Ingeniería Investigación y Tecnología. Vol. XII, Núm. 1, 2011, 15-24
ISSN 2594-0732, FI-UNAM
(artículo arbitrado)
DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

Security in AODV Protocol Routing for Mobile ad hoc Networks

Seguridad en el enrutamiento del protocolo AODV para redes móviles ad hoc

Villanueva-Cruz J.A.
Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET)
E-mail: javillac@hotmail.com

García-Hernández C.F.
Instituto de Investigaciones Eléctricas (IIE)
E-mail: cfgarcia@iie.org.mx

Pérez-Díaz J.A.
Instituto Tecnológico de Monterrey, Campus Cuernavaca (ITESM)
E-mail: jesus.arturo.perez@itesm.mx

Cahue-Díaz G.
Redes, Instalaciones y Servicios a Computadoras (RISC)
E-mail: riscmi@avantel.net

González-Serna J.G.
Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET)
E-mail: gabriel@cenidet.edu.mx

Información del artículo: recibido: mayo de 2007, reevaluado: septiembre de 2009, aceptado: junio de 2010

Abstract

Routing protocols in Mobile Ad hoc Networks (mAd hoc or MANET) are exposed to several types of attacks. An attack detection module is proposed in this research work in order to protect the Ad hoc On-Demand Distance Vector (AODV) protocol against the attack known as sequence number attack (in other words, a mechanism that can counteract this attack). The performance of this module is evaluated with the ns-2 simulator and it is compared in both normal and under attack conditions. Finally, from the attack detection module we can conclude that it detects the sequence number attack, improving by approximately 20% the percentage of delivered packets.

Keywords

- security
- AODV
- protocol
- routing
- mobile ad hoc network
- mAd hoc
- MANET
- attack detection
- sequence number attack
- ns-2 simulator and delivered packets

Resumen

Los protocolos de enrutamiento en las Redes Móviles Ad hoc (mAd hoc o MANET) están expuestos a varios tipos de ataques. Este trabajo de investigación propone un módulo de detección de ataque para proteger el protocolo de Vector de Distancia sobre Demanda Ad hoc (AODV) en contra del ataque conocido como número de secuencia (o sea un mecanismo que contrarresta este ataque). Se evalúa el desempeño del módulo con el simulador ns-2 y se compara bajo condiciones normales y bajo ataque. Por último, del módulo de detección de ataques podemos concluir que detecta el número de secuencia, mejorando aproximadamente en 20% el porcentaje de los paquetes recibidos.

Descriptores

- *seguridad,*
- *aodv*
- *protocolo*
- *enrutamiento*
- *red móvil Ad hoc*
- *mAd hoc*
- *MANET*
- *detección de ataque*
- *ataque de número de secuencia*
- *simulador ns-2 y paquetes entregados*

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

Introduction

In recent years, the usage of wireless and mobile networks has increased considerably (García *et al*., 2004). In this context, the mobile Ad hoc networks (MANET) are an alternative for applications when using other kind of networks is not viable. A MANET is a collection of mobile and wireless nodes which form a temporary network without using a network infrastructure or a centralized administration. These network nodes behave as routers and participate in the routes discovery and routes maintenance tasks in conjunction with the other network nodes.

A MANET is created in a dynamic way, spontaneously in many times; and the lifetime of the nodes that participate in the network is generally short. As a consequence, the nodes come in or get out of the network without a previous notice, thus varying the network topology. This behaviour allows the creation of a network from scratch and without any intervention of users to configure it. The network size varies when nodes approach or move away from the network coverage area. This panorama is what makes MANETs very attractive, allowing to place them in any scenario or for any use.

However, new challenges in security are originated due to the fact that there is not a centralized infrastructure and the devices can move randomly. The conventional security solutions used in other networks cannot be applied in MANET because of the features that this kind of networks have. In addition to the vulnerabilities of the wireless networks, where the channel is open and available, MANETs have other kind of problems because of the fact that an un-authenticated node can participate in the network without being detected. This intruder may just listen to the traffic, send false packets to its neighbors or not collaborate in the network routing at all, provoking that the network doesn't work properly.

Another challenge to face is that there is not a central entity that allows the authentication of users, because MANETs are distributive in nature. As a consequence, the design of new solution mechanisms to face these limitations and adapt them to MANET features is needed.

AODV protocol description

One of the features defining the AODV is the use of routing tables in each node in order to avoid transporting routes information in the packets. Every destination of the routing table is associated to a sequence number and a timer or lifetime. The sequence number allows the network to distinguish between recent information and old information, thus preventing the formation of loops and the transmission of old or expired routes through the network. The timer function is to prevent the usage of links whose status is not known since long time ago.

AODV doesn't keep routes for each network node. These routes are discovered as they are needed. AODV is able to provide unicast, multicast and broadcast transmission. Unicast transmission consists in sending data from one node to another one, multicast transmission consists in sending information from one node to a group of nodes and broadcast transmission consists in sending data from one node to the other network nodes.

Routes discovery

When a node wishes to send data to another node, it checks first whether it has an entry in its routes table for that destination. If it has an active entry, it routes data through the neighbor indicated by the table. However, if the source node does not have an active entry because it is the first time that it is going to communicate with that node or because the time for that destination has expired (this information is obtained by checking the *lifetime* field and the last modification date), a route discovery process is initiated. Hence, a ("Route Request") RREQ packet is generated. This RREQ packet contains information related to the destination node, besides its own information. RREQ packet format and its fields are published in (Perkins *et al*., 2003).

The source node initiates the route discovery process by transmitting a RREQ packet to its neighbors, which do the same transmitting this packet to their neighbors and so on until reaching the destination node or any intermediate node with a sufficiently "fresh" route towards the destination node in its routing table (Perkins *et al*., 2003).

Each RREQ packet is identified with its own identifier (RREQ ID). This identifier is incremented each time a new RREQ is generated and the intermediate nodes use it in order to know whether they have to retransmit the packet or, on the contrary, discard it because it was already retransmitted previously. If intermediate nodes have enough information to reach the destination node, they reply to the source node to avoid unnecessary propagation of the RREQ through the network. Even having this information, intermediate nodes reply only to the RREQ if they have (in their routing table) a route to the destination with a Destination Sequence Number bigger or equal to the one the RREQ has. In other words, they reply only if they have routes equal in age or more

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

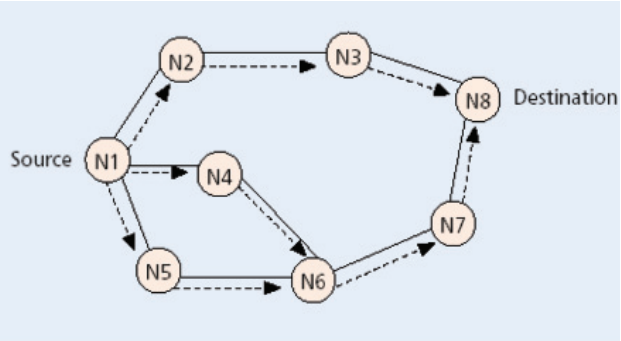

Figure 1. Path discovery in AODV (Deng *et al*., 2002)

recent ones than the one the RREQ has. The route discovery process is shown in figure 1 (Deng *et al*., 2002).

While RREQ is being sent, intermediate nodes are increasing the Hop Count field and they do also register in their routing table the address of the neighbor from whom they received the message first, in order to be able to establish a reverse path. Once the destination node or an intermediate node with recent route has been found, this one replies with a unicast packet called RREP (Route Reply) to the neighbor from whom it received the first RREQ. RREP packet format structure is published in (Perkins *et al*., 2003).

If the node generating the RREP is the destination node, it increases its sequence number by one and places a zero value in the Hop Count field of the RREP packet. If any intermediate node generates the RREP, this one places the destination sequence number stored in its table to that destination, and also the required hops to reach it. When RREP travels back to the source node, a forward path to the destination is established. Every node which RREP is passing through updates the sequence number for the requested destination. The source node begins to transmit data packets as soon as the first RREP is received. Reverse path is illustrated in figure 2 (Deng *et al*., 2002).

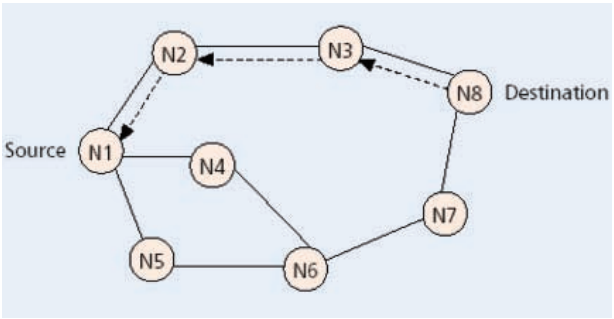

Figure 2. Reverse path in AODV (Deng *et al*., 2002)

The table's entry that keeps the reverse path is deleted after a time interval. In the same way, the table's entry that keeps the forward path is deleted if it is not used in a time interval.

It is possible that the source node receives more than one RREP from its neighbor nodes. In this case, the route from the first received RREP is used and when any other RREP arrives afterwards, the node checks if the latter packet contains a bigger destination sequence number or the same destination sequence number with a smaller hop count, meaning that it provides a fresher route. If any of these conditions is carried out, the table is updated with the new values; otherwise the packet is discarded (Perkins *et al*., 2003).

Attacks on AODV

AODV was designed assuming that none of the nodes forming the network is a malicious node. RFC 3561 (Perkins *et al*., 2003) defines in detail the AODV protocol and it mentions that there is not a native security mechanism for the routing protocol, thus presenting the risk of several attacks. Attacks can be classified in different ways (Zhou *et al*., 1999; Yan, 2003). Some classifications are based on the sources of the attacks (internal and external attacks) or on the methods used by attackers to acquire control. In general, attacks are classified in two types:

- *Passive attacks*: A malicious node accomplishes a passive attack when it ignores some operations, for example, when it does not participate in the path discovery process.
- *Active attacks*: A malicious node accomplishes an active attack by introducing false information into the network. This creates confusion on the procedure and degrades the network performance (Wang *et al*., 2003).

In order to carry out this research work, a specific kind of attack was chosen with which the protocol is exposed. The active attack known as *sequence number attack* was chosen for several reasons:

1) It is one of the most reported attacks from literature, for example in (Deng *et al*., 2002) and (Wang *et al*., 2003),
2) An attacker does not do big efforts to realize the attack and
3) It has a great impact in network performance.

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

- *Sequence number attack* (Ning *et al*., 2003). Protocols such as AODV and DSDV (Destination Sequenced Distance Vector) (Hu *et al*., 2003 and 2002; Guerrero *et al*., 2002; Sanzgiri *et al*., 2002) create and keep routes by increasing the sequence numbers towards specific destinations. Since the sequence numbers from the destinations determine how "fresh" a route is, and according to the protocol the newer or fresher routes are priority, a malicious node is able to redirect a route by assigning a big sequence number in a RREP. This attack is also known as "black hole" and it is similar to the false distance vector attack. The former attack affects more the network performance, since AODV protocol prefers fresher routes better than shorter routes.

In figure 3, the source node initiates a route discovery process to the destination node by sending a RREQ packet. When a malicious node receives the RREQ, and even if it does not have a fresh route in its routing table for the requested destination, it creates an RREP packet with false information about the sequence number.

Aiming that the false information is favoured, the malicious node enters a big sequence number in the Destination Sequence Number field. If this "false" RREP is received before a legitimate RREP by the requesting node, then the malicious node takes part in the route and it can intercept data traffic. Even if the RREP manipulated by the malicious node does not reach the source node before other RREPs, attack can be carried out because the destination sequence number of the "false" RREP is bigger than the one for the original route, which will be replaced with the "false" one.

The strength of this attack lies on the fact that the "false" route will be propagated towards other legitimate nodes, which will update their own table and will, consequently, reply to future RREQs with this false information registered on their routing tables. Therefore, the false information is propagated to other nodes without the intervention of the malicious node (Zhang *et al*., 2000).

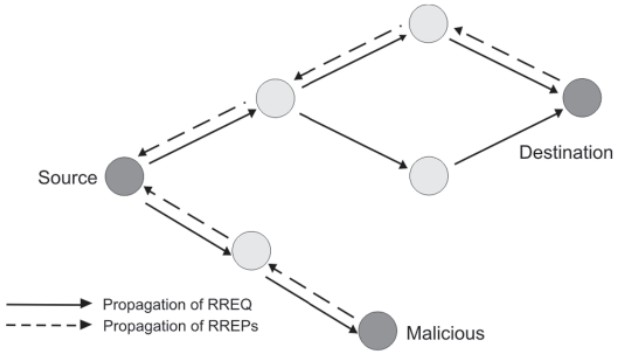

Figure 3. Example of the sequence number attack

Proposed scheme

Before implementing the solution proposed in this paper, we have conducted a deep analysis on the AODV protocol and its source code using the ns-2 simulator (Chung *et al*., 2003; Fall *et al*., 2003; Greis, 2003). We have made particular emphasis on the packet reception and packet sending methods, which are the ones in which the attack in question takes place (Villanueva, 2005). The recvReply method acquires great relevance since this is the one processing the RREP packets when they reach a particular node and the sequence number attack takes place within these packets. Following, we show on figure 4 a graphic representation of the recvReply method, as well as of our proposed enhancement: the attack detection module.

As it is depicted on figure 4, the attack detection module is located at the beginning of the recvReply method. Thus, enabling the packet processing before an eventual attack takes place. Once a RREP packet has reached the attack detection module, the latter should analyze it to determine whether it is malicious or not. If the packet is malicious, the module triggers a corresponding action or output; if not malicious, the method continues until normal termination and, once this occurs, the AODV protocol continues with its normal operation. This attack detection module is incorporated in the routing protocol used by all of the nodes in the mobile Ad-hoc network.

Given the characteristics of the Ad-hoc mobile networks, an intruder detection system should comply with certain minimum requirements (Albers *et al*., 2002):

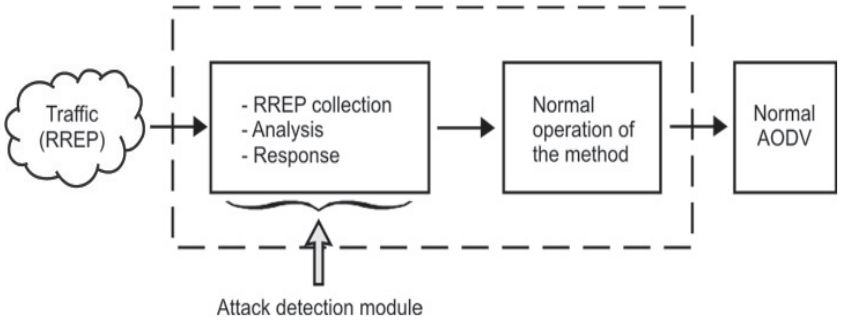

Figure 4. Detection module incorporated in recvReply method

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

- It should not introduce new vulnerabilities into the system.
- It should require a minimum amount of system resources, thus not affecting its performance by introducing additional work load.
- It should operate continuously and remain transparent for the system and for the users.
- It should be reliable and minimize any "false alarms".

As it is expected, our goal is that the attack detection module we are proposing complies with these requirements.

The proposed attack detection module uses the host-based intrusion detection technique (Mira, 2003; Marti *et al*., 2000; Bhargava *et al*., 2001) for detecting the sequence number attack. Given that we know the way the malicious node can carry out the attack, our analysis is based on the detection of misuses. The attack detection module does not introduce changes in the routing protocol and it operates as an intermediate component between the network traffic and the routing protocol, with a neglected delay compared with the other delays of the process.

Implementation of the attack detection module

In order to get a closer view of how the attack detection module works in conjunction with the recvReply method, please refer to figure 5. Ignoring the dotted area of the flow diagram you can get a whole picture of the recvReply method's normal operation (the normal process a node follows when it receives a RREP packet). The dotted area in the same figure 5 represents the modification we are proposing.

Let us consider figure 5 ignoring the dotted area: when a RREP packet is received, the node compares the sequence number the packet brings with the sequence number registered on the node's table; if the number on the RREP is greater (no matter to what extent) the record is updated in the table, thus allowing the creation of a route using the path set by the RREP. This is the moment a malicious node takes advantage of for attacking, by sending a sequence number that is greater to any other RREP the node could receive.

The dotted area on figure 5 represents the attack detection module we are proposing. When a node receives a RREP, it determines if the reply packet has as a final destination the node in question itself, in other words, if the node itself is the one who initiated the route discovery process with anticipation. If the node in question is not the source node, the process after receiving the RREP continues just as described in the preceding paragraph. If the node in question is the source node a second verification takes place this time regarding how big is the sequence number that comes with the RREP compared with the sequence number stored in the node's table. The rationale behind this comparison is that we know that a malicious node should increment this number on the manipulated

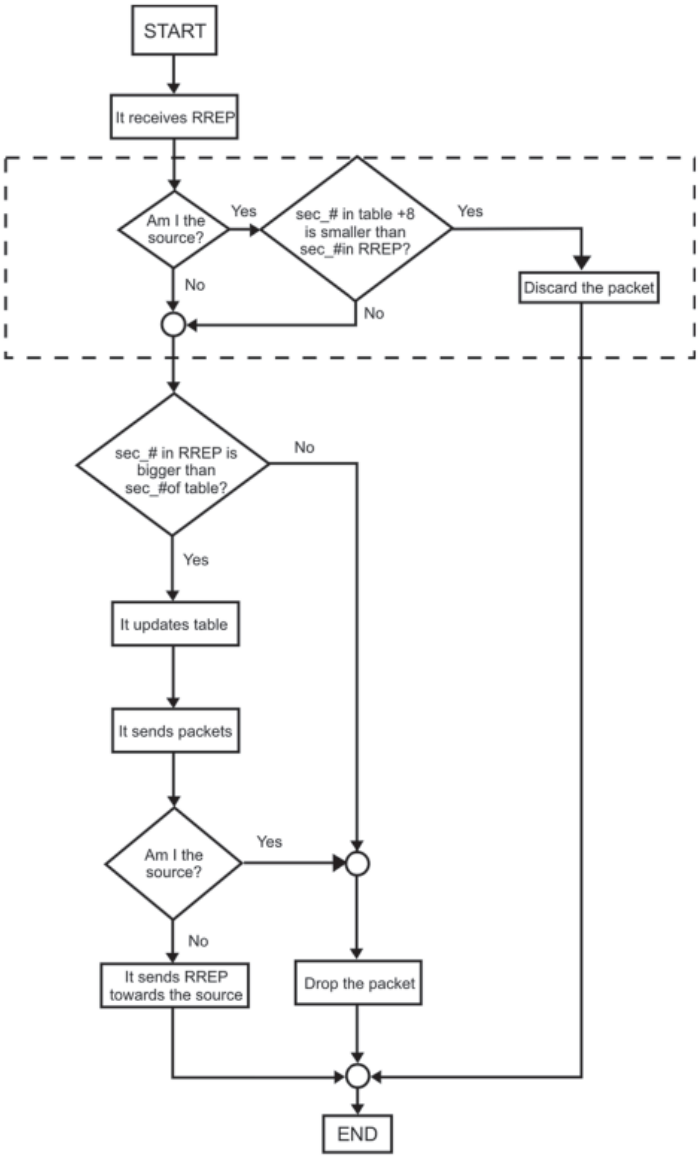

Figure 5. Process of receiving a RREP packet with the incorporated attack detection module

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

RREP to a extremely big value. In our proposal we add a value of eight (as a result from many simulations of different scenarios for our case of study, as explained in the following paragraph) to the sequence number stored in the node's table. If the sequence number in the RREP is greater than the one in the node's table plus eight, we know we are facing a clear sign of an abnormal operation since this number should not be that big. Therefore, the node will not update its table or execute any other action determined by the method. Finally, the node discards the packet, as an output. If the failure condition is not met (that is, the sequence number in the RREP is not greater than the one in the node's table plus eight) the method continues on its normal operation

It is true that nobody knows with certainty the increment an attacker will apply to the sequence number of a RREP package (for this case of study we know the sequence number is increased by a value of +10, though), however, the attacker will have to choose a value great enough to guarantee that other routes can be replaced by his. The number 8 represents a limit (or border) value to determine if the RREP comes from a malicious source or not. We tested other limit values through various simulations and the value of eight proved to have the better efficiency to detect the attacks and also to prevent false detections of attacks, for our case of study.

Simulation results

The AODV protocol performance was evaluated with the "Network Simulator 2" (ns-2), which is one of the most powerful tools used to simulate wired and wireless network protocols. For our case of study, three simulation scenarios were considered: in the first one the simulation was carried out in normal conditions, in other words, all the nodes participated correctly in the routing functions. In the second scenario, one of the nodes was a malicious node which accomplished the sequence number attack. In the third scenario, an attack detection module was proposed and it was incorporated in the AODV protocol and simulated again.

The metrics that we used to evaluate the attack detection module performance are the following: (1) Packet delivery ratio or percentage (considered as our most important metric), (2) Number of RREP packets sent by node number 2 (the malicious node), (3) Accuracy on attack detection, and (4) Average latency of the transmitted packets.

In the simulation scenarios, the nodes mobility and the number of active connections are varied in order to observe their impact in network performance. We enlist the simulation parameters as follows: Operating system - Linux Red Hat 7.3, Simulator - ns-2, Simulation duration - 1000 seconds, Simulation area - 850 m⊛850 m, Number of mobile hosts – 20, Transmission range - 250 m, Movement model - Random waypoint, Maximum speed - 4-20 m/s, Traffic type - CBR (UDP), Data payload - 512 bytes, Packet rate - 2 pkt/s, Number of malicious nodes - 0-1 (0 in normal conditions and 1 under attack) y Host pause time - 10 seconds. The parameters are very similar to those reported in other research efforts, such as (Wang *et al*., 2003). We decided to use these similar values in order to obtain a "standard" comparison measurement with the results obtained. We are not considering very high values of node movement speed given that the consequent frequency of routes variation would be too big, thus impacting the malicious node's effects. The packet sending rate has been chosen in such a way that prevents loses of packets caused by congestion.

Figure 6 shows an example of what occurred during our simulation with the "nam" tool (ns-2). Node 4 should establish a communication with node 5, but node 2 interferes taking into place a sequence number attack.

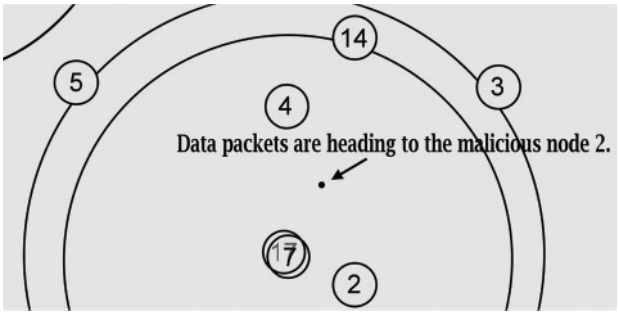

Figure 6. Nam visualization (ns-2) – under attack

The results we obtained on our simulations are presented in the following graphics.

Packet delivery ratio

The graphic on figure 7 shows the percentage of packages delivered when varying the number of connections. The results coming from the three simulation scenarios are included.

The impact produced in the network when it is under attack can be observed; the packet delivery ratio in destination nodes decreases almost to the 40%. When the attack detection module is added and the network is under attack, the packet delivery ratio increases approximately to the 60% (it improves almost by 20%).

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

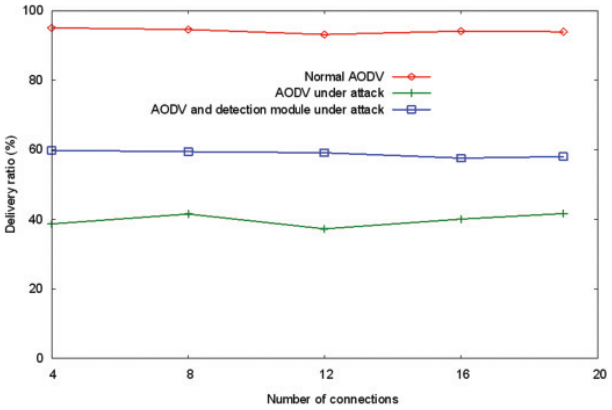

Figure 7. Packet delivery ratio versus number of connections

The packet delivery ratio when varying the node speed (packet delivery ratio versus nodes mobility) resulted very similar to figure 7. Also in this case, the delivery rate increases on a 60% approximately, achieving an improvement of almost 20%.

Number of RREP packets sent by node 2 (malicious node)

Figure 8 shows the number of RREP packets sent by node 2 (the malicious node) versus the number of connections in normal conditions. In order to evaluate this metric and observe the behavior of the curves, we have placed the respective graphics on separate figures. Figures 9 and 10 depict the number of sent RREP packets versus the number of connections without or with the module incorporated, respectively, and both under attack conditions.

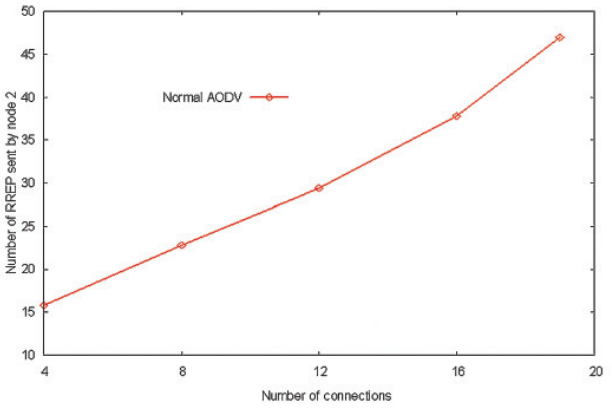

Figure 8. Number of RREP sent by node 2 versus number of connections (normal conditions)

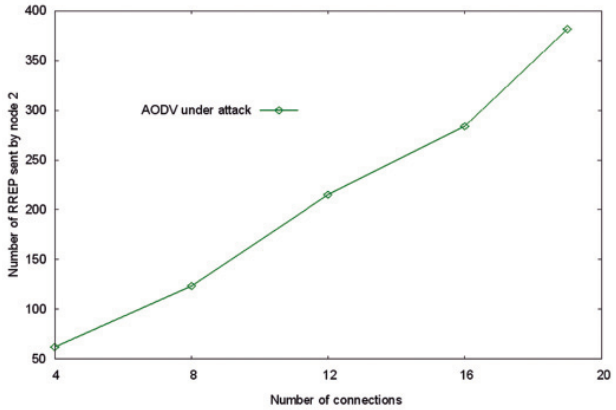

Figure 9. Number of RREP sent by node 2 versus number of connections (under attack)

The three graphics show a proportional behavior between the number of connections and the number of RREP packets sent by node 2. This is normal since a great number of traffic connections in the network provides a greater chance to the malicious node to send RREP packets. Nevertheless, when the attack takes place the number of sent RREP messages (false messages in this case) is much bigger than the number of messages sent under normal conditions. This is because the attack is implemented in such a way that the malicious node replies with a false RREP to any route request that reaches it. With the detection module incorporated the number is even bigger; this is because there is a moment in which the source node discards any RREP it receives (due to broken links or increments in the sequence number). In that moment there is not an available route for the source node, which is continu-

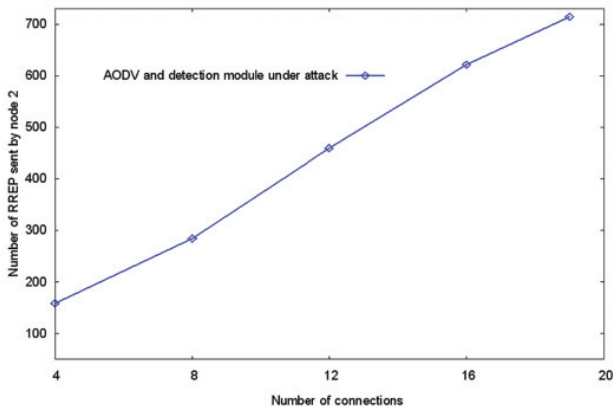

Figure 10. Number of RREP sent by node 2 versus number of connections (detection module and under attack)

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

ously sending route requests, and that explains the increment on the number of RREP.

In this article we are not including the graphics generated when the node speed suffers variation, but the behavior of the curves is very similar to the ones depicted on figures 8, 9 y 10 (Villanueva, 2005).

Accuracy in attack detection

Figure 11 shows the delivery ratio versus the number of connections and packet delivery ratio versus nodes mobility (accuracy in attack detection) resulted very similar to figure 11. In these cases we are considering both normal conditions and the incorporation of our module (both without the presence of malicious actions).

It is important to verify that, when the network is not under attack and has the detection module incorporated, the network performance doesn't decrease in a significant way, otherwise it would not be useful for our purposes. All of the intruder detection systems present false alarms when they consider there is a malicious behavior on the network but there is really not such. Abuse-detection based systems, which is the technique used by our module, fall in less errors than other techniques. Figure 11 shows that, for our case of study, there is not a big difference in the curves that affects the performance.

Transmitted packets average delay

Figures 12 and 13 show the graphics obtained when analyzing the packets' average delay versus the number of connections and the node mobility for every simulation scenario. We are including here the possible delays due to buffering during the route discovering delay, the interface queue, the MAC layer's transmission delay and the time for transferring.

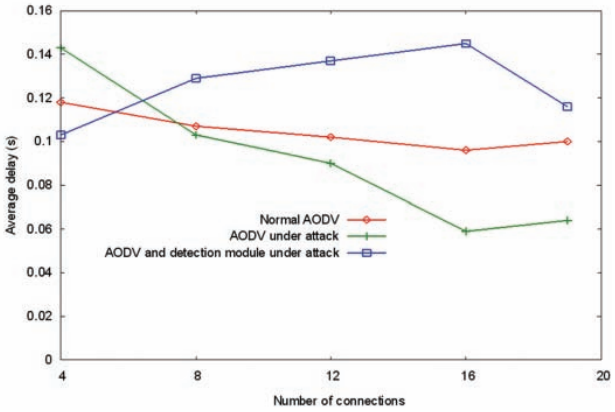

Figure 12. Average delay versus number of connections

Figure 12 shows that there is a decrease on the average delay when the protocol in under attack (compared with the normal operation). It is important to mention that in this case the average is obtained from a fewer quantity of packets, that is, only those that are delivered to their destinations. When the detection module is incorporated there is a light increasing on the average delay due to the time used by the source node in determining whether it is being attacked or not. Figure 13 depicts a similar behavior, even though it is clear that the delays increase as the nodes' velocity augments. This situation is due to the fact that there are more link breaks in the scenario and new route requests have to be originated, therefore the packets need to wait a period of time before being transmitted (Villanueva, 2005).

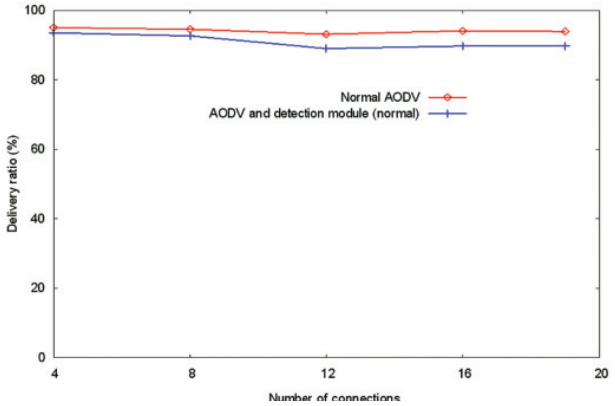

Figure 11. Packet delivery ratio versus number of connections (accuracy in attack detection)

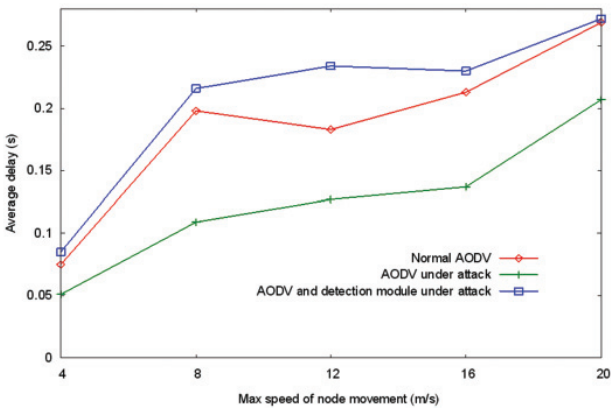

Figure 13. Average delay versus nodes mobility

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

Conclusions

The challenge of providing security is greater when we are talking about a wireless and mobile network. Freedom is the main advantage provided by wireless and mobile devices and it is, ironically, the source of its major problems. In particular, Mobile Ad-hoc Networks (mAd hoc or MANET) present the following challenges: open network architecture, shared wireless environment, limited computational resources, limited battery life, dynamic topology and structure. Finally, from the attack detection module we can conclude that: It does not introduce significant changes on the AODV protocol, thus its operation mode remains practically unchanged and transparent for the users; Detects the sequence number attack, improving in approximately a 20% the percentage of delivered packets; It does not generate a high quantity of false detections; Simulations demonstrated the presence of an insignificant increase on the packets' average delay after incorporating the attack detection module; and This attack detection module could be extended for protection from other attacks and even to isolate the malicious node, and also considering more than one malicious node.

References

Albers P. *et al*. Security in ad hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. 1st International Workshop on Wireless Information Systems, (WIS 2002) and 4rth International Conference on Enterprise Information Systems, April, 2002.

Bhargava S. *et al*. Security Enhancements in AODV Protocol for Wireless Ad hoc Networks, IEEE Semi-annual Proceedings of Vehicular Technology Conference (VTC'01), 2001.

Chung J. *et al*. NS by Example, ns-2 Simulator Tutorial [on line]. Available on: http://nile.wpi.edu/NS/

Deng H. *et al*. Routing Security in Wireless Ad Hoc Networks. *IEEE Communications Magazine*, 40(10):70-75. October 2002.

Fall K. *et al*. The *ns* Manual (formerly *ns* Notes and Documentation). Official ns-2 Simulator Manual, December 2003 [on line]. Available on: http://www.isi.edu/nsnam/ns/ns-documentation.html

García-Hernández C.F., Zaleta-Alejandre E. Quality of Service Management Efficient Scheme for the Universal Mobile Telecommunications System. IEEE-ROC&C'2004, C-01, November 23-28, 2004.

Greis M. Tutorial of the Network Simulator ns. ns-2 Simulator Tutorial [on line]. Available on: http://www.isi.edu/nsnam/ns/tutorial/

Guerrero M. *et al*. Securing Ad Hoc Routing Protocols. ACM Workshop on Wireless Security (WiSe) in conjunction with ACM MobiCom'02, September 2002.

Hu Yih C. *et al*. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless ad hoc Networks [on line]. Available on: http://www.ece.cmu.edu/~adrian/projects/secure-routing/sead-journal.pdf

Hu Yih C. *et al*. Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks. 8th Annual International Conference on Mobile Computing And Networking (ACM MobiCom'02), September 2002.

Marti S. *et al*. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. 6th Annual International Conference on Mobile Computing And Networking (ACM MobiCom'00), August 2000.

Mira E. Sistemas de Detección de Intrusos [on line]. Available on: http://www.uv.es/~montanan/ampliacion/trabajos/

Ning P. *et al*. How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad hoc Routing Protocols. 4th Annual IEEE Information Assurance Workshop, pp. 60-67, June 2003.

Perkins Ch.E. *et al*. Ad hoc On-Demand Distance Vector (AODV) Routing, Request For Comments (RFC) 3561, July 2003.

Perkins Ch.E. *et al*. Ad hoc On-Demand Distance Vector Routing [on line]. Available on: http://www.cs.brown.edu/courses/cs295-1/aodv.pdf

Sanzgiri K. *et al*. A Secure Routing Protocol for Ad Hoc Networks. 10th IEEE International Conference on Network Protocols (ICNP'02), November 2002.

Villanueva-Cruz J.A. Security in AODV Protocol Routing for Mobile Ad Hoc Networks. (MSc Thesis). CENIDET. 2005.

Wang W. *et al*. On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol. 10th International Conference on Telecommunications (ICT'2003), February 2003.

Yan Z. Security in ad hoc Networks [on line]. Available on: http://citeseer.ist.psu.edu/update/536945

Zhang Y. *et al*. Intrusion Detection for Wireless Ad-Hoc Networks. 6th Annual International Conference on Mobile Computing And Networking (ACM MobiCom'00), August 2000.

Zhou L. *et al*. Securing ad hoc Networks. *IEEE Network*, 13(6): 24–30, November/December 1999.

DOI: http://dx.doi.org/10.22201/fi.25940732e.2011.12n1.003

About the authors

José Alonso Villanueva-Cruz. Obtained his B.S. degree in electronics from The Technology Institute of Mérida (ITM), México in 2000, and his M.S. degree in electronics (digital systems, communications) in the National Center of Research and Technology Development (CENIDET) in Cuernavaca, Mexico in 2005. From 2000 to 2002 he was a support engineer in EN Computación in Cuernavaca, Mexico. Also he has diplomas in the area of telecommunications and electronics. His research areas are wire and wireless networks and mobile communications. At present, he works in Telcel as a Terminal Equipment Analyst.

Carlos Felipe García-Hernández. Obtained his B.S. degree in communications and electronics from the University of Guanajuato, México, in 1983 and his M.S. degree in telecommunications systems from the University of Essex, England, in 1986. He is a lecturer at ITESM Cuernavaca at B.S. level since 1996 and in CENIDET at graduate level since 1987. He is a researcher and project manager at the Electric Research Institute (IIE) since 1983. He was a National Researcher Level-I (SNI), from1987 to 1993, he is an IEEE Senior member, a CIGRE corresponding member and a CIME member. He is a professional engineer and a telecommunications consultant, certified with registration No. 555 from the SCT (Telecommunications and Transport Bureau) and the COFETEL (Federal Telecommunications Commission) with the specialty on radiocommunications since 1993.

Jesús Arturo Pérez-Díaz. Obtained his B.S. degree in computer science from the Autonomous University of Aguascalientes (1995). He got his PhD degree in computer science in 2000 from the University of Oviedo, Spain; he became associate professor of the Computer Science Department in the same University from 2000 to 2002. His work was related to network and Internet security. He is now a researcher and professor at ITESM–Campus Cuernavaca and member of the Researchers National System (SNI), his research field is focused in network security and wireless communications. He has Cisco certifications CCNA and CCAI, which allow him to give Cisco certification courses. He lectures in the graduate programs at ITESM, he supervises master and PhD theses in the same field.

Guillermo Cahue-Díaz. Obtained his B.S. degree in communications and electronics with specialization in communication from the National Polytechnic Institute (1987). He got his M.S. degree in computer science from ITESM Campus Cuernavaca (1984). He worked in the computer science unit of the Electric Research Institute from 1978 to 1989. He collaborates with the CENIDET teaching in the Electronics Department since 1987. He has supervised theses and designed speciality courses. He is a member of the Researchers National System (SNI) and expert in teleinformatics registered by the SCT. He is life member of the Mechanic and Electric Engineer Association.

Juan Gabriel González-Serna. Obtained his B.S. degree in computer systems from the Acapulco Institute of Technologic (ITA-SEP), México, in 1992 and his M.S. degree in computer science from the CENIDET Mexico, in 1995. In 1997 he started his PhD degree in the computing research center, National Polytechnic Institute (CIC-IPN), Mexico. He works at CENIDET Computer Science Department as a researcher and professor, and he has been in charge of several research projects on wireless and mobile networks. He lectures B.S. courses in ITESM Cuernavaca since 2003 and graduate courses in CENIDET since 1995.