET.

hole attack, AODV-WADR outperforms AODV[3] in terms of packet loss. The delay that AODV-WADR introduces is considered insignificant compared to its benefits. For further details about PSP, in [4] we define the architecture, the goals and the general concept of the platform to provide secure eMANET communications which have the potential to save many lives in emergency situations.

The remainder of this paper is organized as follows. In Section II we discuss related work while in section III we describe the AODV-WADR mechanism. Section IV deals with the simulation scenarios and results. We present our conclusions and plans for future work in section V.

2. RELATED WORK

According to [5], wormhole attacks can cause (i) tunneling of the packets at the application layer, (ii) tunneling of the packets through a long range wormhole tunnel using high power transmitters and (iii) tunneling the packets via external wired infrastructure. In our work, we examine the second case. Although there is no work done to secure eMANETs against wormhole attacks, we discuss work done that has been done for conventional MANETs.

In [6] authors take advance of the concept of directional antennas to prevent wormhole attacks while in [7] a novel protocol named TrueLink is proposed to defend MANETs against wormhole attacks. The protocol is virtually independent of the routing protocol used. In addition, disjoint path based approaches have been adopted such as the statistical approach in [8] which is based on multi path routing. DelPHI protocol [9] focuses on the delays due to different routes to a receiver. DelPHI is closer to our model because the delays and the number of hops of disjoint paths are used to conclude if a certain path is under wormhole attack. In [10] the authors use only connectivity information to check for forbidden substructures in the connectivity graph and as a result are able to detect the wormhole attack.

In [11] authors propose the concept of a *packet leash* as a general mechanism for detecting and preventing wormhole attacks. Furthermore, they categorize the leashes into *geographical* leashes and *temporal*. A geographical leash verifies that the receiver of a packet is within a certain distance from the sender whilst according to temporal leash the packet has an upper bound on its lifetime which bounds the maximum traverse distance. The latter mechanism is similar to our approach with the critical difference that all nodes must have tightly synchronized clocks using appropriate hardware. Another difference is that our mechanism advocates the sender of the message as the one that decides if a suspected wormhole attack has occurred, and not the receiver as the authors propose in [11]. Obviously, when the receiver is an adversary and consequently helps with the creation of the wormhole tunnel the temporal leash concept is not enough to defend against the malicious collaborative nodes.

[3]as we expected due to the fact that it is a secure routing protocol.

3. AODV-WADR

A representative feature of wormhole attacks consists of relatively longer packet latency than the normal wireless propagation latencies on a single hop. The load on a single route can also increase, leading to typically longer queuing delays. However, this is not a sufficient condition for the existence of a wormhole attack, because packet transmission is affected by various factors like congestion and traditional processing [8].

What happens actually in a wormhole attack is that adversaries destroy the appropriate operation of the MANET routing protocols due to the fact that they introduce new virtual shorter routes to a destination. Thus, the legitimate nodes of a MANET believe that they can reach a destination node in few hops, when this is actually many hops away from them. Thereafter, adversaries can record or drop packets as the first step of the man-in-the-middle attack.

AODV-WADR is integrated into AODV in order to apply low overhead defense against adversaries who establish a wormhole tunnel between different areas in a MANET. Our work considers the case of eMANETs in accordance with the concept of PEACE. We use a novel kind of mobility for the emergency workers called Mission Critical Mobility (MCM) as we will discuss extensively in the next section.

As we mentioned, AODV is a reactive routing protocol designed for MANETs. The algorithm which the protocol uses is an on-demand routing algorithm because it discovers and saves routes between nodes only when deemed necessary. Thus, when an adversary exists and succeeds to create a wormhole tunnel, wrong routing information is flooded though the MANET destroying the trust of the information in the routing tables.

Many attacks can be prevented using cryptography. This can help isolate all nodes that do not have the necessary credentials. Using cryptography is an attractive solution in many scenarios, as long as attackers are unable to compromise a node with the proper credentials. However, cryptography by itself is not an adequate tool to prevent a wormhole attack according to [7]. Links which experience long delays are treated as suspicious links and wormhole verification must be performed only on them.

AODV-WADR helps a node to confirm whether a neighbor has created a wormhole tunnel within the MANET or not, using a combination of *timing* and *cryptography*. After the detection of the wormhole attack by a source node S which tries to find a route to destination D, the former deletes the route which includes the malicious node and adds the adversary to a new blacklist. This list is called *blacklist_wadr* and it is different and independent of the blacklist defined in AODV [2]. A node has the potential to add to its blacklist only the next hop neighbor due to the fact that

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292

AODV-WADR uses information about the next hop node in a route to D. For a more convenient reading of this section, we summarize the following terminology[4]:

- NET_TRAVERSAL_TIME (NetTT): is the maximum expected time in milliseconds waiting for the receiving of a Route REPly (RREP) after the sending of a Route REQuest (RREQ) [2]
- NODE_TRAVERSAL_TIME (NodeTT): is the maximum expected wireless propagation latency on a single hop [2]
- ACTUAL_TRAVERSAL_TIME (ATT): is the actual period of time from the sending of a RREQ until the receiving of a RREP
- ACTUAL_TRAVERSAL_TIME_WADR (ATT_WADR): is the time between the sending of a *msg_wadr*[5] and the receiving of the changed *msg_wadr*
- MAXIMUM_TRAVERSAL_TIME (MTT): is equal to 6· NodeTT. This result arises from the multiplication of the number of hops between S and D (see figure 1) which is equal to 3 for a three hops away route[6], times 2 because NodeTT is the time for one hop traversal
- Hop count: is the hop count which is included in the AODV message and indicates the number of hops between a source (node which asks for a route) to a destination.

In the following we describe the methodology of AODV-WADR. We suppose that a node S wants to discover a route to a destination node D. According to AODV, S broadcasts a RREQ if it does not have a specific entry route for D or else it sends a RREQ to the next hop along the last updated route it has in its routing table for D. In AODV-WADR, S simultaneously starts a timer in order to be able to calculate the ATT from the time it sends the RREQ until the receiving of the RREP message. When S does not receive any RREP during the next NetTT milliseconds, it acts according to AODV[7]. On the other hand, if S receives the RREP, it checks the hop count. If the hop count is not equal to 3, the node ignores the AODV-WADR implementation and it continues its routing operation according to AODV.

If the hop count is equal to 3, S implements AODV-WADR. Hence, one critical criterion in our design is that AODV-WADR enables the detection and prevention of wormhole attacks only by nodes which are three hops away from the destination node. This assumption is realistic and effective for two reasons. First, if S detects and prevents the wormhole attack it is adequate for all the other nodes which have a route to D through S to have secure communication by avoiding the wormhole tunnel. Second, we know that every node keeps information about only the next hop[8] node, it therefore would have been more difficult for a node that is more than three hops away from the destination to consider which node in the route between itself and the destination has launched a wormhole attack. For instance, if a node suspects a wormhole attack and it is more than three hops away from the destination node, then it has to suspect more than two nodes between itself and the destination. Obviously, it can not consider two of them as adversaries randomly because consequently it could suspect an innocent node as malicious as malicious.

One could claim that the extent of applicability seems to be limited due to the fact that only scenarios with 3-hop connections between source and destination can be addressed. However, we point out that all the scenarios could be addressed considering only scenarios of 3-hop connections. To put it simply, due to the nature of AODV which acts in a hop-by-hop manner, a potential node could detect a wormhole attack within a 3-hop distance. This detection is enough to protect the whole MANET from the detected wormhole nodes for the following reason; whenever the legitimate nodes detect and ensure that a node is participating in the launch of a wormhole attack, they terminate any communication with it. In this case, due to the nature of AODV none of the nodes will forward their packets to the destination through the malicious nodes.

To continue with the description of AODV-WADR's function, when ATT is higher than MTT, S suspects a wormhole attack due to the fact the message was transmitted slower. What happens is that adversaries use enhanced hardware to transmit the packets further away than one hop distance but the time of transmission can not be smaller than the time of a IEEE 802.11b transmission towards a single hop. However, the above phenomenon can be caused due to wireless propagation effects or delays in the CSMA/ CA algorithm. That is why AODV-WADR has to check if this behavior is due to the existence of a wormhole attack or not.

Therefore, after the suspicion, S establishes a cryptographic algorithm between itself and D in order to create a shared secret key. Both S and D nodes have to run a Diffie-Hellman (DH) key exchange algorithm. For this purpose, S informs D that they have to implement the DH mechanism. If S does not receive a response from D during the next NetTT milliseconds, it deletes the route to D from its routing table. Furthermore, S adds the next hop node to a blacklist. This blacklist is used by S in order to keep itself informed about the nodes that it should not trust again excluding them from its routing tables.

The DH exchange key mechanism called also DH protocol, it is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Specifically, the protocol uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.

DH is one of the well known asymmetric cryptographic algorithms. Usually, the latter are used in MANETs to transport symmetric keys between the nodes that want to exchange data securely. In most of the cases of key transport, one of the nodes decides the key. This node encrypts the key using the public key of the other node and sends the message. Obviously, in these cases the key is decided by only one of the participating nodes. However by using the DH exchange mechanism both nodes participate in the

[4]some terms are from [2].
[5]this is the name of the AODV-WADR message.
[6]we explain in the following why we consider only three hops routes in AODV-WADR.
[7]see [2].
[8]according to [2].

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292

decision of the secret key, making the decision mechanism more fair for both parties.

Additionally, in extreme emergency situations it is not realistic to assume the existence of *certification authorities*. All the nodes are bilateral and they cooperate in a distributed manner to implement all of the appropriate security services for MANETs.

Each node that detects the wormhole attack will never again update its routing tables with a route which is in its *blacklist_wadr*. For example, the first hop node M_1 (as it is depicted in figure 1, in the route $S, ..., D$) is considered as the creator of the wormhole tunnel and after the detection it is included in the *blacklist_wadr* of S. As a result, the communication between the source and the destination node will be established in the future through a different route preventing wormhole attacks created by the detected adversary node.

In the case of a failure in the wireless link, the deletion of the next hop node will be inappropriate. However we realize that the performance of communications will not be affected in this case. If a node deletes incorrectly a suspicious node from its routing tables, it will always have a chance to establish a new connection with the innocent node. This will happen due to the fact that other legitimate nodes will not add the potential innocent node in their blacklist unless a same link failure occurs.

Algorithm 1 AODV-WADR - PART I

a node S broadcasts a RREQ message to discover a route within MANET and records the current time t.
if S receives the RREP within NetTT **then**
  S records the receiving time $t^{'}$.
  S records the *hop count* from RREP.
  if $hopcount == 3$ **then**
    S calculates the ATT as $t^{'} - t$.
    if ATT is higher than 6· NodeTT **then**
      S suspects a wormhole tunnel in route r.
      S runs algorithm 2.
      exit
    else
      S considers the route between itself and D as safe and continues its operation according to AODV.
      exit
    end if
  else
    S continues its operation according to AODV.
    exit
  end if
else
  S continues its operation according to AODV.
  exit
end if

After the successful creation of the common unique secure session key, S sends an encrypted message *msg_wadr* to D using the Advanced Encryption Standard (AES)[9] [12] and it starts a timer in order to calculate the actual traverse time (ATT_WADR) of *msg_wadr*. If ATT_WADR is higher than

[9]is an encryption standard comprising three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. In our case, each AES cipher has a 128 bit block size, with key sizes of 128, 192 and 256 bits, respectively.

Algorithm 2 AODV-WADR - PART II

S sends a message to D in order to create a a shared secret session key (this key can be used to encrypt subsequent communications using a symmetric key cipher.) for their communication link using the *Diffie-Hellman Exponential Key Exchange* algorithm.
if S receives a respond data message from D within NetTT **then**
  S and D implement *Diffie-Hellman Exponential Key Exchange* protocol.
  S sends an encrypted with the secure session key message *msg_wadr* to D using the Advanced Encryption Standard (AES) and records the current time t_{wadr}.
  D decrypts *msg_wadr*, adds its ID number, encrypts *msg_wadr* using AES and sends it back to S.
  if S does not receive *msg_wadr* within NetTT **then**
    S considers a wormhole attack.
    S deletes r from its routing table.
    S informs its *blacklist_wa* with the next hop node.
    exit
  else
    stores the receiving time $t^{'}_{wadr}$.
    S calculates ATT_WADR as $t^{'}_{wadr} - t_{wadr}$.
    if ATT_WADR is less or equal to 6· NodeTT **then**
      S considers the route r between itself and D as safe and continues its operation according to AODV.
      exit
    else
      S considers a wormhole attack.
      S deletes route r from its routing table.
      S informs its *blacklist_wa* with the next hop node.
      exit
    end if
  end if
else
  S considers a wormhole attack.
  S deletes route r from its routing table.
  S information its *blacklist_wa* with the next hop node.
  exit
end if

MTT the node detects a wormhole attack. Afterwards, it deletes the next hop node from its routing table and adds it in the *blacklist_wadr*.

We choose for the encryption of *msg_wadr* the AES algorithm because it is fast in both software and hardware, easy to implement and requires little memory [12]. The selection of AES is based also on the fact that the standard has been designed to be resistant to well known attacks and exhibits simplicity of design too. The whole procedure of AODV-WADR from the moment it runs the DH protocol until the sending of *msg_wadr* is depicted in figure 2. For simplicity reasons, we highlight the exchanged messages between two legitimate devices to avoid depicting the intermediate node which forwards these messages during AODV-WADR.

4. PERFORMANCE EVALUATION

In this section we discuss the simulation results. We used the network simulator ns-2, to evaluate the performance of AODV-WADR. We avoided comparing AODV-WADR

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292

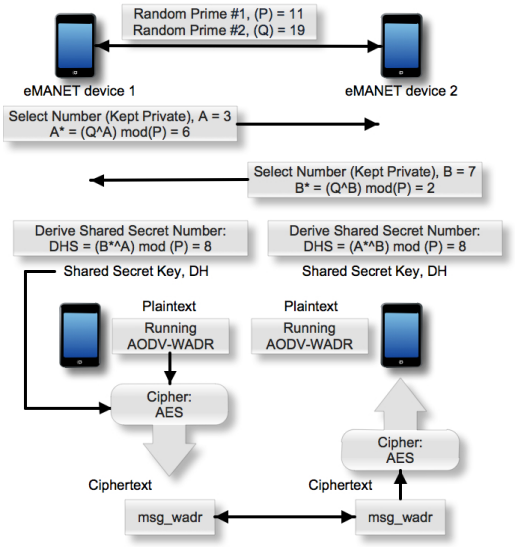

Figure 2: Two devices check the legitimation of each other by running the AODV-WADR protocol.

with other security approaches for conventional MANETs because we believe that the main characteristic of our work should be focused on securing AODV for eMANETs which has not been done by any other work according to our knowledge.

The mobility was simulated using the Mission Critical Mobility (MCM) [13] model for ns-2. MCM implements the two-way ground propagation model and the Random Waypoint mobility model considering obstacles. In the MAC layer we used the IEEE 802.11b protocol. MCM is a mobility model that captures the properties of the mobility of the nodes (firemen, policemen, medics, etc.) of eMANETs. The MCM model is proposed in the context of PEACE and it is available in [14].

We show a series of results to make clear that AODV-WADR is more efficient in terms of packet loss than AODV when malicious nodes have launched one or more wormhole attacks. In our simulations, we use different types of field configurations including 10, 25, 35, 50 and 65 mobile nodes which are moving randomly, pausing for a fixed time of 5

Table 1: The simulation parameters used in ns-2 simulator during the evaluation of AODV-WADR.

Examined approaches	AODV, AODV-WADR
Pause Time	5 sec
Number of Nodes	10, 25, 35, 50, 65
Data Rate	64 kbps
Nodes' Speed	1, 2 m/s
Simulation Time	1000 sec
Mobility Model	Mission Critical Mobility
Simulation Areas	1000m x 1000m, 2000m x 2000m
Traffic Types	UDP, TCP

seconds and then are moving randomly again in a 1000m x 1000m area or 2000m x 2000m area. The two different speeds which are considered are 1 m/s and 2 m/sec. The simulation time is limited to 1000 seconds due to the fact that after a series of experimentations, we observed the same trends in the results for longer simulations.

Furthermore, the data rate chosen is 64 kbps and the PDAs transmit text and voice data over TCP or UDP. To evaluate the performance of AODV-WADR, we compare its performance with the AODV in terms of delay and packet loss. We highlight the simulation parameters in table 1.

First, in figures 3 and 4 we depict the packet loss as a function of the number of nodes in TCP and UDP data traffic, respectively, for a $1000m \times 1000m$ area. Second, in figures 5 and 6 we depict the corresponding results for a $2000m \times 2000m$ area. In both cases, we observe that there is a lower packet loss in AODV-WADR. Such reduction occurs due to the detection of the wormhole tunnel and the exclusion of the malicious nodes, which have launched a Denial-of-Service attack, from the path between source and destination. In this way, the availability of the network resources is increased. Also, due to TCP sends more packets it consequently has higher packet loss than UDP otherwise the ratio of lost packets to sent packets is similar for both protocols.

From Fig. 5, we notice that for an $2000m \times 2000m$ area there is higher packet loss than an $1000m \times 1000m$ area because we have further links so more packets are generated including acknowledgements of TCP. These finding are the opposite in the case of UDP as Fig. 6 shows. The lower

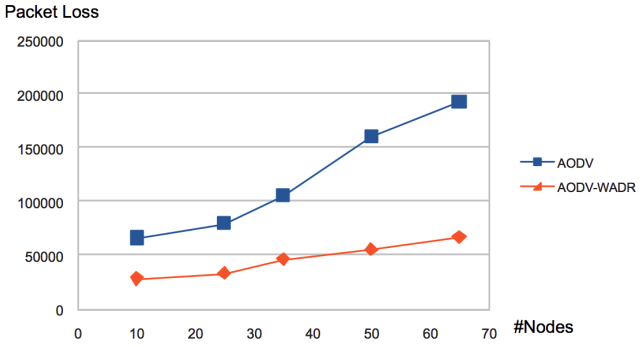

Figure 3: The packet loss for different number of nodes moving in a $1000m \times 1000m$ area (TCP traffic).

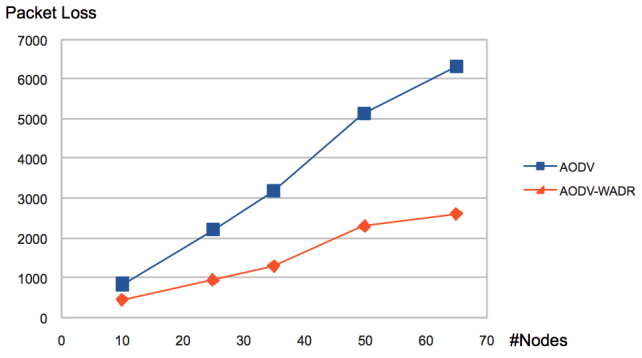

Figure 4: The packet loss for different number of nodes moving in a $1000m \times 1000m$ area (UDP traffic).

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292

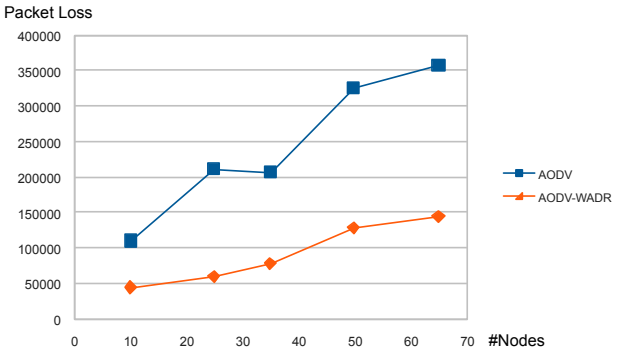

Figure 5: The packet loss for different number of nodes moving in a $2000m \times 2000m$ area (TCP traffic).

packet loss in the case of the $1000m \times 1000m$ area is explained due to the less interference caused in a larger network area when the number of devices remains the same.

In figures 7 and 8 we show the delay that each approach introduces for a $1000m \times 1000m$ area. The delay is higher in AODV-WADR due to its security functionalities. This is the tradeoff between security and AODV-WADR cost. The same trends are observed in the case of $2000m \times 2000m$ area, as we show in figures 9 and 10. In the latter case of $2000m \times 2000m$ area the delay is higher. The delay is higher in TCP because the protocol causes more congestion than UDP. As latency increases, in TCP, the sender may spend more time waiting on acknowledgements instead of sending packets. We also notice that the delay is higher for a larger network area because AODV-WADR needs more time to identify malicious nodes due to longer end-to-end communication links. Consequently, the process of adjusting the window size becomes slower since this process depends on the received acknowledgements which have to travel longer distances in a larger network area.

Last, in figures 11 and 12 we depict the improvement of packet loss for AODV-WADR, for both areas. According to the diagrams, we observe that the improvement of packet loss for TCP traffic is higher than in the case of UDP traffic in most simulations. This happens because the protocol has

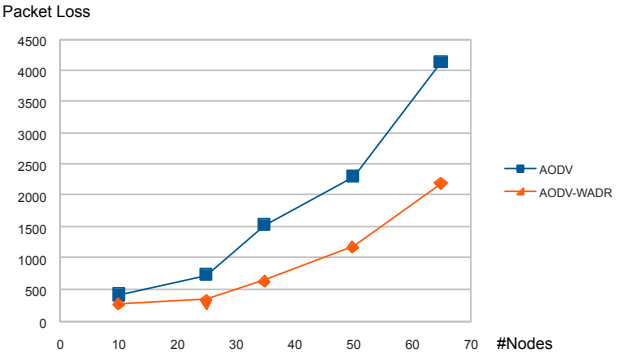

Figure 6: The packet loss for different number of nodes moving in a $2000m \times 2000m$ area (UDP traffic).

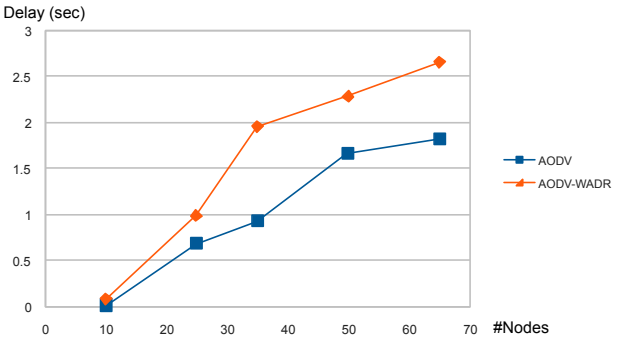

Figure 7: The delay for different number of nodes moving in a $1000m \times 1000m$ area (TCP traffic).

to retransmit any dropped packets, so for lower packet loss the improvement is more pronounced in TCP.

5. CONCLUSIONS

This paper has proposed an effective mechanism for AODV called AODV-WADR to detect and react to wormhole attacks for MANETs in extreme emergency cases, namely eMANETs. AODV-WADR does not require statistical methods, GPS coordinates or specialized hardware, since employing such methods or hardware may not be feasible in eMANETs. AODV-WADR uses the DH protocol and the AES cryptographic standard for encryption. In future work, we are planning to protect the hop count information which is the only mutable information in the messages. One possible way to achieve this aim is to use hop count hash chains as in the SAODV mechanism [15]. Additionally, it would have been reasonable if we had assumed that eMANET nodes can always be preassigned with a certain initial shared secret by the manufacturer, as in [16]. As a result AODV-WADR could even be resistant to man-in-the middle attacks.

6. ACKNOWLEDGMENTS

The authors wish to acknowledge the support of the ICT European Research Programme and all their partners in PEACE: PDMF&C, Instituto de Telecomunicaes, FhG Fokus, University of Patras, Thales, Telefonica, CeBit.

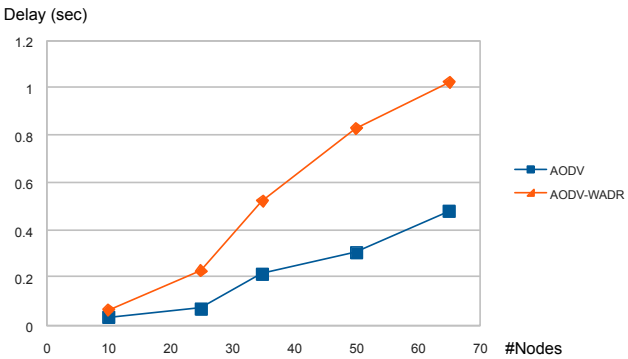

Figure 8: The delay for different number of nodes moving in a $1000m \times 1000m$ area (UDP traffic).

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292

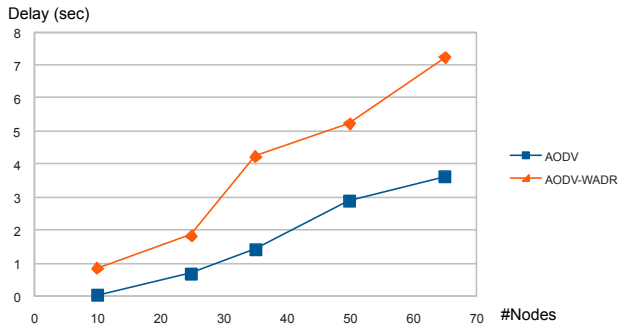

Figure 9: The delay for different number of nodes moving in a $2000m \times 2000m$ area (TCP traffic).

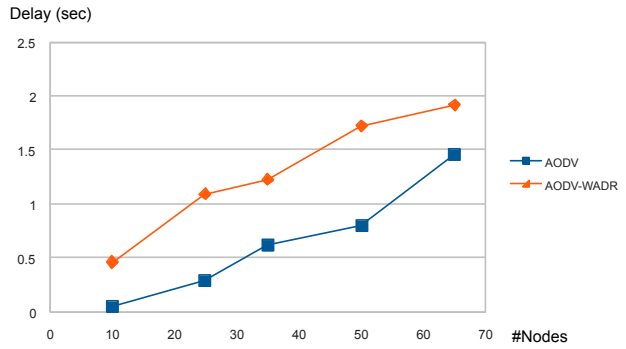

Figure 10: The delay for different number of nodes moving in a $2000m \times 2000m$ area (UDP traffic).

7. REFERENCES

[1] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey on attacks and countermeasures in mobile ad hoc networks," *Wireless Network Security, Springer Book, ISBN: 978-0-387-28040-0*, pp. 103–135, 2007.

[2] C. Perkins, E. Royer, and S. Das, "Rfc 3561 ad hoc on-demand distance vector (aodv) routing," Tech. Rep., 2003. [Online]. Available: http://tools.ietf.org/html/rfc3561

[3] T. Clausen, P. J. (editors), C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L.Viennot, "Optimized link state routing protocol (OLSR)," pp. 1–75, October 2003, network Working Group. [Online]. Available: http://ietf.org/rfc/rfc3626.txt

[4] E. A. Panaousis and C. Politis, "Securing ad-hoc networks in extreme emergency cases," *World Wireless Research Forum, Paris*, May 2009.

[5] A. A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad-hoc wireless networks," *International Journal of Network Security*, no. 2, pp. 191–202, 11 2005.

[6] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," *In Proceedings of Network and Distributed System Security Symposium, San Diego, US*, February 2004.

[7] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks."

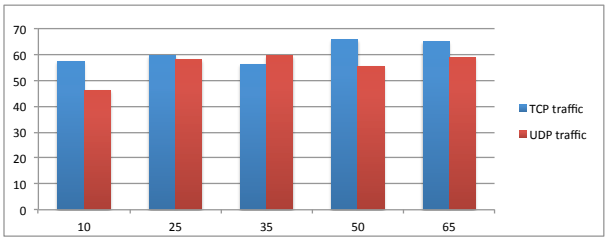

Figure 11: The improvement of packet loss for a $1000m \times 1000m$ area.

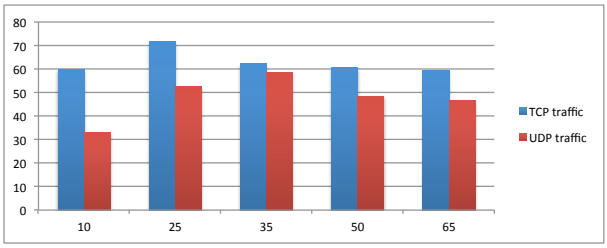

Figure 12: The improvement of packet loss for a $2000m \times 2000m$ area.

[8] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 127–133, April 2008.

[9] H. S. Chiu and K.-S. Lui, "Delphi: wormhole detection mechanism for ad hoc wireless networks," *1st International Symposium on Wireless Pervasive Computing*, p. 6 pp., Jan. 2006.

[10] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," *26th IEEE International Conference on Computer Communications (INFOCOM)*, pp. 107–115, 2007.

[11] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," vol. 3, March-3 April 2003, pp. 1976–1986.

[12] J. Daemen and V. Rijmen, "The design of rijndael aes - the advanced encryption standard, isbn: 978-3-540-42580-9," *Springer-Verlag New York.*, 2002.

[13] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "An obstacle-aware human mobility model for ad hoc networks," *17th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*, September, 2009.

[14] [Online]. Available: http://www.wltl.ee.upatras.gr/humo/

[15] M. Guerrero Zapata, "Secure ad hoc on-demand distance vector (saodv) routing," *Internet-Draft, draft-guerrero-manet-saodv-06.txt*, Sep. 2006.

[16] C. Chigan, L. Li, and R. Bandaru, "Providing unified security mechanisms for manet network layer," *International Conference on Wireless Networks*, pp. 721–726, 2004.

Digital Object Identifier: 10.4108/ICST.MOBIMEDIA2009.7292
http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7292