Specification of the Security model based on the non reputation and the confidence in the Mobile Ad Hoc networks

Souleymane OUMTANAGA, Michel BABRI, Aby Affoué Thérèse

LARIT, 08 BP 475 Abidjan 08, Côte d'Ivoire

Abstract:
This paper presents a model of communication security in the Mobile Ad Hoc networks (MANETS) after a comprehensive analysis of the existing security mechanisms. Our approach will consist in assigning a hierarchical structure to the protocol COSR.

Key words:
MANETS, hierarchical structure, COSR, DSR.

1. Introduction

The Mobile Ad Hoc networks work with no basic facilities previously constructed .Given their high degree of flexibility they allow a quick connection of a large number of mobile nodes .For any communication with other nodes, each *one must* rely on intermediate ones. This fact exposes this kind of networks to attacks compared to wireless networks with facilities and the ones called wired networks. In such networks, the developed security protocols can therefore not be directly applied to the MANETs. the study and the establishment of the security mechanisms in the Ad Hoc networks remains a real challenge given : - the lack of a central authority , -the partition of the radio technology IEEE 802.11 channel –the control of the resources , - the physical exposure .
The routing protocol such as those based on the routing board DSDV [1] and the ones which govern the demand DSR [2]have been subject of many works .Later the secured protocols have been inserted to cope with the behavior of mischievous nodes like Ariadne [3],CONFIDENT [4] and more recently COSR [5].
In this paper, we suggest a model of communication security in the Mobile Ad Hoc networks. Our approach consists in solving the non cooperation problem of the nodes in one hand, and in assuring a confidence connection between the nodes on the other hand, thanks to a logical partition of the network in many groups and the establishment of another local confidence node in each group .This other confidence represents the head and plays the role of a certification authority of the group. Section 2 studies the revealed exposures and attacks of the network 802.11 structure. Section 3 tackles the suggested model. It also deals with a comparative survey with a few existing security mechanisms. We end with a conclusion followed by some coming research prospects.

2. Main attacks against Manets and especially those against DSR

Given their specific characteristics MANETS are subject to many attacks among which we have: spoofing, sinkhole, wormhole, Sybil, rushing, flooding, and non- cooperation attacks.

2-1 The ones blocked by the COSR.

Protocol COSR enables to block any attacks an endangered node tries to attract to it; all is neighbor data (sinkhole); the attacks against protocol DSR which enables a mischievous node to affect the route demand messages (rushing).

2.2 Limit of the COSR

Protocol COSR is ineffective face to fraudulent attacks such as spoofing attack, and Sybil attack. In the same way, it should be clear that COSR partly manages flooding and non-cooperation attacks since the reputation values and the controlled messages are uncertified.

3. The suggested model

Security models are numerous in literature [4], [13]. They can be divided into four groups: - confidence and key management models [6],[8], - interference detection systems [9], - secured routing protocols [10], [12], – cooperation models [4],[5], [13].
Confidence is a key element for any solution to the security problem in the Ad Hoc networks. Our service is based on the nodes reputation and on another confidence which allows the legal nodes to authenticate themselves each other .this model aims for considering the maximum of security services .In addition, its structure takes into account a cryptography module in the reputation based solutions. Figure 1 is an illustration.

3.1 The architecture

The architecture of the model (figure 13) encompasses five elements: the monitor, the statistic element, the reputation model, the protocol reputation, and the routing reputation.

3.1.1 The monitor

Its role is to monitor the neighbor nodes with a weak reputation or instance for two nodes x and y ,with NR (i) as the reputation of the node (i), then node (x) can monitor node (y).

Manuscript received August 5, 2011
Manuscript revised August 20, 2011

This element has three modules: the neighbor control, the data relay control, and the capability of forwarding control (Co F). The neighbor control demands that the MAC layer works in a promiscuous mode. The data relay control module checks if the next break has really transmitted the packet .As for the Capability of Forwarding (CoF) control it takes responsibility for collecting the information on the capability of forwarding of the physical and MAC layers of a node. These information mainly concern the level of congestion of the node, its residual energy level, its mobility term, and its power.

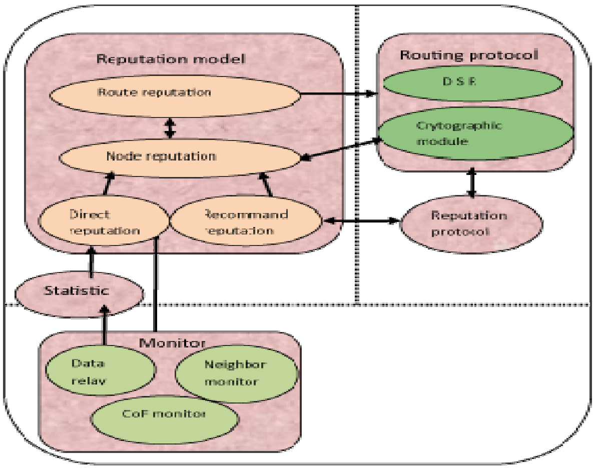


Figure 1: Architecture of the suggested model

3.1.2 The statistic component

It comprises one single module: the statistic module. It values the direct reputation of the nodes by establishing the link between the received messages and the really transmitted messages.

3.1.3 The reputation model

As for the reputation model, it uses the information of the monitor and the statistic component to determine the reputation of the node and insert a route reputation. It comprises four modules: the module in charge of evaluating the direct reputation, the one in charge of evaluating the recommendation reputation, the module which calculates the reputation of the nodes and the evaluator of the route reputation.

3.1.4 The reputation protocol

It permits to combine information from the reputation model and the routing protocol.

3.1.5 The routing protocol

It is composed of the traditional DSR protocol and a cryptographic module. This protocol uses the reputation of the nodes and the route reputation in order to choose the best way. The cryptographic module of this component ensures the authentification of the entities and the certification of the reputation information. It also ensures a secured exchange among the network‘s entities.

3.2 Working of the protocol.

In this sub-section we will define the principle of the suggested model and we will describe the various statuses of the nodes in the network. The route discovery and the route collection mechanism will also be presented.

3.2.1 Principle

To reach the set purposes, the following specifications will be required:

- Divide the network in many different groups (clusters) using not only the reputation and the mobility of the nodes, but also the number of neighbor nodes of good reputation as a metric for electing the head of the group (or cluster head).
- Insert a dynamic public key infrastructure (PKI) within each group. The Certification Authority (CA) is the head of the group and the Registration Authorities (RA) are the akin nodes at one break to the CA with a reputation value which is superior or equal to 0.9.These nodes RA represent a protection barrier for the CA [14].
- Use the cryptography based on the elliptic curve to secure confidential exchanges of the group and the inter-group.

After the sharing of the network, each node is allocated a status according to some criteria we will define later.
The suggested security model uses the reputation as a confidence metric. Thus according to the degree of confidence (value in interval [o.1] a given node can provide the following functions:
CA (Certification Authority), RA (Registration Authority),GN (Gateway node),MN (member Node) or VN (Visitor Node).

Status	value of reputation	Function and characteristics
CA	≥ 0,9	CH : - issues the certificates, - calculates the reputations, - manages the list of members
		Direct neighbor of CA : - filters requests of certificate, - supervises the members,

RA	≥ 0,9	- rapports to CA
NP	≥ 07	Gateway node belongs a least to 2 clusters : it ensures inter group communications
NM	≥ 0,5	Member node locates at most than k-hop, where k is the size of the group
NV	< 0,5	Visitor node at k-hop of CA

Table 1: different statuses

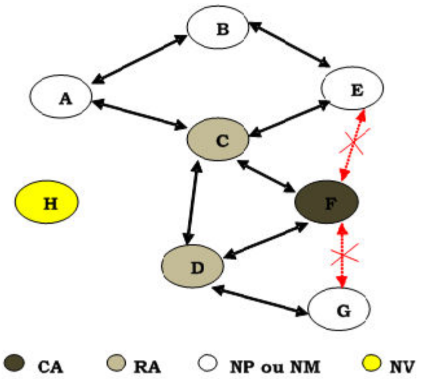


Figure 2 addition of a node as a member of a group.

On figure 2, nodes A and G belong to the same group .Here, node H wants to join the group .If this visitor node is known by a gateway node or a RA (for instance node A), the latter recommends it to the group .As a result, this visitor automatically becomes member of the group and can benefit from favors open to the network members. On the other hand, if the visitor node is unknown from GN and RA entities of the group, it will begin with a reputation value equal to 0.1 and should show its total cooperation before being member of the group.
The bidirectional link between node F and G , the one between F and E are interrupted because only RA are authorized to communicate directly with the node CA of the group .
These communications between the different nodes are based on mechanisms called route discovery and route collection mechanism we are going to describe bellow.

3.2.2 Implementation of the discovery and the route support.

Like DSR on which it is based, the suggested model is made up of the route discovery (RREQ) and the route support (RREP) stages .An illustration is given on figure 3. Node A having no way toward F initiates a request composed of its reputation value and its certificate.

Any intermediate node receiving this packet conducts the following actions:
Stage 1: Check of the reputation: first it checks if the reputation value of A complies with the one published by CA and if this is superior or equal to 0.5.
Stage 2: Validation of the certificate: this intermediate node checks the validity of the certificate (the public key of CA being known by all the members of the group). This packet is deleted if the certificate is invalid.
Stage 3 : real setting of the route : in case the certificate is valid , if it has a route toward the destination ,it replies by a packet RREP containing the list of the nodes on that route ,its certificates and its reputation value .If no route to the destination is registered in its mask ,then it removes the certificate from the previous node ,adds its address to the list ,inserts its reputation value and its certificate and retransfers the packet to its direct akin .
As soon as the originator node A has received all the packets RREP, it determines the reputation of each of the routes; this one is the product of the reputation values of the nodes belonging to this route.

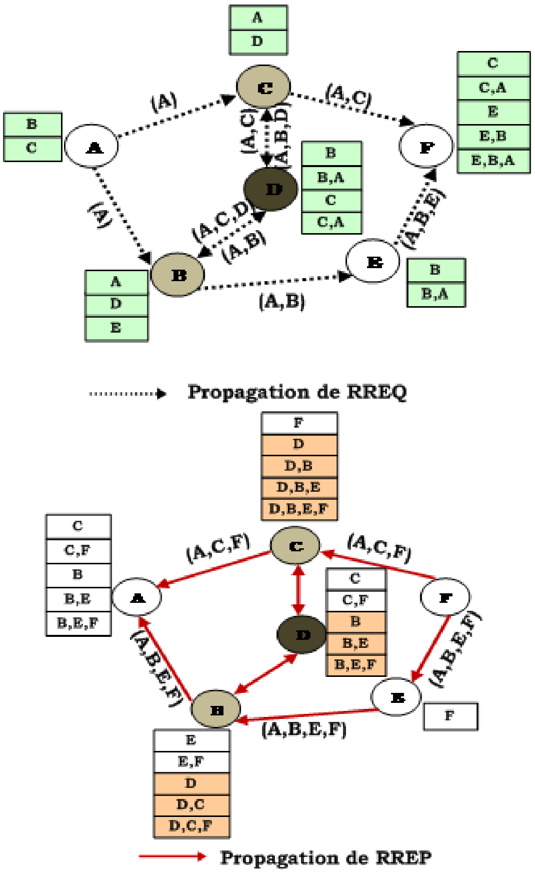


Figure 3: Route REQuest (RREQ) and Route REPly(RRRP)

The best route is the one with a higher reputation value .As the reputation value belongs to the interval [0.1], our mechanism by default considers the number of breaks. Thus as long a ways is, as smaller is its reputation value. However, a high route reputation with a malicious node will be dropped in favor of a route with a lesser reputation but more reliable. More, the data confidentiality is provided by the sharing of a secrete key based on elliptic curves. Algorithm SAE presents the mechanism described bellow.

To carry out the maintenance of its group each CA temporally diffuses the list of the group members, as well as the associated reputations and the list of the dismissed certificates .As stable the cluster is, higher is the diffusion time. In lack of any packet coming from its CA for a defined time, a node must redefine its status thanks to Algorithm SEA.

In addition, if the node (for instance A and F) wants to exchange confidential information, the sharing of a secrete key by using the cryptography based on the elliptic curves for their exchanges will be done as follows:

Stage 1: Choice of the elliptic curve point: the nodes A and F publicly agree on the elliptic curve and on one point P (x, y) on this curve as:

y^2 mod p = X^3+ ax + b) mod p

a and b € R / $4a^3$+ ax +27 b^2) ≠ 0

Stage 2: exchange of secrete numbers: nodes A and F secretly chose respectively an integer number d_a and d_f they exchange through a secured channel. This exchange relies on public keys obtained during a route research previously described.

Stage 3: Determination of the secrete key: nodes A and F calculates the common secrete key determined by

d_A (d_F P) = (d_f (dAP)= P

which is one point of the elliptic curve .

3.2.3 Secured Election Algorithm (S E A) of cluster head.

This algorithm divides the network in different groups (cluster) with one head per group (cluster head). The basic is that to be candidate to the cluster head status, a confidence node must have at least one confidence akin, and have no cluster in its proximity at k breaks.

More, to improve its results, we define a stability metric marked Relative mobility (Rm). It deals with the number of packets RERR (Route ERRor) generated by a node [15] . For instance if Rm (x) < Rm (y) then x is less mobile compared to y.

The election message format is the following:

Id	Id	Val of reputat.	Nb of conf. neighbor	Relat. mobility .	Nb hops to 1 candidate	Sequence number	signature

Table 2 : format of an election message

The algorithm SEA we suggest divides the network‘s nodes in various groups (cluster) with one head per group (cluster head). A confidence node decides to be candidate for the cluster head status when there is at least one confidence akin node and that it detects no cluster in its proximity of a k break.

Therefore, the suggested algorithm takes into account the following criteria:

- Only one cluster head per cluster.
- Any node with a reputation value superior or equal to 0.9 can be a cluster head (CA) ;
- The nodes located at a break from the cluster head with a reputation value superior or equal to 0.9 are RA ;
- The nodes of a group are in maximum at k breaks from the cluster head ;
- The gateway nodes are nodes with a reputation value superior or equal to 0.7 and belonging to at least two clusters ;
- The member nodes are the ones located to k breaks of the cluster head with a reputation value superior or equal to 0.5 :
- All the other nodes located in maximum to k breaks of the cluster head with a reputation value inferior to 0.5 will be visitor nodes.

In order to improve the results of this algorithm, we define the relative mobility between the two akin nodes as stability metric. Most of these mobility metrics are calculated according to the “hello” messages periodically emitted in the routing protocols like DSDV and OLSR. On the other hand , protocol DSR no longer insert any mechanism of a periodic exchange .The management of the control message can be used to assess the relative mobility (Rm) without causing additional traffics .The number of packets RERR (Route ERRor) generated by a node will be considered as a mobility metric [15].

For instance, if Rm (x) < Rm (y) then x is less mobile compared to y.

The following notations are used in the algorithm:

Id : Identity of a node ;

cl-id(id) : cluster identity of the node i ;

R_m (i) : the relative mobility of the node i ;

NR (i) : reputation of the node i ;

NC (i) : number of the confidence nodes akin to i ;

NS (i ,j) : number of breaks from the node i to j ;

Status (i) :status of node i , Status (i) € { CA, RA, NP, NM, NV } ;

K : size of the group .

```
Algorithme-1 CA election: when a confidence node v receive an election packet;

begin
 if NR(u) < 0,9  then drop the packet ;
  else  if  NS (u,v) > K then drop the packet ;
          else
              if  ( $R_m(v)$ >= $R_m(u)$ )  and  ( NC(u) > NC(v) ) then
                          begin
                            statut(u) = CA ;
                             broadcast statute of u  //     TTL=k
                            if  NS(u,v) = 1 then  Statut(v) = RA ;
                              else  Statut(v) = NM ;
                            fi
                          end
               else
                   if  ( $R_m(u)$ > $R_m(v)$ ) or  (NC(v) > NC(u) )
                          then  node  v  is  still  candidat  to  CA
                          status ;
                     else   execute  Lowest-ID ;
                   fi
               fi
          fi
```

Maintenance of the clusters
Maintenance of clusters

Each CA periodically diffuses the list of the group members, the combined reputations, and the list of dismissed certificates to ensure the maintenance of its group. The diffusion period increases if the cluster mobility decreases or reduces the opposite case.
Therefore, when a node doesn't receive a packet from its CA for a defined time (the double of the CA diffusion period), it runs the algorithm-2 bellow to define its status.

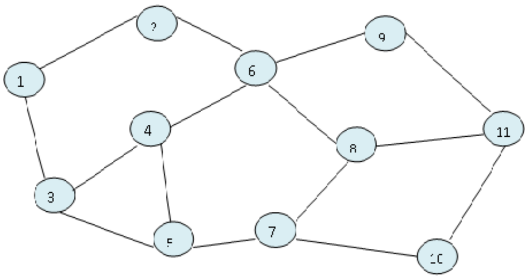
The robustness of algorithm SEA we suggest depends on the number of confidence nodes (node with a reputation value superior or equal to 0.9) existing in the network. Therefore, it is essential to adjust the group size to the number of confidence nodes for a better protection of CA. Thus, the number of clusters depends on the number of confidence nodes. We suppose that each node has on average half of its akin nodes as confidence nodes during the initialization stage.
Stage 1: all the nodes are colored blue-grey, and they represent the network population.
Stage 2 :two confidence akins at maximum two breaks compare their number of akin nodes confidence (NC) and their relative mobility (Rm) .The one which wins the competition becomes CA (colored in black)
Stage 3: these confidence nodes to one break become RA.As long as there is an isolated node (blue or black) then they will try to join a group. In case it is not possible and that it fulfills the terms for being candidate to the CA status, it therefore sends an election packet.

```
Algorithme-2 when a node x never reaches its CA
            Cl-id(x) = y ;
           Status(x)=NM ;
        end
    else
        if  x  receives a reply from another CA denoted z then
             begin
                 if  ( NR(x) >= 0,9  et NS(x,z)=1 ) then
                           Status(x) = RA ;
                 else
                   if (x receives  at least 2 replies from 2 different CA)
                        and NR(x) >=0,7 then
                             Status(x) = NP ;
                   else  Status(x) = NM ;
                   fi
               fi
           end
        else request a certificate to the RA node;
     fi
fi
```

An example with 2-hops clusters

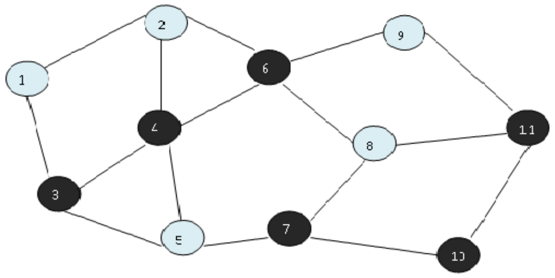
The nodes detecting at least two CA are gateway nodes (orange).

<u>Stage 1</u>



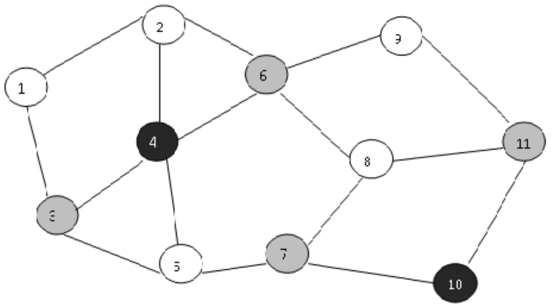
Nodes 1 to 11 form the network.

Stage 2 :



Nodes 3,4,6, 7 ,10 ,and 11 are confidence nodes , (3, 4 , and 6) begin the competition .The same mechanism happens with nodes (7 ,10 ,and 11)

Stage 3 :



Node 4 and 10 have won the competition .Node 3 and 6 become RA of the identity group 4 and nodes 7 and 11 those of the identity group 10.

Thus we obtain two groups in which nodes 4 and 10 act as CA. Nodes 5 and 9 belong to the two groups and can be gateway nodes.

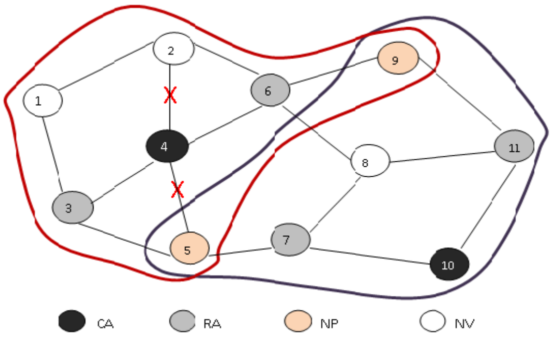


Figure 16: a clustering case with a group size equal to 2.

After this partition phase, algirithm-1 will be re-executed provided that a confidence node with at least another akin confidence node detects neither a CA nor a RA in its proximity of two breaks.

As for algorithm-2, it will be executed if a node is out of the reach of its CA.

In the coming section, we will value the algebraic results of our model in order to appreciate the results.

3.3 Valuation of the suggested security model

This part aims at showing the results of the suggested security model and at comparing it to other security models by using the same mechanisms. This, in order to algebraically prove that it can be a good model for solving the problems of the mobile ad hoc network.

First, we will compare the suggested Algorithm SEA with the clustering algorithms Lowest-ID and MOBIC. Then, we will compare our key management mechanism with the one based on the threshold cryptography .Finally, the advantage of our security protocol compared to protocol COSR will be shown.

3.3.1 Comparison between Lowest-ID, MOBIC, and SEA.

The suggested Algorithm SEA aims at establishing a hierarchical architecture in the protocol COSR. It will enable to sample the security problems so as to solve them at a local level in order to reach a better global security level.

We can sample the ad hoc network like a non-adjust related graphic G (V, E) with;

V: group of the network's nodes;

E: group of ridges allowing a communication between two nodes,

$$E = \{(x,y) \in V^2 / x \neq y \wedge d(x,y) \leq R$$

R= transmission range of nodes

The Euclidian distance between two nodes $x_1$and x_2 is :

$$d(x,y) = \sqrt{\sum_i (x_{1i} - x_{2i})^2}$$

The group of akin nodes of a node x can be defined as follows:

$$N(x) = \{y / (x,y) \in E\}$$

The connectivity degree of a node is:

$$deg(x) = card(N(x))$$

Let deg (G), be the medium connectivity degree between the network's nodes; it represents the average of akin nodes at a break of each of the network nodes.

$\deg(G) = \frac{1}{n} \sum_{i \in V} card(N(i))$; where $n = card(V)$ (n: the nodes number)

Let β1 be the number of clusters formed after the execution of algorithm Lowest-ID and MOBIC, and β2 those formed after the execution of algorithm SEA. We will always have β1≥ β2 because the first two algorithms form only clusters to one break. Therefore, they will have the same number of clusters provided that all the nodes have the same selection parameters.

Let Nbre-msg (Lowest-ID), Nbre-msg (MOBIC), Nbre-msg (SEA), be the number of messages generated and treated when algorithm Lowest-ID, MOBIC, and SEA are respectively executed.

For a mobile Ad Hoc network composed of group of n nodes, we will have:

$$\boxed{\begin{aligned}\text{Nbre\_msg(Lowest} - \text{ID)} &= n + n * \lceil deg(G) \rceil + n \\ &= \boldsymbol{n} * (\lceil \boldsymbol{deg(G)} \rceil + \boldsymbol{2})\end{aligned}}$$

(Each node of the network sends a message containing its identifier so n messages ,more it compares this identifier to those of its akins .Yet , each node has at most [deg (G)] akins hence n* [deg (G)]. Finally, the nodes with weaker identifier send their status of CH and the other nodes reply through a message each to define their status, altogether we have n messages)

$$\text{Nbre\_msg(MOBIC)} = \boldsymbol{n} * (\lceil \boldsymbol{deg(G)} \rceil + \ 4)$$

(MOBIC generates 2*n messages more than Lowest-ID because to ensure a stability to a cluster ,each node of the network sends two messages to assess its relative mobility compared to its akins . After this operation, the number of the exchanged and treated messages is the same as the Lowest-ID's ones, but this time each node sends its mobility value instead of its identifier.)

$$\text{Nbre\_msg(SEA)} = \frac{n}{2} + \frac{n}{2} * \left\lceil \frac{deg(G)}{2} \right\rceil + n = \frac{n}{2} * (\left\lceil \frac{deg(G)}{2} \right\rceil + 3)$$

(concerning algorithm SEA ,only confidence nodes execute the election algorithm , so the $\frac{n}{2}$ confidence nodes send one message each and treat one message of all their confidence akins .However, one node has on average half of its akin nodes , this gives $\frac{n}{2} \left\lceil \frac{deg(G)}{2} \right\rceil$ because each confidence node treats one message of each confidence akin. Finally, each node sends one message for declaring its status, so n messages.

To sum up Algorithm SEA generates and treats less messages than the two others during the clusters establishment stage .Worst, this number is equal to the Lowest-ID's one .And yet, this algorithm doesn't consider the mobility of the nodes.

MOBIC ensures a stability level within the clusters thanks to the mobility criteria .But in algorithms Lowest-ID and MOBIC the implementation process is re-executed as soon as the members of a group change. On the contrary, in algorithm SEA ,whatever the change of the network topology ,if a node can no longer reach its RA or CA , it can be re-affiliated to another CA .The election process is executed only when a node is eligible for the CA status and that it doesn't detect a CA in its proximity of k breaks . Clearly, algorithm SEA requires less control messages for the establishment and the support of clusters to Lowest-ID and MOBIC .More, it is well adapted to the dynamic environments of the mobile Ad Hoc network.

3.3.2 Valuation of the device management mechanism of the suggested protocol.

The use of a public key facility to ensure the authentification between the nodes constitutes a real handicap for the security protocol we suggest. However, to reduce the generated cost compared to the use of the busy tape, the number of calculations and the energy resources, we use the asymmetric cryptography at the local level of the initialization stage. For a network of n size, the certificate generation is of O (n) command .On the way of k size, the signing check is of O(k) command. The control messages size doesn't change .After each validation of a received controlled packet, an intermediate node removes the certificate of the previous node then affixes its own one before re-diffusing it .Then, the control messages size has a variation of O(1) command .To neglect the coast of a generated calculation by the coding and the decoding of the messages, we also suggest the use of the cryptography based on elliptic charts for ensuring confidential communications between peers.

However, it should be noticed that our key management mechanism decreases the use of network's resources compared to the device management mechanisms based on threshold cryptography. Indeed, in these security mechanism, the role of the CA is dispensed on the n nodes and each CA holds a portion of the secrete device, which prevents its deal by an attacker. An attacker must have at least k portion of key for reconstructing the secrete device. Nevertheless, the choice of this k remains the real challenge to take up in these security systems. k must be small enough for a node to reach the quorum of k servers so as to validate a public device . At the same time, this k must be big enough to prevent its reconstruction by an attacker .Moreover, the use of the threshold cryptography requires a pre-configuration of n servers and an authority in charge of the distribution of the devices; which is opposed to the mobile Ad Hoc networks reckoned to be dynamics.

The hierarchical reputation protocol based on a suggested device facility doesn't suffer from these problems in the secrete device protection mechanism of the CA of a group. We establish a confidence commune (group of R.A) around node CA. It constitutes a front between CA and the member nodes with weak reputations, the visitor nodes, and the unknown ones. Thus, only the members of this confidence commune can directly communicate with the CA.

3.3.3 Comparison between the suggested protocol and the protocol CORS

First of all, it should be emphazed that protocol COSR enables to block the selfishness but not the malice of the cooperative nodes. And yet , the security model we suggest prevents not only the malicious action of the unknown nodes and visitors but more ,it obliges the confidence nodes to keep on adopting benevolent behaviors .This ,thanks to the use of certificates and signatures during the exchanges .In fact, in protocol COSR a node can lie compared to the reputation and recommendation information ,which is not the case in our protocol .Here ,all the information are reliable preventing so the different entities to disclose false information .

Secondly, in an open environment where any confidence relation is not pre-established, the use of another confidence is more than necessary for establishing the confidence between the different peers. If it is true that in protocol COSR a node decides to treat or not the demands of the others by going through the reputation of this latter, the fact remains that the reputation information in this protocol is not certified by another one in which both trust .Therefore this latter can refuse to treat the demands of a legal node by malicious intent or even treat the demands of a malicious node without knowing it. Such behaviors increase the network's charge in vain and can disturb all the established security mechanism.

Then, to discover a way, the packet RREQ is re-diffused by all the akins until the purpose is reached .Therefore we have a retransmission of at least: k* ([deg (G)] – 1) and to the maximum k*([deg (G)]-1) with k: the number of breaks between a source and a destination.

Finally, protocol COSR is exposed to Sybil and Spoofing attacks like all the reputation protocols with no authentification mechanism.

The security protocol we suggest is not victim of these weaknesses. On one hand, all the members of a group benefit from a certificate delivered by the head. This certificate ensures a mutual authentification between the group's entities .As a result, any malicious node can boast the identity of a legal node. More, in this security protocol a node knows all the members of its group and their status. The network's sharing makes the local services more available, excludes traffics of extended impacts, makes easier the detection and the effect face to an interference, and so on.

On the other hand, the reputation information are signed by the CA and are known by all. Therefore, when a node receives a packet, the validity of the information on the certificate and its reputation value are enough for deciding its credibility or not. As a result, there is no possibility to teach by malicious intent or to make a mistake and reject the packet of a legal node. In addition, the link nodes are those belonging to at least two groups. They assure inter-groups communication .From then on ,to have a way from a source to a destination ,only t rediffusion are necessary and worst 2t rediffusions ; with t :the number of group separating a source and a destination .

In all, the suggested security protocol enables to reach a best security level ,with a weak increase of the need in network resources compared with protocol COSR.But ,during the assessment of the different weaknesses of this protocol, it is clear that ours is the best adapted .

4. CONCLUSION

The aim of this research work is to define a model which enables the communication security in the mobile Ad Hoc network while considering the exchange security and a total cooperation of the different entities of the network .To do that, we have inserted a cryptographic module in the security protocols based on the reputation due to the nodes' reputation in order to ensure a confidence relation between the network's entities .Indeed, the Ad Hoc networks being opened ,a security model based on the confidence has appeared more adapted in the solving of the security problem of this kind of network .Then , confidence can depends on the cryptographic mechanisms where confidence nodes must be the certified ones. This confidence can also be based on the reputation mechanisms which force the nodes to cooperate .Thus, these ones can join their confidence in a separate way to the nodes with a good reputation level.

In this research , we have chosen a complementarity of these two confidence approaches so as to make the most of their different advantages .It is from this perspective that our security model is based on protocol COSR (Cooperation On-demand Secure Route) which is a reputation protocol .Our concern was to guarantee the confidence among the mobile Ad Hoc network's entities .We have then suggested a partition algorithm (SEA :Secure Election Algorithm)of the network for assuring efficiently a local security in each group in order to reach a good global security level. This process makes easier the detection and the insulation of the malicious nodes. Moreover, a public device facility has been established in each group .The role of the certification authority is allocated to the head of the group which is surrounded by other confidence nodes which assure its protection. The certification authority delivers certificates to the members of its group what enables them to authenticate themselves each other.

Contrary to protocol COSR where the reputation information are not certified , in our proposal it is up to the certification authority to diffuse the certified information based on the reputation of the different entities of the group. The suggested security model minimizes the value the controlled messages (send in diffusion) during the way searching mechanisms .This represents a real saving of the network's resources and a contribution to the reactivity of the traditional protocol DSR (Dynamic Source Routing). Algebraic results have been provided in order to compare our model with the main existing mechanisms .This comparison shows the effectiveness of our model in the management of the security problem in the mobile Ad Hoc networks. However, we plan to make some simulations in order to attest these results.

REFERENCE

[1] C.E.Perkins and P.Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. ACM SIGCOM,…

[2] Josh Broch, David B. Johnson, and David A. Maltz. The Dynamic Source Routing Protocol for MobileAd Hoc Networks. Internet-Draft, draft-ietf-manet-dsr-03.txt, October 1999. Work in progress. Earlier revisions published June 1999, December 1998, and March 1998.

[3] Y. Chun Hu, A. Perrig and D.B. Johnson. Ariadne, "*A secure on-demand routing protocol for Ad hoc networks*", Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.

[4] B. Sonja and L. B. Jean-Yves. *"Performance analysis of the confidant protocol"*. In MobiHoc, pages 226- 236. ACM, 2002.

[5] F. Wang, B. Huang, and T. Y. Laurence. "*COSR: Cooperation On-demand Secure Route*" In EURASIP Journal onWireless Communications and Networking. 25 June 2010.

[6] A. Rahman, and S. Hailes."*A distributed trust model*". In Proceedings of the New Security Paradigms Workshop (NSPW-97), pages 48--60, New York, September 23-26 1997. ACM.

[7] F. Stajano, R. Anderson. "*The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks*", the 7th international workshop on security protocols, LNCS 1796, Springer-Verlag, 1999.

[8] J-B. Hubaux, L. Buttyan and V. Capkun. "*The quest for securing in mobile Ad Hoc networks*", in 2nd ACM Symposium on mobile Ad hoc Networking and Computing, Octobre 2001.

[9] S. Sunita, and K. S. Shishir. "*A Comprehensive Survey on Intrusion Detection in MANet*" International Journal of Information Technology and Knowledge Management july-December 2010, Volume 2, No. 2, pp. 305-310.

[10] P. Papadimitratos, Z.J. Haas. "*Secure Routing For Mobile Ad Hoc Networks*", *SCS* Communication Networks and Distributed Systems Modelling and Simulation Conference *(CNDS 2002)*, San Antonio, Etats-Unis, 27-31 Janvier 2002.

[11] Y. C. Hu, D. B. Johnson, and A. Perrig. "*SEAD: secur efficient distance vector routing for mobile wireless ad hoc networks*," in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications, IEEE, June 2002.

[12] G. Zapata and N. Asokan. "*Securing ad hoc routing protocols"*. In W. Douglas Maughan and Nitin H. Vaidya, editors,Workshop on Wireless Security, pages 1-10. ACM, 2002.

[13] B. Levente and H. Jean-Pierre. Nuglets: "*a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks*". In Technical Report DSC/2001/001, EPFLDI –ICA, January 2001.

[14] A. Rachedi et A. Benslimane. "*Architecture Hiérarchique Distribuée pour sécuriser les Réseaux Ad hoc Mobiles*", 8ème journées Doctorales en Informatique et Réseaux, Marne la Vallée, Janvier 2007.

[15] A. Altalhi et G. Richard.*" Virtual paths routing : A highly dynamic Routing protocol for ad hoc wireless networks*".Dans : Proceedings of the PerCom Workshops, pp. 81–86. Mars 2004.