ASROP : AD HOC SECURE ROUTING PROTOCOL

Rida Khatoun, Lyes Khoukhi, Ahmed Nabet and Dominique Gaïti

ICD - ERA - University of Technologies of Troyes (UTT), STMR, UMR CNRS 6279
12, rue Marie Curie 10000 - Troyes, France

Email: rida.khatoun@utt.fr

ABSTRACT

Mobile ad hoc networks (MANETs) are a new concept of wireless communications for mobile devices, which offer communications over a shared wireless channel without any pre-existing infrastructure. Their wireless nature and self-organizing capabilities are some of MANET's biggest advantages, as well as their biggest security restrictions. Forming end-to-end secure paths in such MANETs is more challenging than in conventional wireless cellular/wired networks due to the lack of central authorities. An attacker can easily disrupt the routing process by injecting false control messages, changing the paths of packets or simply by blocking the packets of other nodes. In this paper, we propose a novel efficient secure routing protocol, named ASRoP, to effectively secure the routing discovery process in ad hoc networks. ASRoP provides powerful security extensions to the reactive AODV protocol, based on Diffie-Hellman (DH) algorithms and our modified secure remote password protocol. The simulation results show the efficiency of the proposed ASRoP protocol, and its cost towards both the users and the network. ASRoP promises to offer a real opportunity to prevent attacks related to lack of authentication without degrading routing performance.

KEYWORDS

Wireless Network, Ad hoc Network, Security, Wireless Routing Protocol

1. INTRODUCTION

In recent years, wireless ad hoc networks (MANETs) have received tremendous attention because of their self-maintenance and self-configuration capabilities. A MANET is a set of autonomous wireless mobile devices that communicate with each other over wireless links. Such networks do not require the deployment of any infrastructure for their operation; thus, it is expected that they will play a vital role in future civilian and military settings, being useful to provide communication support where the deployment of a fixed infrastructure is not possible or economically profitable. The topology of MANETs is in general dynamic, because the connectivity among the nodes may change with time due to the dynamics of nodes or churn. Communication is performed by relaying data packets along suitable routes, which are dynamically discovered and maintained through cooperation between the nodes; thus, any routing protocol design must consider the limitations and constraints of MANETs.

Several routing schemes have been proposed in the literature (e.g. AoDV [1], DSR [2], etc.). These schemes focus mainly on finding routes between sources and destinations nodes, and on efficiency issues such as scalability with respect to network size and traffic load [3]. Usually, the length of routes is the main metric used in these schemes. It is observed that most of these routing schemes have ignored the aspect of network security; thus, they are vulnerable to attacks since they do not consider a secure path during the route discovery process. To alleviate this limitation, several approaches have been proposed to secure ad hoc routing. Some of these approaches employ mechanisms used to protect routing protocols in wired networks based on the presence of a centralized infrastructure; however, these solutions may not be appropriate for a decentralized environment such as ad hoc network.

DOI : 10.5121/ijwmn.2012.4501

In this paper, we propose a novel secure routing scheme for mobile ad hoc networks based on AODV on-demand protocol, named ASRoP. It is specifically designed to an open wireless ad hoc network where each node should verify the identity of the node with which it communicates. On the contrary to the classical use of remote secure routing protocol which is actually employed in "client-server" context; our contribution proposes to use a modified version of this protocol in distributed ad hoc mobile environment. This allows nodes to be authenticated before considering any information during the route discovery phase. In our ASRoP, we focus on attacks carried out by traditional external illegitimate nodes which do not have the access rights to the ad hoc network. Our protocol considers also some other attacks that may be carried out by internal malicious nodes that inject false information about the network topology. Moreover, the proposed protocol ensures the reliability of the route (s) obtained during the route discovery phase. The contributions of this paper can be summarized as follows:

- a new security protocol based on AODV that ensures the establishment of a secured routes between source and destination nodes, while it reduces the load of cryptographic functions conventionally used
- a new way of detecting and rejecting forged or replayed messages
- a new key exchange method achieved in a fully distributed fashion without any need for a permanent or temporary infrastructure

The rest of the paper is organized as follows. Section 2 highlights some vulnerabilities of MANETs and presents a brief state of the art of some secure routing solutions. In Section 3, we detail our proposed secure routing protocol ASRoP. The performance evaluation of ASRoP are presented in Section 4. Finally, Section 5 concludes this paper.

This document describes, and is written to conform to, author guidelines for the journals of AIRCC series. It is prepared in Microsoft Word as a .doc document. Although other means of preparation are acceptable, final, camera-ready versions must conform to this layout. Microsoft Word terminology is used where appropriate in this document. Although formatting instructions may often appear daunting, the simplest approach is to use this template and insert headings and text into it as appropriate.

2. ROUTING SECURITY IN AD HOC NETWORKS

2.1 Vulnerabilities in ad hoc networks

Despite the fact that wireless networks are more flexible than wired networks, they are also more vulnerable to attacks. This is due essentially to the fact that wireless channel is accessible to both legitimate network users and malicious attackers. In traditional wired networks; to eavesdropping, an intruder would need to listen physically to the cable. However, in wireless networks, an attacker is able to listen to all messages in the transmission area [4]. Therefore, just by being in the same coverage area, the intruder has access to network communications and can easily intercept the data transmitted without the sender knowing about the intruder attacks. As the intruder is virtually invisible, it can also record, edit, and then retransmit packets as they are issued by the sender, even claiming that the packets originate from a legitimate party. In addition, due to environmental constraints, wireless communications can easily be disturbed; the attacker can perform this attack by generating some noises. Attacks on MANET could be categorized in 5 layers; Application layer, Transport layer, Network layer, Link layer, and Physical layer [5. In this paper, we focus on network layer attacks; this kind of attacks aims to change the routing protocol to redirect traffic to a specific node that is under the control of attackers. An attack may also prevent the construction of the network, announcing incorrect

routes, and more generally to corrupt the network topology [6][7]. Routing attacks can be classified into two categories: incorrect traffic generation and incorrect traffic relay.

2.1.1 Incorrect traffic generation

This category includes attacks that involve sending false messages. For example, control messages sent on behalf of another node (spoofing), or control messages containing incorrect or outdated routing information. The network can present a Byzantine behavior [8] [9], i.e. contradictory information sent from different parts of the network. The consequences of this attack are the degradation in network communications, isolated nodes and routing loops [10] [11]. Cache Poisoning and DoS (Denial of Service) are examples of incorrect traffic generation in routing schemes.

- Cache Poisoning: in the distance vector routing protocol, an example of incorrect traffic generation is that an attacker may announce a metric of 0 for all destinations, which will induce all nodes send their packets through this node. Then the node deletes all packets which will cause a significant loss of exchanged communications.
- DoS: an attacker can perform a denial of service in the network by saturating the wireless medium with broadcast messages, which will reduce the rate of transmission of nodes and prevent communications. An attacker can send invalid messages just to paralyze nodes, overload their CPU and consume their energy resource. In this case, the attack aims not to change the network topology, but rather to disrupt network functionality and communications.

2.1.2 Incorrect traffic routing

Information sent from a legitimate node can be corrupted by another node [12] [13]. Examples of this category are:

- Black hole attack: malicious nodes falsely claim a fresh route to the destination to absorb transmitted packets from source to that destination and drop them instead of forwarding.
- Green Hole: the attacker distributes a portion of the received messages and blocks the others. For example, it filters the data packets to be hidden and passes the control packets.
- Message tampering: an attacker can also modify messages before forwarding them. This is may be happen only if no mechanism is used to ensure the integrity of data packets.
- Replay attack: as the topology is dynamic, an attacker can produce replay attacks, using control messages already recorded and transferred to other nodes in order to modify the nodes routing tables with false information.
- Rushing attack: this attack can be launched against reactive protocols. In these protocols, nodes only rebroadcast the first request received for each route discovery and ignore others. When a route discovery is initiated, the attacker floods the network by request messages. If the attacker's messages arrive firstly, the attacker will be involved in the route discovery process [14].
- Wormhole Attack: two malicious nodes cooperate and falsify the number of hops by announcing a short cut between two imaginary parts of the network. In the Figure 1, the source S chooses to route the data packets by {S, M1, M2, D} instead of {S, A, B, C, D} because it is the shorter route but in reality, attackers use a longer route {S, M1, A, B, C, M2, D} since that the link between M1 and M2 is unreal.}

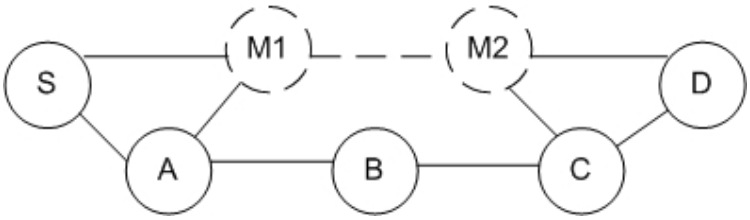

Figure 1. Example of Wormhole attack

According to the authors of [12] [15] [10] [6] [16], attacks are classified according to several criteria:

- internal or external attack: if the attacker compromises an existing node, the attack is considered as internal. Otherwise, it is an external attack.
- active or passive attack: the purpose of an active attack is to modify the protocol so that traffic packets passes through a node which is controlled by an attacker. A passive attack takes control over a corrupted node to eavesdrop the traffic. This does not jeopardize the functionality of the network, but affects the anonymity of the exchanged messages. This attack allows the attacker to analyse data packets that can be used later.
- single or distributed attack: In a single attack, a single entity is used. More sophisticated attacks, called distributed attacks, compromise several nodes and are generated from various sources. This kind of attack is more dangerous and difficult to detect.

2.2. Routing security in MANETs

The traditional routing protocols aim only to discover optimal routes. Some current works have introduced the concepts of security in these protocols without changing their basic principles by including authenticity and integrity of the exchanged messages. Some research works have targeted a specific protocol and present themselves as an extension of its original version, or they provide some countermeasures against attacks. In what follows, we summarize some relevant protocols which are classified into several categories according to the mechanism used.

2.2.1 Solutions based on asymmetric cryptography

The protocols using asymmetric cryptography need a trusted third party or so-called *TTC* which provides certificates to the participating nodes. ARAN and SAODV are examples of these protocols.

- ARAN: Authenticated Routing for Ad-Hoc Networks [17]. This protocol uses a reactive trusted party to generate certificates. Before joining the network, each node must obtain a certificate signed by the server. In ARAN, each node signs the discovery and replay packets before retransmitting. Intermediate nodes cannot reply with a route replay. Only the destination node has the right to respond. This provides an end-to-end authentication between the source and destination; however this leads to increase dramatically the latency especially for long routes.

- SAODV: Secure Ad hoc On-demand Distance Vector Routing [18]. It is a secured extension of AODV protocol. In this protocol, the non-mutable fields in AODV messages are signed by the private key of the sender while a hash function is used to protect the fields' integrity. The signature ensures the functions of authentication, integrity and non-repudiation. Despite its robustness, SAODV is vulnerable to the wormhole attack.

2.2.2 Solutions based on symmetric cryptography

This set of solutions is built on symmetric cryptography, hash functions, and hash chains.

- SRP: Secure Routing Protocol [18]. It was designed to provide trust routing information by securing the route discovery step. SRP requires private keys shared by the hosts. The destination checks the integrity and authenticity of routing messages using a hash function then broadcasts its reply by different routes. This later technique permits an additional protection against malicious nodes that attempt to alter *route replay* messages. The weakness of this protocol is at the route discovery: an adversary can produce *Route Error message* to invalidate routes that are still available.

- SEAD: Secure Efficient Ad hoc Distance vector routing protocol [19]. It is a proactive protocol developed for securing DSDV protocol. SEAD authenticates the sender and provides protection against the tampering of mutable fields (e.g., the number of hops, sequence number). By applying a hash function repeatedly on a random value, a chain of hash is obtained. Then, the elements of this chain are used by the nodes in the authentication procedure without a need for public key encryption. This avoids the costly cryptographic operations. To authenticate the source of an update, a shared secret key between each pair of node is required.

2.2.3 Solutions based on reputation

This solution addresses the selfish behavior problem which considerably disrupts the routing process. The main goal of a reputation system is to make decisions about the reliability of entities and improve trust within the network by encouraging the participation in routing. To make such decisions, a reputation system analyzes ancient interactions and exchanges between nodes. Each scheme discussed above has its own requirements and constraints to achieve the desired security. Protocols based on the cryptographic mechanism require key management. Protocols based on reputation include a new metric (reliability of the path) to select a route to a destination. Intermediate nodes are limited to route packets in some protocols while in others they are permitted to respond to the source if they know the path. While many theoretical studies have been proposed in the literature, the satisfaction of safety constraints inherent in ad hoc infrastructure still need more investigation.

3. PROPOSED SOLUTION: AD HOC SECURE ROUTING PROTOCOL (ASROP)

Our proposed Protocol ASRoP is inspired from SRP authentication algorithm [20]; this is due mainly to the effectiveness of the hash chains used in SRP since they reduce the costs of the traditional cryptographic mechanisms. We note that almost methods based on authentication via certificates are very expensive and may be not enough secured if a certificate was not issued by trusted third-party. Since ad hoc networks are very dynamic, the certificate-based solutions may be limited. It is important to note that a password in SRP is never transmitted during the messages exchange process, even encrypted. In this way, a hacker node cannot intercept the password by listening to the network; and this prevents problems of using passwords for authentication.

Our ASRoP solution includes two main steps: in the first one the nodes exchange information to negotiate the parameters which are required to establish a shared secret information between neighbors; this secret information is used as a password in the second step. In the second step, the nodes involved in the route discovery verify the identity of each node that provides information about the route. Note that in ASRoP, *HELLO* packets are sent at regular intervals to update the neighboring table which permits to any node to obtain a global view about its neighborhood.

3.1. Authentication scheme

As we stated previously, our proposal is based on SRP [20] which is a secure password-based authentication and key-exchange protocol; it is efficient for negotiating secure connections using a password provided to users, while eliminating the security issues typically associated with reusable passwords. This protocol also performs a secure key exchange in the process of authentication, allowing security layers (privacy protection and/or integrity) to be activated during the session. Key servers and certificate infrastructures are not required. The following steps, illustrated in Figure 2 explain the process of authentication *Client/Server* or two nodes in general (we included some modifications in the results verification phase).

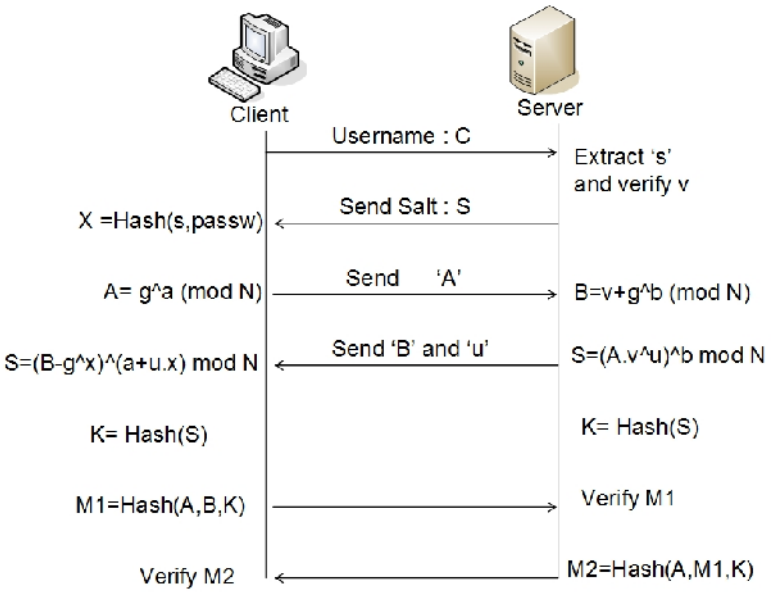

Figure 2. Secure remote password protocol authentication

1. The two entities choose two distinct numbers g and N. N is a prime number and g is a primitive root modulo N.
2. The client calculates $x=hash(s \parallel hash(UserName \parallel ":" \parallel Password))$ where s is a random string used as the user's salt. Salt is known by both user and server.
3. The client sends its username to the server.
4. The server checks the password entry, calculates a verifier v=g^x mod N.
5. The client generates a random number a which is a private key generated randomly and not publicly revealed, calculates A and sends A to the server.
6. The server generates its own random number b which is a private key generated randomly and not publicly revealed, calculates B and generates another random parameter u and sends it with B to client. u is random scrambling parameter obtained from B (the MSB 32 bits of hash(B)).
7. Both Client and server compute the same value S using the available values but with different operations.
8. If the password P of client entered in step 2 corresponds to that used in the calculation of v, the two S will match.

9. Both entities hash *S* to create a session key cryptographically strong.
10. The client sends *M1* to the server as proof that it has the right session key. The server computes *M1* and verifies that it corresponds to that sent by the client.
11. The server sends *M2* to the client as proof that it has the right session key. The client computes *M2* and verifies that it corresponds to that sent by the server.

In ASRoP, the authentication process is performed during the route discovery phase, and specifically when a destination node sends response message to a source node. During this step, each node involved in the creation of the route does not exploit any information from a node only if this later is authenticated. The authentication is ensured by the modified SRP protocol using the shared key obtained in the first step. Upon receiving the route request, the intermediate node has two possibilities: either it responds to the source if it is the destination or it has a valid route to reach the destination. In the first case, the intermediate node initiates an authentication process with the next hop. The authentication is performed hop by hop along the path.

3.2. Keys exchange

At this stage, all nodes exchange information to establish a secret key with their neighbors (at one hop) by applying the *Diffie-Hellman (DH)* algorithm. Each node sends a request for each neighbor in order to share a secret, and each neighbor responds to the request, using parameters generated according to DH algorithm. Figure 3 shows the step dealing with a secret sharing between nodes.

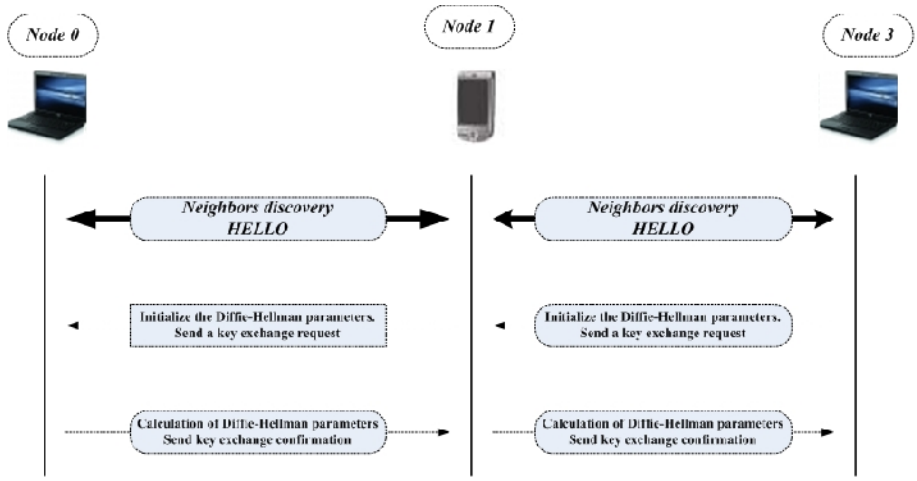

Figure 3. Exchange keys between nodes

Upon receiving a Hello message that reveals a neighbor, the node decides whether to reply or not, the decision is taken based on the identifier (ID) of the neighbor. Only the nodes having an ID greater than their neighbors can initiate a key exchange request (Figure 4). Following this step, each pair of nodes shares a secret which can only be known by these nodes; thus, all nodes share secret keys with their neighbors.

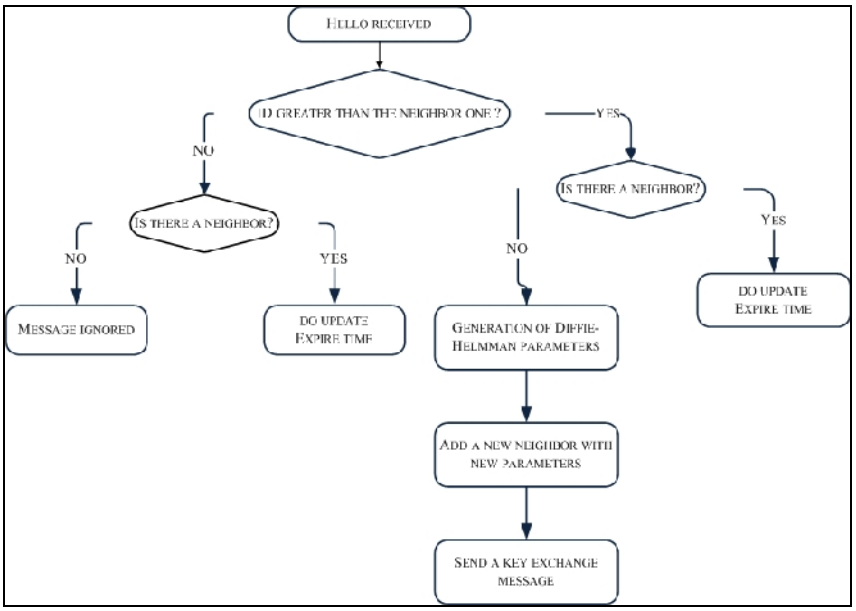

Figure 4. Decision policy of Hello packet reception

3.3. Format of messages in ASRoP

The design of our proposed ASRoP is based on AODV routing protocol, which is an efficient reactive routing scheme. To adapt AODV to a secure ad hoc network and to apply the authentication principle used by SRP, we added several changes and new parameters to SRP. Each node maintains a neighbor table that contains information (parameters used to calculate the secret) about neighboring nodes. In ASRoP protocol, we kept the same format of messages (*Hello, route request, route reply and route error*) used in AODV, and we added two other kinds of messages (*KeyExchange* and *Authentication*).

3.3.1 Format of KEYEXCHANGE packets

These packets (Figure 5) are used during the first step of ASRoP to share the secret key using the Diffie-Hellman algorithm; this secret key is used as a password during the second step. Each KEYEXCHANGE packet includes the following information:

- **IP@_D, @IP_S**: destination and source IP Addresses;
- **Prime**: a very large prime number;
- **Generator**: integer used in calculations;
- **Public Key**: the public key of a node calculated according to the Diffie-Hellman algorithm;
- **Confirmation**: indicates whether the packet is a request or a reply.

Figure 5. Exchanges key packets: KEYEXCHANGE

3.3.2 Authentication packet: AUTH

This packet (Figure 6) is used to exchange useful parameters to perform a mutual authentication between two nodes that share the same secret according to the principle of SRP. AUTH packet includes the following information:

- **IP@_D, @IP_S:** destination and source IP addresses;
- **Reply_Dest:** destination IP address of the reply packet route;
- **Type:** authentication packet type (*authentication request*, *authentication response*, *request for verification* or *authentication success*);
- **Parameters:** values used in the calculation and verification of authentication.

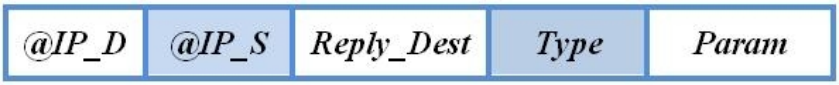

Figure 6. Format of AUTH packets

3.4. ASRoP analysis

In the following, we provide a security analysis of the proposed ASRoP by evaluating its robustness in the presence of attacks. The proposed protocol is efficient for negotiating secure connections using a password or a key, while eliminating some security issues typically associated with reusable passwords. ASRoP performs a secure key exchange during the authentication process, allowing security layers (privacy protection and/or integrity) to be activated during the session lifetime. Key servers and reliable certificate infrastructures are not required in our solution, and clients should not store or manage long-term keys. ASRoP offers both security and deployment advantages over existing challenge-response techniques, making it an ideal drop-in replacement where the authentication of a secure password is required [k1].

It is impossible to deduce the key from another legitimate node because it is the only one which knows its value, even if an attacker listens on the communication medium he cannot deduce the key since the latter is never transmitted over the channel (except in the first exchange which we assume as secure).The advantage of the proposed protocol lies in the fact that a node cannot participate in a process of route discovery only if he owns the rights. Hence, unauthenticated nodes cannot send control messages.

If an internal node tries to spoof the destination identity by responding to the source node, its message will inevitably be rejected. Indeed, the authentication process will not be realized. This ensures that the established route between two nodes is always valid and cannot be changed by an attacker.

In this section, we have explained in details our proposed protocol which ensures the routing security in MANETs to guaranty the communication of user's data despite the presence of intruders and attacks related to routing. However, our protocol is still not perfect; if a legitimate node refuses to cooperate (selfishness), the authentication is no longer sufficient and we need more advanced mechanisms such as reputation systems. We can say that the proposed ASRoP protocol is a first line of defense against any external intrusion.

3. SIMULATION AND PERFORMANCE EVALUATION

In the following, we conduct a simulation study using ns-2 to evaluate and compare the performance of our proposed protocol, i.e., ASRoP, with AODV scheme. Two scenarios will be illustrated in order to properly evaluate our protocol: in the first scenario, the velocity is set to 1 m/s which represents the velocity of walking man, whereas in the second one, the velocity is set up to 25 m/s which is dedicated for vehicular case. The performance evaluation involves the metrics which are often used in the evaluation of routing security protocols:

- *End to End Delay*: this parameter represents the average time for transmitting a data packet from source to destination. It introduces all the delays for the route establishment. This metric is very interesting in many applications (e.g. real-time voice traffic) requiring a critical delay.
- *Packet Delivery Ratio*: it is the rate of packets successfully delivered. This metric represents the percentage of packets delivered successfully to their destinations compared to the sum of data packets transmitted in the network.
- *Route Acquisition Delay*: it is the average time for discovering a route between a source and a destination.
- *Average Path Length*: it represents the average number of hops between a source and a destination; often used as a metric for choosing the optimal path (shortest path in terms of number of hops).
- *Dropped packets*: it is the number of data packets lost due to network congestion or packets collision.
- *Routing Load*: this parameter represents the quantity of control packets generated by the protocol to discover and maintain a route.

The simulations are done on *NS-2 version 2.34* in a *Linux* environment. The used models in the simulation are standard and have the following properties:

- **Antenna Model**

We used an omnidirectional antenna that broadcasts to 360° around it. With this model a node can communicate with all its neighbors in any direction, unlike the type of directional antenna that requires that the transmitter antenna is pointing in the direction of the receiving antenna. The radio range is fixed at 250 m, which is a realistic value considered by existing wireless cards.

- **Propagation model**

The propagation model informs us about how the signals will be attenuated according to distance. For example, the *free space model* considers the ideal case where there is only one propagation path between transmitter and receiver and it is in direct view, while the *Two-ray ground model* considers both the direct path and a reflection on the ground.

- **Traffic model**

Usually, a generated traffic in network has to consider several parameters. We set our parameters as follows: the size of a packet is equal to 512 bytes and the sending frequency is 4 packets per second; thus, the flow rate of each source is equal to 4*512*8 bit/sec = 16 kbits/sec. The number of connections is set to 5 to avoid overloading the network. Since the purpose of our simulations is to analyze the properties of the proposed solution, traffic sources generate a constant rate *CBR (constant bit rate).*

- **Mobility Model**

Varying the characteristics of mobility conveys a significant impact on routing performance. In our simulated network, mobile nodes move according to the RWP model (*Random Waypoint Model*). This model is widely used in research in mobile wireless networks. It provides scenarios where all mobile nodes move randomly during simulation.

4.1. Performance study

We have studied the behavior of the proposed protocol on a large scale by changing the number of nodes. All simulations are repeated 250 times and a confidence interval of 0.95 was considered. Two steps are considered to assess the performance of ASRoP: the first one investigates the impact of network density on ASRoP; while in the second step, we study the performance of ASRoP under various nodes velocity.

4.1.1 Scenario 1: variation of network density

Table 1. Simulation parameters in scenario 1

Parameters	Values
Antenna	OmniAntenna
Number of Nodes	10-100 nodes
Mobility	1 m/s
MAC layer type	IEEE 802.11
Radio propagation model	Two ray ground
Mobility model	Random way point
CBR traffic	4 packets/s
Packets size	512 bits
Pause time	10 sec
Network dimension	1000 * 1000
Transmission range	250 m
Simulation time	250 sec

4.1.1.1 End to end delay and route discovery time

Figure 7 shows an increasing trend in the average time from start to finish depending on the number of nodes. We can observe that the average time of ASRP protocol is significantly higher than that of AODV protocol. This is due to the time required by the ASRP operations used for authentication which makes the route discovery process slower than in AODV. However, this is not dramatic because it does not impact the protocol performance.

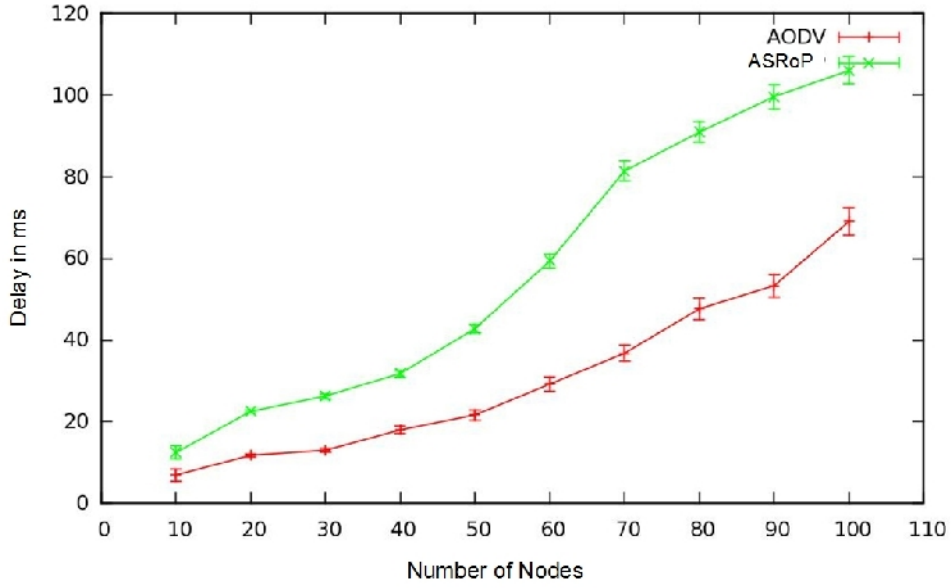

Figure 7. End to end delay

We notice the same trend in Figure 8 which illustrates the evolution of the route discovery time based on the number of nodes. The figure shows that the route discovery in ASRP requires more time than in AODV. In the case of 50 nodes, the route discovery time is 0.49 ms using AODV and 1.26 ms using ASRP. In the case of 100 nodes, the route discovery time is 3.19 ms using AODV and 4.56 ms using ASRP. However, this time is in milliseconds, we can say that ASRP allows route discovery in a reasonable time.

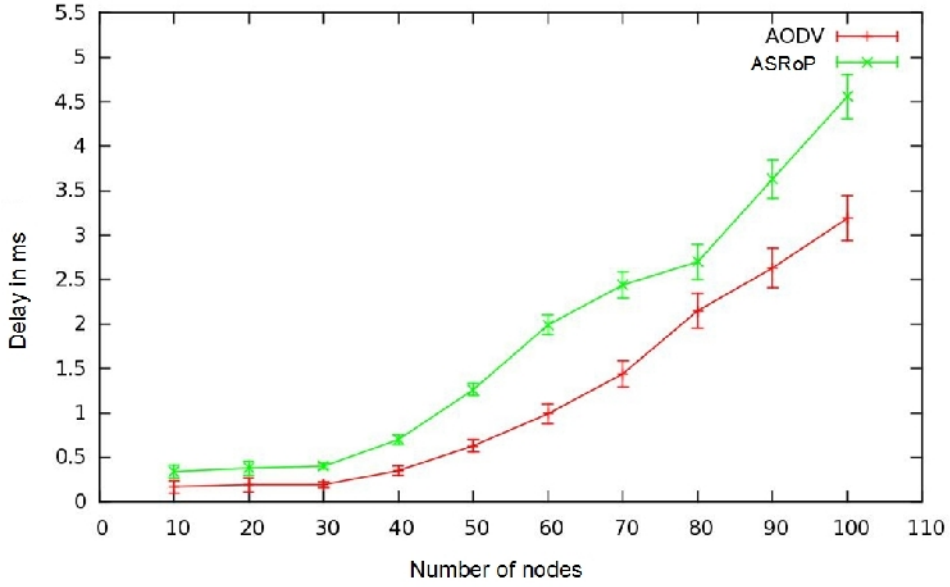

Figure 8. Route discovery time

4.1.1.2 Packets loss

By analyzing the Figures 9 and 10, we can say that the considered metrics (successful delivery rate and packets loss rate) do not make differences between the ASRP and AODV protocols. The two curves, in both figures, have the same trend. The rate of successfully delivered packets varies between 0.97 and 0.99. This high rate implies that the delivery of data packets is achieved successfully, thus the performance was not degraded even with the presence of security extensions.

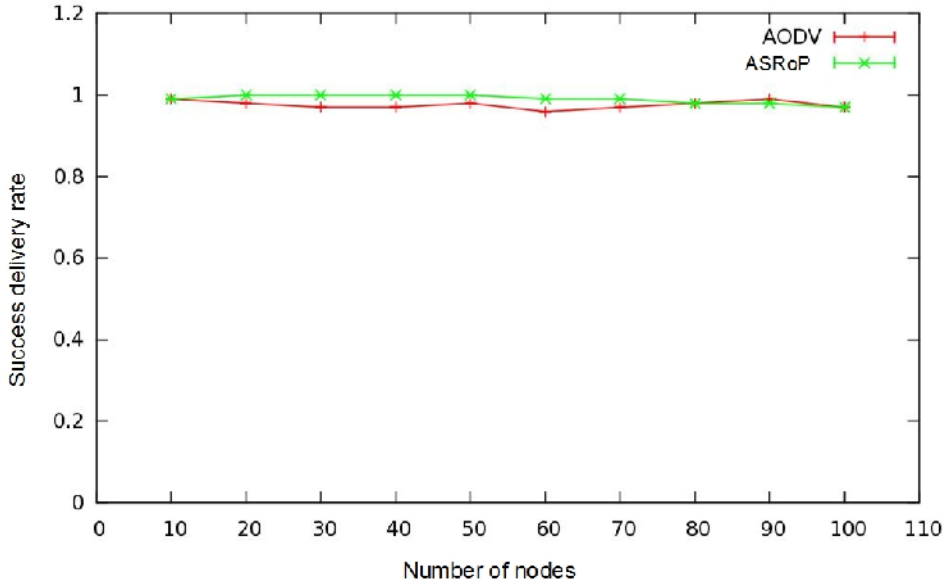

Figure 9. Successful delivery rate

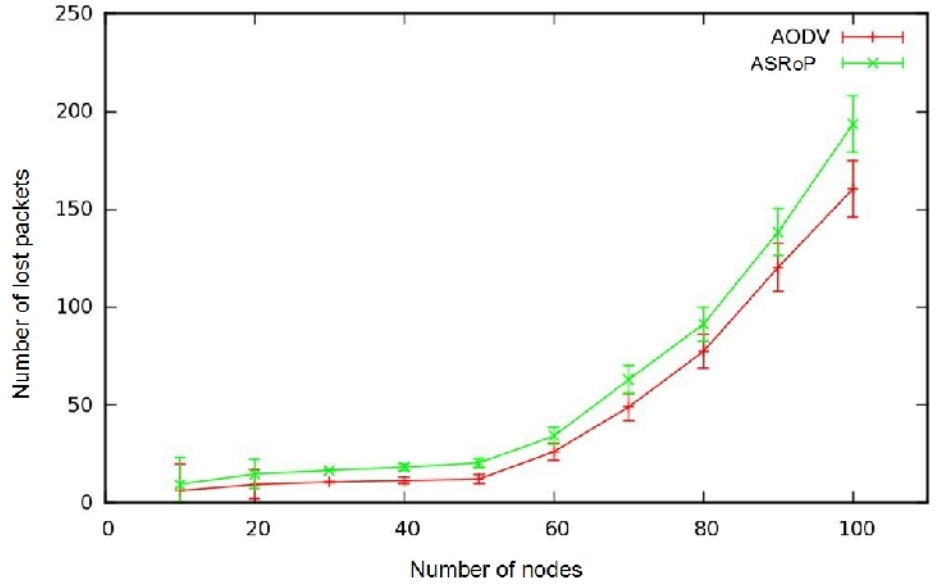

Figure 10. Packet Loss rate

We remark also that small performance degradation occurs by increasing the number of nodes: the scaling leads to an increase of exchanged messages, which causes an increase in the number of lost packets. This is often due to collisions between packets.

4.1.1.3 Number of hops by route and routing overhead

Traditionally, the shortest path in terms of number of hops is considered as the best path to route data. The AODV protocol uses this metric to choose its routes. We assumed that the first path obtained is the best one. This means that updating the routing table is due to the arrival of the first response (the fastest one). In Figure 11, we notice that the curves in the two protocols are very close. The obtained average number of hops proving that the length of routes established by ASRP is not necessarily longer than that of AODV.

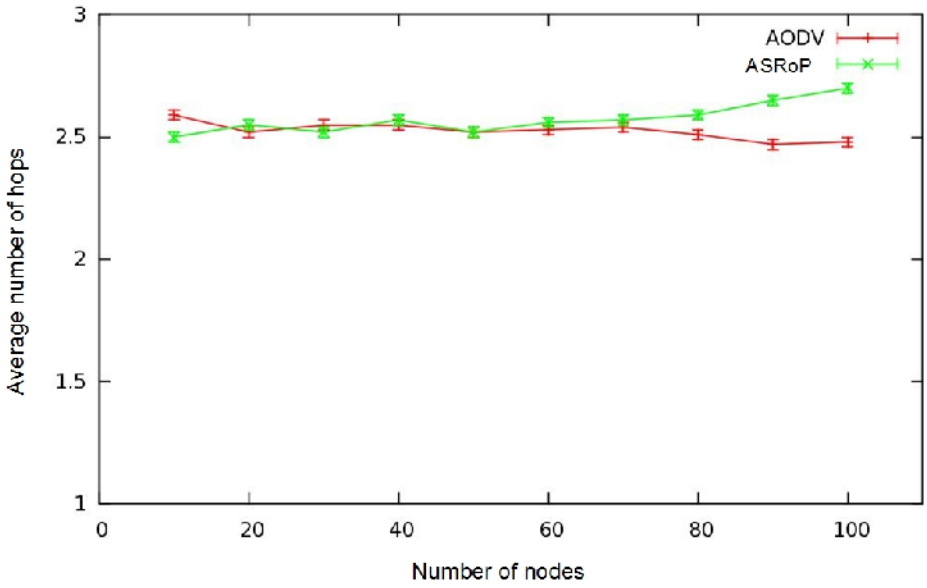

Figure 11. Number of hops/route

Figure 12 shows the number of control packets in function of the number of nodes. This parameter let us observe the cost of a protocol in terms of resource consumption and enable to understand the resistance of the protocol in case of congestion. In both protocols the variations of the number of nodes has a direct influence on the number of exchanged packets; this is due to the diffusion of various control messages. However, the number of exchanged control packets is greater in ASRP that in AODV. This is mainly due to the new extension realized in ASRP, which requires in the first step to share the keys and in the second one to run the authentication process.

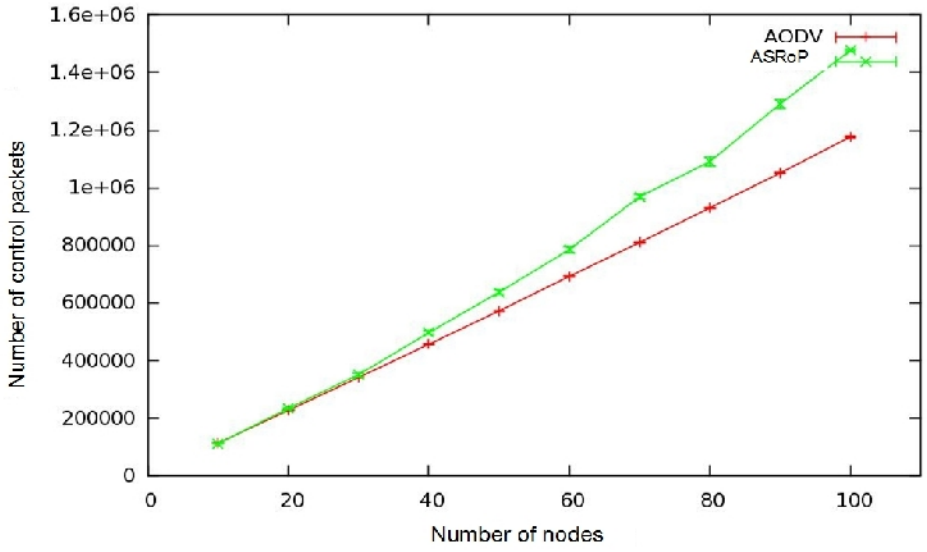

Figure 12. Number of control packets

4.1.2 Scenario 2: variation of nodes velocity

In this section, we study the impact of nodes velocity on the ASRoP. The simulation parameters are listed in the table 2.

Table 2. Simulation parameters in scenario 2

Parameters	Values
Antenna	OmniAntenna
Number of Nodes	25 nodes
Mobility	1-25 m/s
MAC layer type	IEEE 802.11
Radio propagation model	Two ray ground
Mobility model	Random way point
CBR traffic	4 packets/s
Packets size	512 bits
Pause time	10 sec
Network dimension	1000 * 1000
Transmission range	250 m
Simulation time	250 sec

4.1.2.1 End to end delay and route discovery time

Figure 13 shows an increasing trend in the average end-to-end delay depending on the mobility of nodes. We can observe that the average delay in ASRoP is significantly higher than that in AODV. This is due to the time required by the cryptographic procedures and messages exchanged making the route discovery process slow.

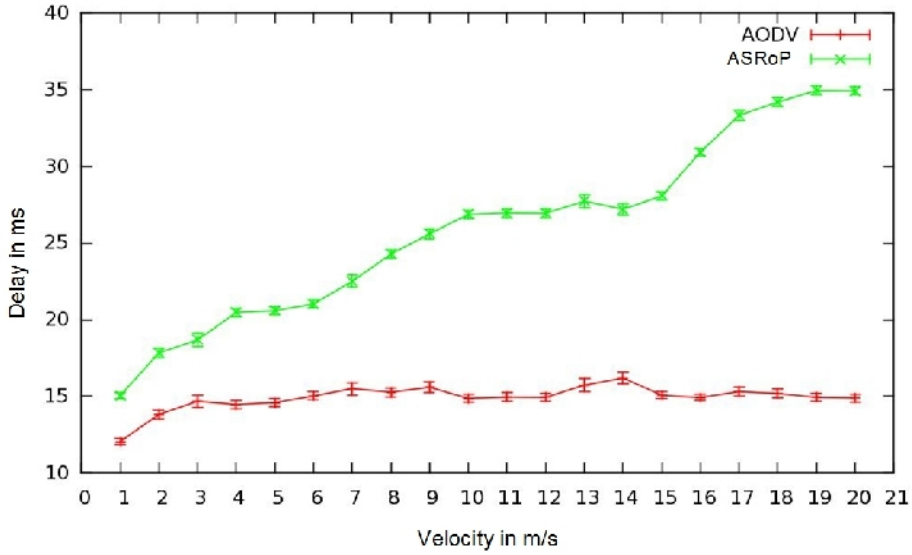

Figure 13. End to end delay

We observe the same behavior in Figure 14 which represents the evolution of the route discovery time in function of nodes mobility. In this figure, we can observe that the route acquisition in ASRoP requires more time than in AODV. This figure illustrates the strong impact of mobility on ASRoP protocol: having high mobility leads to more control messages, since there is less connectivity (nodes can get away from each others). However, this time as it is in milliseconds, we can say that ASRoP allows getting a secure route in a reasonable time.

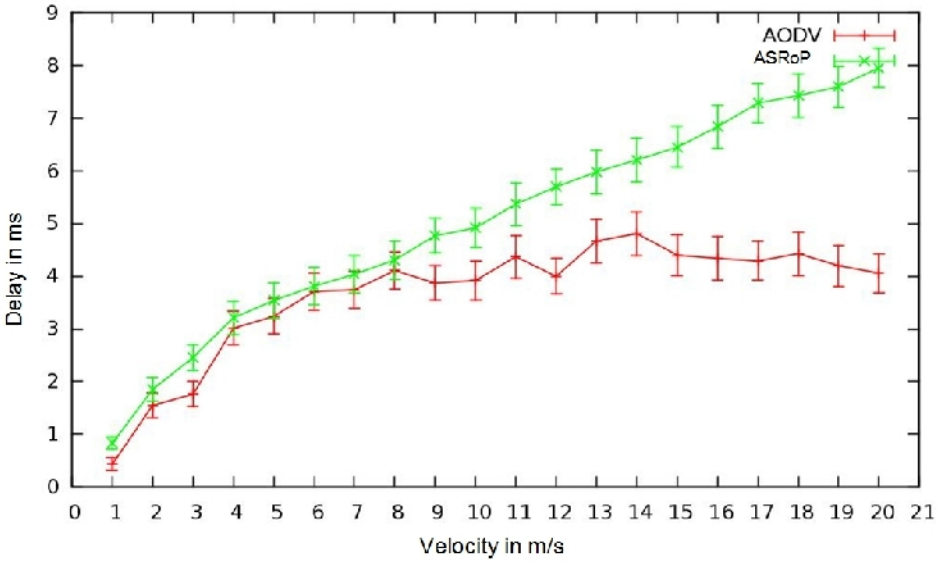

Figure 14. Route discovery time

4.1.2.2 Packets loss

By observing the two graphs in 15 and 16, we can say that these two metrics do not illustrate a difference between the two protocols; the two curves have almost the same trend. The rate of successfully delivered packets varies between 0.96 and 0.99. This high rate implies that the delivery of data packets is very successful, so the performance was not degraded even with the presence of security extensions.

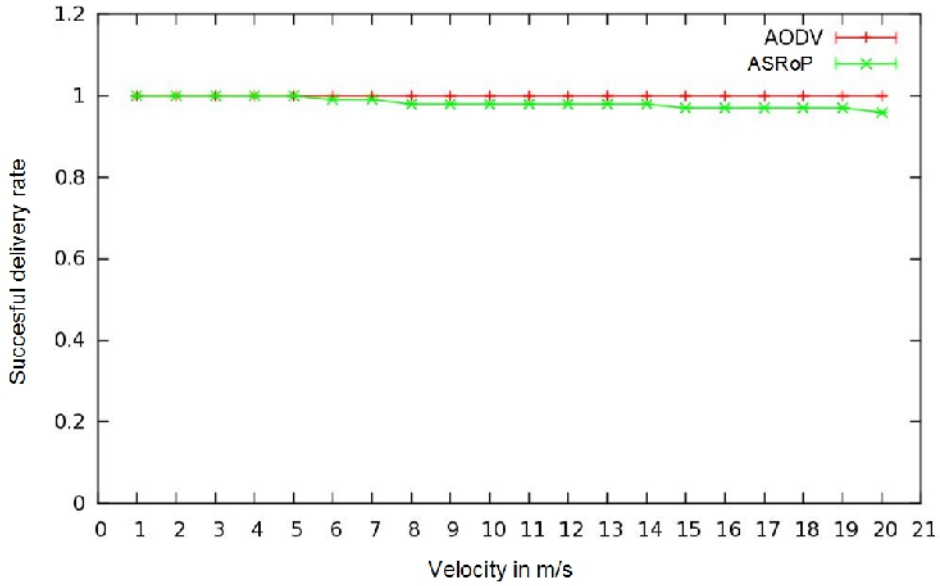

Figure 15. Successful delivery rate

We observe that small performance degradation occurs when increasing the mobility of nodes: the node's mobility leads to augment the frequency of broken links, thereby to increase the number of lost packets. This loss is illustrated in Figure 16 but it is controlled by the routing algorithm that tries to adapt to mobility through a local repair of the broken paths.

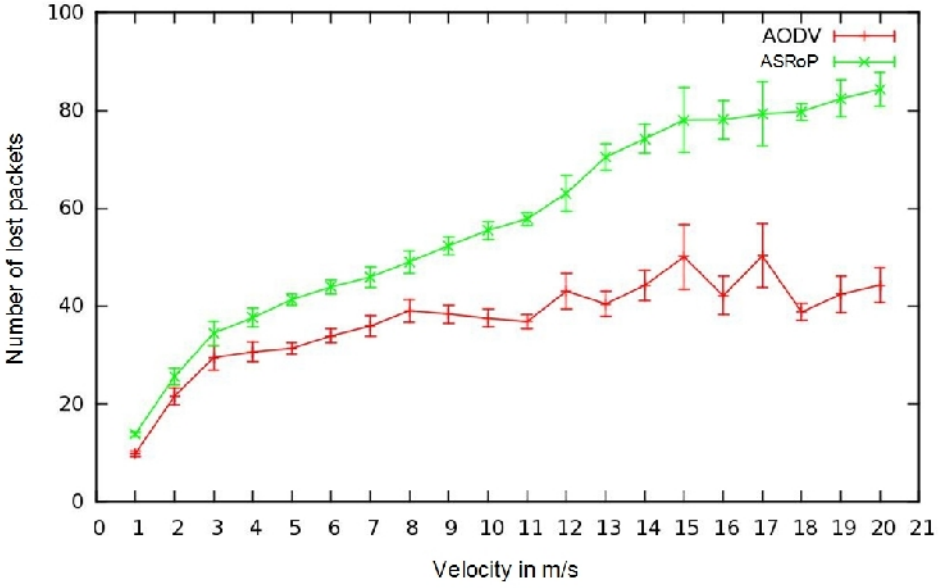

Figure 16. Packets loss rate

4.1.2.3 Number of hops by route and routing overhead

In Figure 17, we notice that the curves of the two protocols are very close. The obtained average number of hops proves that the length of routes established by ASRoP is not necessarily longer than that of AODV.

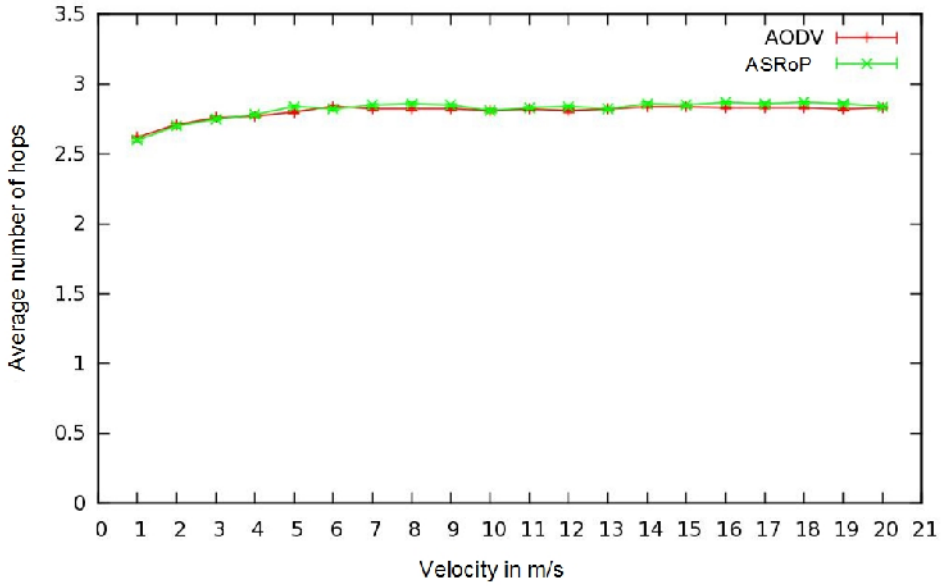

Figure 17. Number of hops/route

In Figure 18, in both protocols the mobility has a direct influence on the number of exchanged packets. This is mainly due to the diffusion of various control messages; however, their number is greater in ASRoP than in AODV. This is due to the new extension which requires a first step to share the keys and a second to run the authentication process. The number of control messages decreases when the mobility increases, as we can observe by comparing the two Figures 18 and 12.

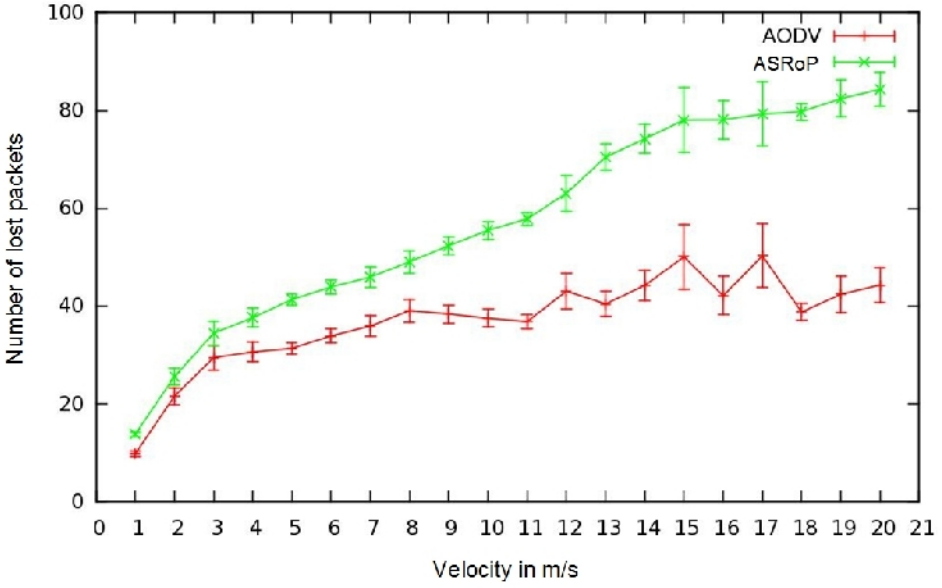

Figure 18. Number of control packets

Through these results, we can clearly see the impact of mobility and variation of the number of nodes on the evaluated metrics. The simulations have shown that compared to AODV, our security solution consumes slightly more resources and that the delays are longer is ASRoP than in AODV. Indeed, in each hop, the exchange of messages, which ensures authentication increases the security cost of ASRoP.

5. CONCLUSIONS AND PERSPECTIVES

In this paper, we have analyzed some security attacks a MANET may face, described some ad hoc routing security solutions, and presented a new secure routing protocol named ASRoP. The idea that we consider most appropriate to ensure secure communications between entities in an ad hoc network is the establishment of a cryptographic mechanism to ensure authentication of messages. The proposed ASRoP is based on Diffie-Hellman algorithm and SRP authentication protocol that we have exploited to negotiate a secure session using a user password, while eliminating the security concerns often associated with reusable passwords. The performance evaluations have proved that ASRoP offers good results; specifically in terms of the rate of successful delivery packets and end-to-end delay of packets transmission. The ASRoP results are almost the same as for AODV protocol, with the advantage of securing communications in ASRoP. However, a comparison with other secure AODV protocols (e.g. [21] [9]) would be very useful in order to demonstrate efficiently the robustness of ASRoP. In a future work, we plan to add a reputation mechanism for ASRoP and evaluate the proposed ASRoP with other parameters. In addition, simulating realistic attack scenarios would be very interesting to test the robustness of ASRoP in practical cases.

REFERENCES

[1] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir R. Das. Ad hoc on-demand distance vector (aodv) routing. RFC Experimental 3561,Internet Engineering Task Force, July 2003.

[2] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. In Thomasz Imielinski and Hank Korth, editors, Mobile Computing, volume 353, chapter 5, pages 153_181. Kluwer Academic Publishers, 1996.

[3] Ha Duyen Trung, Watit Benjapolakul, and Phan Minh Duc. Performance evaluation and comparison of di_erent ad hoc routing protocols. Comput. Commun., 30:2478_2496, September 2007.

[4] L. Abusalah, A. Khokhar, and M. Guizani. A survey of secure mobile ad hoc routing protocols. Communications Surveys Tutorials, IEEE, 10(4):78_93, 2008.

[5] P. Sakarindr and N. Ansari. Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks. Wireless Communications, IEEE, 14(5):8 _20, october 2007.

[6] Dongbin Wang, Mingzeng Hu, and Hui Zhi. A survey of secure routing in ad hoc networks. In Proceedings of the 2008 The Ninth International Conference on Web-Age Information Management, WAIM '08, pages 482_486, Washington, DC, USA, 2008. IEEE Computer Society.

[7] G Xu, C Borcea, and L Iftode. A policy enforcing mechanism for trusted ad hoc networks. Dependable and Secure Computing, IEEE Transactions on, 2010.

[8] K. Driscoll, B. Hall, M. Paulitsch, P. Zumsteg, and H. Sivencrona. The real byzantine generals. In Digital Avionics Systems Conference, 2004. DASC 04. The 23rd, volume 2, pages 6.D.4 _ 61_11 Vol.2, 2004.

[9] Ming Yu, Mengchu Zhou, and Wei Su. A secure routing protocol against byzantine attacks for manets in adversarial environments. Vehicular Technology, IEEE Transactions on, 58(1):449_460, january 2009.

[10] Hakima Chaouchi and Maryline Laurent-Maknavicius. La sécurité dans les réseaux sans fil et mobiles, Tome 2, Technologies du marché. April 2007.

[11] M. Krasnovsky and V. Wieser. A performance of wireless ad-hoc network routing protocol. In Radioelektronika, 2007. 17th International Conference, pages 1 _3, 2007.

[12] Hu. Yih-Chun and A. Perrig. A survey of secure wireless ad hoc routing. Security Privacy, IEEE, 2(3):28 _39, 2004.

[13] Sridhar Radhakrishnan, Gopal Racherla, and David Furuno. Mobile ad hoc networks: principles and practices, pages 381_405. CRC Press, Inc., Boca Raton, FL, USA, 2003.

[14] L. Tamilselvan and V. Sankaranarayanan. Solution to prevent rushing attack in wireless mobile ad hoc networks. In Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium on, pages 42 _47, 2006.

[15] Ashish Raniwala, Ashish Raniwala, and Ashish Raniwala. Architecture and protocols for a high-performance, secure ieee 802.11-based wireless mesh network, 2009.

[16] Youngho Park, Won-Young Lee, and Kyung-Hyune Rhee. Authenticated on-demand ad hoc routing protocol without pre-shared key distribution. In Proceedings of the 2007 ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security, pages 41_46, Washington, DC, USA, 2007. IEEE Computer Society.

[17] K. Sanzgiri, D. LaFlamme, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. Authenticated routing for ad hoc networks. Selected Areas in Communications, IEEE Journal on, 23(3):598 _ 610, 2005.

[18] P. Papadimitratos and Z.J. Haas. Secure link state routing for mobile ad hoc networks. In Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, pages 379 _ 383, 2003.

[19] Yih-Chun Hu, D.B. Johnson, and A. Perrig. Sead: secure e_cient distance vector routing for mobile wireless ad hoc networks. In Mobile Computing Systems and Applications, 2002. Proceedings Fourth IEEE Workshop on, 2002.

[20] ThomasWu. The secure remote password protocol. In In Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, pages 97_111, 1998.

[21] D. Cerri and A. Ghioni. Securing aodv: the a-saodv secure routing prototype. Communications Magazine, IEEE, 46(2):120 _ 125, february 2008.

Authors

Dr. Rida KHATOUN received the M. Sc in Computer Engineering and the Ph.D from the Université de Technologie de Troyes in France in 2004 and 2008. He is currently an associate professor at the University of Technology in Troyes, a member of the Institute Charles Delaunay (ICD). His research interests include DDoS attacks detection and defense, intrusion detection system, wireless networks security and computer security infrastructure.

Dr. Lyes Khoukhi is an associate professor at the University of Technology of Troyes (France), since 2009. In 2008, he was researcher at the Computer Sciences department of the University of Montreal (Canada). He received Ph.D degree in Electrical and Computer Engineering from the University of Sherbrooke (Canada) in 2007, and M.Sc degree in Computer Engineering from University of Versailles (France) in 2002. His research interests include wireless communications, mobile ad hoc networking, multimedia and quality of service, and intelligent systems.

Ahmed Nabet received his MS degree in computer networks from the University of Pierre and Marie Curie (Paris 6) and his engineering degree in telecommunications from the Bejaia University in 2009. His research interests include computer security networks, security infrastructure, and mobile ad hoc networks.

Professor Dominique GAITI received the Ph.D. and the "Habilitation à diriger des recherches" degrees in Computer Science from the University of Paris VI and Paris IX on 1991 and 1995 respectively. She is currently a professor at the University of Technology in Troyes (France), a member of the Institute Charles Delaunay (ICD). She is the leader of the team "autonomic networking" in this institute. She was a research scientist at the University of Columbia (New York-USA), 1992-1994 and a researcher at the University of Paris 6, member of the LIP6 laboratory (Paris - France), 1996-1997. She is the chairman of the IFIP WG 6.7 on "smart networks". Her research interests include the smart networks, the intelligence in networks, and the control and management (through intelligent agents) in all types of networks. She is the author of one book and has edited several proceedings.