A PKI over Ant Colony based Routing Algorithms for MANETs –AntPKI–

Benamar Kadri, Djilalli Moussaoui, and Mohammed Feham
(corresponding authors: Benamar Kadri)

STIC Lab., Department of Telecommunication, University of Tlemcen, Tlemcen, Algeria
(Email: benamarkadri@yahoo.fr)

(Received Nov. 7, 2011; revised and accepted Feb. 1, 2012)

Abstract

Last years have known the emergence of new paradigm of networking called wireless mobile ad hoc networks, giving birth to a variety of networks ranging from personal or body networks to wide area networks. Regarding their nature and the used medium lot of problematic are not well carried out such as routing and security, however in the last years lot of propositions have been deployed to solve these two problems. Swarm intelligence techniques are one of the most promising propositions. The swarm intelligence (SI) routing inspires from insect communities such as bees and ants to find and optimizes routes within an ad hoc networks. However all the existed implementations of swarm routing do not give any consideration to security, which is a persistent need for wireless networks. Therefore in this paper we are going to treat the aspect of security over SI routing by giving a lightweight implementation of public key infrastructure (PKI) over ant routing algorithm. Our proposed scheme called AntPKI gives an implementation of PKI which is completely independent from the underlying SI routing protocols and tries to ensure all the security services by taking advantages of the nature of the underlying routing protocol.

Key words: AntPKI, ARA, MANETs, PKI, routing, security, swarm intelligence.

1 Introduction

Unlike traditional wireless networks, wireless mobile ad hoc networks (MANETs) are infrastructure less networks consisting of a set of handled devices such as lap tops, PDA, mobile phones…etc, often mobile and moving in a limited area. Accordingly mobile nodes within an ad hoc network must collaborate to execute some of the habitual network services such as routing and security [3].

Routing is a crucial service that must be achieved by the ad hoc network, because the nature of nodes which are very often constrained devices with limited battery power and processing capabilities as well as the nature of the area of deployment which is unpredictable and unstable make the routing service a challenging task which can only be achieved by the collaboration of all the network nodes. In the way that each node plays two roles, the first one as an ordinary node and the second one to achieve the routing service and ensure data forwarding and route establishment which leads to lot of routing problems which are not treated in the conventional routing protocols [13].

The second crucial service of MANETs is security which is the most challenging task to be carried out by the scientist community. Since the MANET is very often part of a hostile environment such as battlefields which make it subject of a variety of attacks, in the other hands the nature of the used medium (radio waves) which is opened to anyone with the proper hardware and the network stack exposing the exchanged data to several attacks such as eavesdropping, data modification, impersonate ….etc [15].

In literature, these two problematic are treated separately, by developing routing protocols without any consideration to the security service which always leads to incomplete solutions, since the security is not natively implemented and all the proposed security solutions are extensions given to overcome the limitations of security which makes them vulnerable to lot of attacks.

2 Routing in MANETs

In order to treat routing in MANETs lot of algorithms are proposed toward the specificities of MANETs such as node mobility, devices' constraints as well as the used medium. According to the strategy followed by the routing algorithms several categories exist:

2.1 Proactive Protocols

This category of routing is inherited from the conventional ones, since it keeps the whole topology of the network by each node over the network in the routing table. Node mobility and topology changing are treated by periodically exchanging the routing tables between neighbors. Routes are found immediately however the maintenance of the routing tables consumes the network resources in high mobility networks [4].

2.2 Reactive Protocols

In order to treat the disadvantage of the proactive routing and minimize the overhead due to topology changing the reactive routing protocols propose to occasionally react to the demand of route establishment by launching a route discovery mechanism to find routes only when needed, since at a given moment only a subset of the network nodes are communicating at the same time. This kind of routing is very suitable for MANETs however the overhead during route discovery can block the network due to flooding [12].

2.3 Hybrid Protocols

Tacking advantages of the reactive and the proactive routing protocols, the hybrid ones use a hierarchical structure of the network to ensure routing, in the way that the entire network is organized into clusters or regions in which we use a proactive strategy to ensure routing inside each cluster and a reactive one to ensure inter-cluster communication [14].

2.4 Swarm Intelligence based Routing

This category of routing is recently developed for MANETs inspired from insect communities such as bees and ants which very often collectively execute smart actions with only a little intelligence at each insect, which can be very practice from the MANETs perspective since each node within a MANET can be viewed as an ant in a hostile environment with limited capabilities and trying to find its way to food or to the nest. Using artificial pheromone and probability computing this kind of routing finds the best path according to a variety of parameters defined according to the network context [1].

3 Swarm Intelligence based Routing

As devoted in the previous section, the swarm intelligence routing paradigm is completely inspired from insect swarms such as ants and bees. Since these swarms of insects have lot of desired characteristics compared to MANETs, in the way that ants or honeybees swarms are made up of hundreds to thousands of small insects with little intelligence and communication capabilities in an unpredictable environment, however always generate smart solutions and achieve the objectives of the community such as finding or optimizing the path to the food [1].

From MANETs' perspectives, it seems that the characteristics of such communities are very suitable, since a MANETs is very often composed of a variety of handled devices with limited capabilities working together for ensuring the connectivity of the network and ensure the continuity of the routing service.

The most known swarm intelligence based routing algorithms are inspired from the ant colony, the swarm intelligence in this community is achieved using a special form of communication based on pheromone which is a substance related to hormones produced by each ant during its movement, this pheromone is sensed by other ants within the community in order to find their route in the nature, since ants are attracted by pheromone which leads it to the food or the nest.

Ants always follow the higher pheromone concentration which often leads to follow the shortest trail and causes a self-accelerated reaction without any centralized intervention, which ensures path optimization, because the shortest path have always the greatest concentration of pheromone.

3.1 The Ant Routing Algorithm

Using the same idea devoted in the previous section to find food and optimize the route from the nest to food, the Ant Routing Algorithm ARA [5] uses artificial ants and pheromone to discover and optimize route from a given source node S to a destination node D in a MANET.

Generally, ARA uses two kinds of artificial ants for route discovery and establishment:

The first one is called forward ant (FANT), which is used to discover routes from the source to the destination node. Therefore this ant travels over the entire network in order to find any possible route from S to D, similar to the discoverer ants in real ant colony which go far in the nature in order to find any possible source of food, during her trip over the network each ant deposits a constant amount of artificial pheromone used after by the intermediate nodes to shorten paths.

The second kind of ants are called backward ants (BANT), these ants follow the same path established by the FANTs in order to establish the final route from S to D. Therefore the BANT travels over the same path discovered by the corresponding FANT from D to S in order to inform S about all the possible routes.

During their lifetime the BANT and the FANT modify at each hop the artificial pheromone for each edge over the network by adding a constant amount of pheromone $\Delta\varphi$ at each visit to any intermediate node emulating real ants. Consequently, ARA uses a pheromone table in which it saves the level of pheromone for each edge. So, each node has a record in this table for each edge, the pheromone table is increased by FANT and BANT and accordingly decreased due to time.

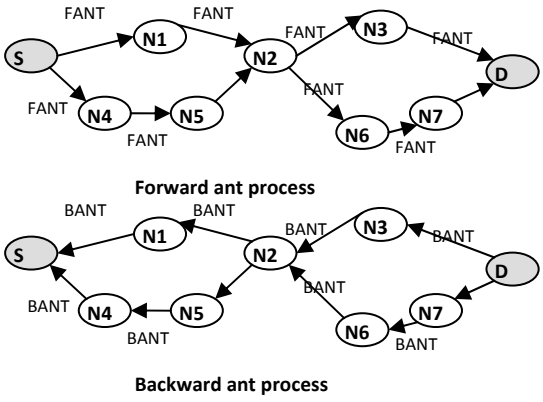

Figure 1: Forward and backward ants in ARA

Using the value of pheromone for each edge, each node computes the probability to use one of these edges for routing using the following equation:

$$p_{i,j} = \begin{cases} \dfrac{\varphi_{i,j}}{\sum_{j \in N_i} \varphi_{i,j}} & j \in N_i \\ 0 & j \notin N_i \end{cases} \qquad (1)$$

$$\sum_{j \in N_i} p_{i,j} = 1$$

As we can observe ARA is a distributed routing algorithm inspired from ant colony to establish routes within a MANET. ARA has lot of suitable characteristics for MANETs which makes it one of the most favorite algorithms for large scale ad hoc networks. However, from the security point of view, it seems that ARA does not implement any security mechanism to ensure the integrity, authentication, confidentiality of the exchanged data over the network, in the way that ARA defines only the necessary mechanisms and procedures to establish and maintain routes.

4 PKI in MANET

A public key infrastructure is a set of components for managing digital certificates in a given community or network, PKI is recognized as the most powerful tool providing trust and security in conventional networks. PKI relies on asymmetric cryptography to ensure authentication and non-repudiation over the whole network based on a trusted authority called certificate authority CA which signs and verifies certificates of the entire network, therefore the robustness and availability of the PKI services depends on the availability and the security of the CA, consequently the greatest intention must be given to the CA when deploying a PKI [14]. Depending on the application and the environment where a PKI is deployed other component can be added such as Registration Authority (RA) and Certificate Revocation List (CRL).

The current standard of certificate [14] contains a set of information such as names, address, public key of the holder…etc, however according to the requirement of each system new fields can be added to allow a perfect identification within the community, such as IP or MAC address. The whole document is passed into a hash function for being signed and certified by the CA. The certificate of each individual within the community is published by the CA as well as the revoked ones which allow other individuals of the community to verify and authenticate messages coming from the other members of the same community.

PKI was deployed for several conventional networks since it guaranties a great level of security and authenticity however it stills unclear if such infrastructure can be deployed for a MANETs due to the infrastructure-less nature, limitation in devices' capabilities as well as the security problems since a MANET is usually part of hostile environment where the possibility of a node to be compromised or captured is higher than in any other conventional network which exposes the PKI services to several attacks such as the impersonate attack. Therefore, new approaches must be defined to deploy PKI for MANETs taking into account the specificities of these networks such nodes' mobility, physical attacks, devices constraints…etc.

In literature, lot of implementations of PKI for MANETs has been proposed trying to overcome the constraints of a MANET by proposing a set of mechanisms and procedures to deploy efficiently a PKI:

The trivial implementation of PKI for any network is to affect the whole services of the CA to one node in the network to be responsible of certificate publishing, renewal, revocation…etc, which is the case in all the conventional networks. Nevertheless deploying such architecture for a mobile network creates a point of failure which is the node handling the CA services, since the disappearance of this node due to mobility for example causes the service desertion. Therefore, affecting all CA services to only one node in a MANET is not efficient; consequently the CA's services must be distributed to more than one node in order to ensure the continuation of the security service. Although, in literature lot of propositions have been deployed in order to implement a PKI for MANET by distributing the CA services over the network's nodes.

4.1 Partially Distributed Certificate Authority

This solution proposed by Zhou and Hass is based on a (k, n) threshold scheme to distribute the CA's signing key to k nodes over the network using Shamir's secret sharing scheme [17]. In the way that the CA's services are accomplished by contacting these k servers and any decision is achieved only by the coalition of these k servers which ensures more security, because it is difficult for an attacker to compromise all the k servers in the same time. Therefore a valid signature can only be obtained by the K servers in order to ensure the CA's services such publishing and revocation of certificate over the network. Availability and scalability is ensured by choosing the appropriate value of k in order to ensure that at any time there are at least k servers in the neighbourhood of each node.

This solution is essentially proposed to overcome the problematic of availability, scalability and security, however the mechanism of key sharing adds a great overhead to the network due to message exchanging for certificate signature, verification and publishing, which makes this solution useless for constrained devices which are always the case of MANETs composed of handled devices with limited capabilities.

4.2 Cluster based PKI

The authors in [11] propose a cluster based scheme to implements the PKI for ad hoc networks. This solution is based on partially distributed certificate authority, in order to divide the CA's signing key among cluster-heads, which means that any CA operation is achieved by the coalition of all cluster-heads in the network. However the use of

threshold cryptography may add an overhead due to the number of exchanged messages during any operation (verification, renewal…etc), it may also encounter other problems to ensure scalability when adding new cluster-heads or whenever a cluster-head leaves the network. In recent work we have also proposed a simplified implementation of PKI for ad hoc networks, employing clustering architecture in order to simplify and distribute CA services over the network. The proposed scheme divides the whole network into clusters and chooses the most powerful node among cluster members to ensure the CA services for the corresponding cluster. The cluster-head is the CA of its cluster collaborates with other CAs over the network to ensure inter-cluster PKI services using a mechanism of multi-signature [11].

4.3 PKI-DSR

The authors in [8] give an implementation of PKI which can be applied to any reactive routing protocol, the proposed solution uses the underlying routing protocol operations to execute the PKI operations such as certificate publishing, revocation and attacks detection, which makes this solution more suitable for ad hoc networks since it does not add any overhead to the network because the security operations are executed during the execution of routing operations. The proposed scheme uses the route discovery mechanism in order to publish nodes' certificate and the route reply to establish the session key between the source and the destination node. In the way that the certificate of the source node is attached to the route discovery request and flooded over the whole network which guaranties the publication of this certificate without any extra operations for that purpose, as well the route reply request is used to transmit the session key to secure end to end communication between the two entities.

The example given for the application of this solution is built over the dynamic source routing DSR, the proposed protocol is called PKI-DSR according to the simulation results of PKI-DSR compared to the original DSR, PKI-DSR add a little overhead to the network whenever there is attacks against the network, otherwise there is no overhead.

4.4 µPKI

µPKI is a lightweight implementation developed especially for wireless sensor networks [9]. µPKI has taken into consideration the constraints of sensor nodes such as battery and computing power. µPKI is based on a set of handshakes in order to secure the communication between the base station and sensors as well as sensor to sensor communication, µPKI uses symmetric encryption to secure end to end communications between the network's sensors and the base station, the symmetric key is negotiated and established during the handshake phase using the public key of the base station, since the authentication is built around the base station's public key. In addition to the symmetric encryption, µPKI uses MAC (message authentication code) for each packet to ensure integrity. Compared to other schemes µPKI is more optimal and ensure a great threshold of security using simple operations, it also uses periodic key update in order to enforce security and resist against long term attacks.

5 Attacks against routing in MANETs

Due to the nature of the used medium which is opened to everyone with the adequate hardware and the network stack, as well as the nature the underlying technique of communication which is based on multi hop routing in which every node is responsible of executing routing primitives to ensure the network connectivity. A large variety of attacks against MANETs exists:

Black hole: the objective of this attack is to attract the traffic from a particular node or region through the attacker [10], by injecting false routing information advertising the attacker having the shortest path to the destination which redirects the network traffic over the attacker, in order to stop the network service or to execute other attacks such as man in the middle, data modification or eavesdropping …etc.

Routing table poisoning: This attack is performed against table driven routing protocols, in the way that the attacker diffuses false routing information to its neighbors in order to disturb or block the traffic over the network [6].

Denial of service attacks: in this kind of attacks the attacker tries to disrupt, deny or degrades the service of the network, it is executed in different ways and decreases network performances, this kind of attacks is the most dangerous since all attacks defined previously can be subject of denial of service attacks if they are executed permanently against the network [2].

Spoofing attack: also called impersonate attack is executed in the absence of an authentication mechanism, in the way that the attacker spoofs the identity of a legitimate node in order to gain access to the network or to execute malicious actions using the spoofed identity such as black hole, replay or data modification like denial of service attack, this attack can be avoided using a mechanism of authentication such as digital certificate [7].

6 AntPKI

As we have described above, lot implementation of PKI have been proposed in literature in order to make in practice an effective security solution that take into consideration all the characteristics of MANETs, however the majority of these solutions give a set of a stand-alone specifications that implements independently the PKI without taking into consideration the underlying routing protocol in order to optimize the PKI's operations by using some of the routing procedures for PKI's services implementation such as in PKI-DSR, since the exploitation of the routing operations may minimizes the overhead due to PKI's services.

In the same context, in the following sections we are going to present an implementation of a PKI over ant colony based routing protocols; this kind of routing knows a great development due to its characteristics which are very

suitable for MANETs, however all the recent proposed protocols do not give any consideration to security. Therefore, we are going to propose an implementation of PKI called AntPKI to be used over this kind of routing; our proposed implementation will make use of the specifications of underlying protocols in order to publish, revoke and secure end to end communications.

6.1 ANTPKI Strategy

As mentioned above, ant colony based routing protocols generally use a set of request known under the name of ants used to discover and establish the path between two nodes in the network. ARA for example uses two kinds of ants. The FANT used for route discovery, it is forwarded by each node over the network until it arrives to the destination node, which replies with a BANT which is sent to the source node in order to establish the final path. Consequently each node in the network may forward at a given time a FANT or BANT during the routing process. Accordingly, any implementation of a PKI over ant based routing must use these ants in order to implement the security procedures of a PKI and publish self-issued certificates of the network nodes.

6.2 System Bootstrapping

In a conventional PKI there is a centralized server responsible of the generation, publication, renewal and revocation of each certificate within a given community, however due to the characteristics of a MANET these services cannot be done in the same way since there is no concept of centralized authority which can accomplish this task, consequently the network nodes must collaborate between themselves in order to accomplish this task.

To overcome the absence of the certificate authority, in AntPKI the certificate are self-issued by each node in the network, hence each node is responsible of the information contained in its certificate as well we suppose that each node have the capability of generating and keeping in secret its certificate, private and public key. The certificate structure is inherited from X.509 V3 standard by adding some additional fields which can be useful in our case such as the IP or MAC address. So, when any node joins the network for the first time it must generate a certificate and fills it with the adequate information such as the user name, validity period, public key, MAC and IP address, signs this certificate with its private key, and waits for the appropriate moment to publish the certificate for the rest of nodes.

In order to handle the revocation and the publication service of PKI, each node must have the capacity to handle and manage two directories, the first one is for saving revoked certificate and the second one is to save valid certificate.

6.3 PKI Management and CA Services

The most important services of a PKI is the publication and the revocation lists, because they are visited by each entity in a given community in order to verifies the validity of the certificates and consequently ensure the security of the network. Therefore in AntPKI we have defined a mechanism for certificate publishing which uses the underlying protocol to publish certificate over the entire network.

Therefore, we are going to make use of the mechanism of route discovery in order to publish the certificate of each node for the rest of nodes over the network.

(1) Certificate publishing

The ant colony based routing is based on ants in order to establish and maintain routes over the network. Therefore, in AntPKI we are going to utilize these ants in order to publish and secure links over the network. AntNET or ARA is based on the FANT in order to discover routes over the network; this ant visits each node over the network deposing a kind of substance called pheromone used after to compute probability in order to evaluate routes. Our interest in this ant is that it visits each node over the network during the period of route discovery, which makes it the preferred period to publish certificate. Our proposed solution to publish certificate is by using the FANT to handle the certificate publishing over the network, thus we propose to create a new field in the FANT which will contain the certificate of the source node. Consequently, each node when launches a route discovery, it inserts its certificate into the FANT before launching it. As a result, the certificate of the corresponding node is diffused over the entire network; consequently each intermediate node retrieves from the FANT the certificate of the source node and saves it in the corresponding directory for future use, in the same process of route discovery each intermediate node use the FANT as support to transfer its certificate to its neighbors.

The structure of the forward ant is changed by creating new fields, the first one is used by the source node in order to publish its certificate for the rest of nodes and the second one is used by intermediate nodes to publish their certificate for their neighbors.

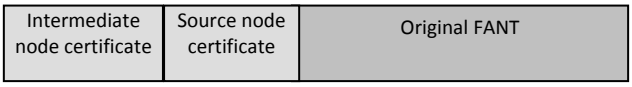

Figure 2: Structure of new FANT

(2) Certificate Revocation

The revocation mechanism is used in a PKI in order to cancel some certificates from use for validity reason since each certificate is valid only within a given period, or for security reasons due to an attempt from the corresponding node to build up an attack against the network, if the network has an intrusion detection system. For this reason each node, keeps a revocation list where it saves the revoked certificate, the certificate revocation list is updated by an accusation mechanisms defined by AntPKI. Since, in AntPKI each node when detects any malicious attention from a neighboring node using an underlying intrusion detection system, it sends an accusation request which contains the certificate of that node otherwise if it has not its certificate it send an accusation with the IP or MAC address of that node. The accusation request is diffused over the entire network; the corresponding certificate is automatically revoked whenever the number of accusations reaches a predefined value. Whenever the certificate is revoked due to

the detection of an attack AntPKI does not revoke only the certificate of the corresponding node however it revokes all the information contained in the certificate such as names, IP and MAC address, accordingly the corresponding node is excluded from all the possible services of the network.

(3) Certificate renewal

This mechanism is launched by the interesting node, whenever a node wishes to renew its certificate due to the expiration of its delay or the modification of the certificate fields, it generates the new certificate involve it in a renewal request and diffuses it over the entire network, each node when receiving this request changes the old certificate with the new one.

7 AntPKI Functioning

In the previous section we have presented the operations that manage digital certificates using AntPKI; however distributing and publishing certificate is only useful if they are used for securing links between each pair of nodes in the network.

In order to ensure security services such as integrity, confidentiality and non-repudiation using AntPKI we propose to use three mechanisms of cryptography:

Asymmetric encryption: this method of cryptography is used for digital signature, for producing digital certificate and packet signature; we also propose to use asymmetric encryption for session key establishment since it guaranties a great level of confidentiality and authentication.

Symmetric encryption: this method of cryptography is based on a single key shared between two entities in a given community, it is very practice to encrypt big amount of data in a short time, which makes it the preferred solution to encrypt ordinary traffic over the network.

Message authentication code "**MAC**": usually this solution is used to provide integrity, which can be viewed as a hash function applied on a data packet, resulting on a digest. This digest is encrypted using a symmetric encryption with a key shared between the communicating parties. The MAC is always joined to the original packet and verified by the destination node using the same key to detect any alteration to the packet integrity.

7.1 Session Key Establishment

In order to ensure the confidentiality over the network we propose to encrypt the ordinary traffic over the network using symmetric encryption which is very suitable regarding its costless compared to the asymmetric one. Thus, we propose to establish a session key between each two communicating entities to encrypt ordinary traffic, this session key is established by the cooperation of the entities using their public key and using as support the backward ant BANT to optimize the network resources.

As we have presented in the previous section, the certificate of the source node is diffused over the entire network using the FANT, using the same idea the destination node uses the BANT to publish its certificate along the discovered route. Consequently, the BANT structure is modified by including a new field which will contain the certificate of the destination node. We also use BANT as support for establishing the session key between the communicating parties (source and destination); accordingly the original BANT packet structure is modified to include another field used to transmit the session key by the destination node to the source node.

Whenever, the FANT arrives to the its destination, the destination node saves the certificates contained in this request, generates a BANT and inserts its certificate in the appropriate fields, then it generates a random session key, encrypts it using the public key of the source node obtained from its certificate and sends the BANT over the discovered route.

Figure 3: Structure of new BANT

Whenever the source node receives the BANT, it can conclude three kinds of information from this request:

- The established route needed for data forwarding.
- The certificate of the destination node.
- The session key encrypted by the destination node's public key.

The source node retrieves the session key from the BANT, decrypts it using its private key and according to the specifications of the underlying routing protocol it waits for the adequate moment to begin using it for data encryption and authentication.

In order to ensure more security and to resist against long term attacks which tries to conclude the used encryption key by analyzing the exchanged traffic for a long period we propose to use a periodic key update to periodically update the session key. The key update is launched by one of the two communicating parties after the expiration of the period and consisting on the creation of a new random session key encrypts it with the public key of the other node and sends it over the same route, when receiving this request the second node decrypts it using its private key and begin immediately using the new key.

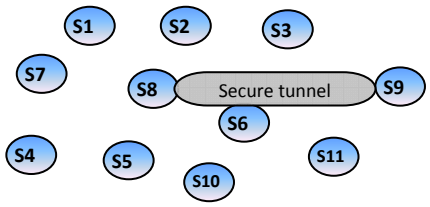

Figure 4: Session key establishment.

7.2 Integrity and Authentication

As we have implicitly mentioned above, integrity is ensured using MAC (Message authentication code), joined to each packet transmitted over the network. The MAC is joined to the packet either this packet is encrypted or not, because some control messages do not need to be encrypted however they need to be authenticated. The MAC can be encrypted using the session key shared between the communication parties and established during the route discovery or using the public keys. A MAC using public key encryption ensures both authentication and integrity which makes it the preferred mechanism to be used over AntPKI.

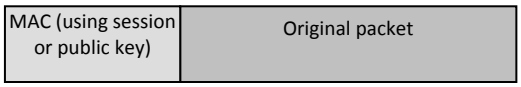

Figure 5: Structure of new packet

8 Analysis

8.1 Key Management Specifications

In this section we are going to analyze AntPKI regarding the habitual evaluation criteria of key management schemes:

Fault Tolerance: this propriety deals with the continuation of services whenever one or more nodes over the network are lost, AntPKI guaranties efficiently this property since the lost of any node over the network does not affect AntPKI since in AntPKI each node is responsible of the generation, publication and the use of its certificate.

Security: this aspect deals with the confidentiality and integrity of the exchanged data over the network, as we have presented above AntPKI uses two methods of cryptography to ensure and enforce security. The first one is used for authentication and integrity using MAC (Message authentication Code) signed by the public keys or by the session key of the communicating parties which guaranties both integrity and authentication. The second method is using symmetric encryption to guaranty confidentiality of the exchanged data using a session key established during the route discovery period

Scalability: this propriety deals with the network widening. As devoted above AntPKI is built over ant colony based routing which deals efficiently with the network widening which means that AntPKI also does so, because AntPKI uses the same request of the underlying routing protocol to ensure PKI's services which does not affect the network performance.

Availability: this propriety guaranties that the service of security is available whenever needed by any node over the network, in AntPKI the PKI's services are always available since these services are guaranteed by each node alone which distributes and simplifies its management between the whole network nodes.

Certificate publishing: as we can observe at each route discovery each node over the network tries to diffuse its certificate to all the network nodes by using the underlying FANT as support for this purpose, because the FANT travels over the whole network which guaranties the certificate publication to every node in the network. Consequently each node gathers in its certificate directory a great amount of certificates which are used to verify the integrity and authenticity of the exchanged data.

Network performance: regarding the network performance AntPKI does not add any overhead to the network because it use as support the underlying routing protocol to handle the specifications of AntPKI such as certificate publishing, which guaranties the efficiency of AntPKI. However, during the detection of attackers a small overhead is added to the network in order to revokes the certificate of this node and exclude him from the network.

8.2 Resistance Againnst Attacks

As given in the previous section AntPKI guaranties all the key management criteria such as availability, scalability…etc, which are very important to deploy a key management scheme, however AntPKI must ensure more security by resisting against all known attacks, therefore in this paragraph, we try to evaluate the robustness of AntPKI face to the majority of existed attacks:

Passive attacks: These kinds of attacks like eavesdropping permanently capture and analyze the exchanged data over the network in order to retrieve information like the network architecture, security or routing mechanisms. Passive attacks cannot be executed against AntPKI because the exchanged data over the network is encrypted using symmetric encryption, which makes it out from any tentative of eavesdropping. To ensure more security we have used periodic key update in order to resist against long term attacks executed by collecting a great amount of encrypted data.

Modification, replay and Insertion: These kinds of attacks alter the integrity of the exchanged data, using the key agreement defined above each communicating nodes share a symmetric key used to ensure data confidentiality enforced by a periodic key update, in the other hands data authentication and integrity is guaranteed using digital signature.

Black hole attack: In this attack, the malicious node tries to attract the exchanged traffic over itself; by replying with false BANT which drives all the exchanged data to this node giving him the possibility to execute any other attacks. Using AntPKI black hole attack is not possible since AntPKI is based on digital certificate giving the possibility to both source and destination nodes to authenticate each other and verify the validity of discovered routes.

Spoofing attacks: Using our approach it seems that this attack can't be executed since the mechanism of certificate publishing using forward and backward ants ensure the publication of nodes' certificate over the

network used after for ensuring the authentication and the security of nodes over the network similar to conventional network.

9 Conclusion

In this paper we have presented an implementation of PKI for MANETs over ant based routing algorithm, as it is known PKI is the most secure and popular solution to guaranty security in conventional networks however it is unclear if it can be efficiently implemented in MANETs due to the characteristics and the constraints of this kind of networks. Our proposed scheme called AntPKI is a simplified implementation of PKI for MANETs over swarm intelligence routing. AntPKI uses the mechanism of route discovery as support for certificate publishing using FANT and BANT which guaranties that the certificates of both communicating parties reach the majority of the network nodes. Using the underlying routing protocol as support for security management optimizes the network performances and leads to an efficient PKI implementation.

In addition AntPKI guaranties data confidentiality using a session key established at the same moment of the certificate publishing and using the same requests (FANT and BANT).

Reference

[1] A. Agah and S. K. Das, "Preventing dos attacks in wireless sensor networks: A repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145–153, 2007.

[2] T. Clausen, P. Jacquet, and L. Viennot, "Comparative study of routing protocols for mobile ad hoc networks," in *Proceedings of Med-Hoc-Net'02*, pp. 1-10, Sardegna, Italy, Sep. 2002.

[3] T. Engel, D. Fischer, T. Scherer, and D. Spiewak, "A survey on security challenges in next generation mobile networks," in *Proceedings of the Third International Conference on Mobile Computing and Ubiquitous Networking*, pp. 116-125, 2006.

[4] M. Gunes et. Al, "ARA the ant-colony based routing algorithm for MANETs," in *Proceeding of the International Workshop on Ad Hoc Networks*, pp. 79-85, 2002.

[5] X. Hong, K. Xu, and M.Gerla, "Scalable routing protocols for mobile ad hoc networks," *IEEE Network*, vol. 16 no. 4, pp. 11-21, 2002.

[6] B. Kadri, A. Mhamed, and M. Feham, "A new management scheme of cluster based PKI for ad hoc networks using multi-signature," *IEEE Global Information Infrastructure Symposium*, pp.167-172, 2007.

[7] B. Kadri, M. Feham, and A. Mhamed, "Securing reactive routing protocols in MANETs using PKI (PKI-DSR)," T*he Journal of Security and Communication Networks*, vol. 2, no. 4, pp. 341-350, 2008.

[8] B. Kadri, M. Feham, and M. Abdellah, "Lightweight PKI for WSN (μPKI)," T*he Journal of Security and Communication Networks*, Vol. 10, No. 2, pp. 135-141, 2010.

[9] B. Kadri, D. Moussaoui, and M. Feham, "Link quality based ant routing algorithm for MANETs (LQARA)," in *Proceeding of the 12 th Post Graduate Network Symposium*, pp. 218-223, 2011.

[10] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on aodv based mobile ad hoc networks by dynamic learning method," *International Journal of Network Security*, vol. 14, no. 3, pp. 121-141, 2012.

[11] G. Lackner, U. Payer, and P. Teufl, "Combating wireless LAN MAC-layer address spoofing with fingerprinting methods," T*he Journal of Security and Communication Networks*, vol. 9, no. 2, pp. 164-172, 2009.

[12] N. Nikaein, C. Bonnet, and N. Nikaein, "HARP hybrid ad hoc routing protocol," in *Proceeding of International Symposium on Telecommunications*, pp. 56-67, 2001.

[13] C. E. Perkins, *Ad Hoc Networking*, Addison Wesley, 2001.

[14] R. Ramanathan and J. Redi, "A brief overview of ad hoc networks: challenges and directions," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 20 -22, 2002.

[15] J. Rittinghouse and J. Ransome, *Wireless Operational Security*, Digital Press, 2004.

[16] B. Schneier, *Cryptographie Appliquee Algorithms, Protocoles*, Wiley, 2001.

[17] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Networks*, vol. 13, no. 6, pp. 24–30, 1999.

Benamar Kadri is an associate professor in wireless network security, received his engineer degree in computer science in 2004, and his M.S. degree in 2006 from the University of Tlemcen, Algeria. Finished his PhD in wireless ad hoc networks security and routing in 2010. Member of STIC laboratory in the University of Tlemcen, his recent work is dealing with mobile wireless networks, their security, routing and management.

Djilalli Moussaoui is an associate professor in university of Tlemcen, received his engineer degree from the university of Tlemcen in 2004, and his M.S. degree in 2006 from the same university. Member of STIC laboratory in the University of Tlemcen, his recent work is dealing with mesh networks, their QoS and routing.

Mohammed Feham received his PhD in Engineering in optical and microwave communications from the University of Limoges, France in 1987, and his PhD in science from the university of Tlemcen, Algeria in 1996. Since 1987 he has been assistant professor and professor of microwave and communication engineering his research interest is in telecommunication systems and mobile networks.