MANET - Auto Configuration with Distributed Certification Authority models Considering Routing Protocols Usage

Robson de Oliveira Albuquerque, Maíra Hanashiro, Rafael Timoteo de Sousa Junior, Claudia J. B. Abbas

Universidade de Brasília - Campus Universitário Darcy Ribeiro - Faculdade de Tecnologia - Depto de Engenharia Elétrica e Redes de Comunicação - Laboratório de Redes - sala B1 - CEP: 70910-900 - Brasília - DF – Brazil

Luis Javier Garcia Villalba

Universidad Complutense de Madrid (UCM) - Departamento de Sistemas Informáticos y Programación (DSIP) - Facultad de Informática, Despacho 431- C/ Profesor José García Santesmases s/n - Ciudad Universitaria - 28040 Madrid - Spain

Abstract. In this paper, we discuss about certification, authentication, auto configuration and routing for mobile ad hoc networks (MANETs). The proposal is based on the works of [1] and [3]. We describe distributed certification, MAE authentication, auto configuration process and routing protocols. Then, we show some problems of these models and we propose some solutions considering routing and others protocol modifications.

1 Introduction

Wireless networks are defined as computers networks that are connected to its work area through wireless links, such as radios frequencies and infrared rays. Wireless local area networks (WLAN) arised with the main purpose to overcome the limitations imposed by traditional wired networks, thus permitting faster network installations and mobility.

According to 802.11 [4] standard, established by the IEEE board founded in 1990, WLAN can be sorted in independent networks (Ad Hoc) and access point dependent.

In an infrastructured WLAN (based in access point) all communication among mobile nodes (MN) goes through mobile support stations (MSS) and usually it is directly connected to a wired network. In this situation MN cannot communicate among each other directly.

In Ad Hoc WLAN, refered as Mobile Ad Hoc NETwork (MANET) by IETF, MN can communicate with each other because there is no MSS. In this kind of networks,

de Oliveira Albuquerque R., Hanashiro M., Timoteo de Sousa Junior R., J. B. Abbas C. and Javier Garcia Villalba L. (2005).
MANET - Auto Configuration with Distributed Certification Authority models Considering Routing Protocols Usage.
In *Proceedings of the 3rd International Workshop on Security in Information Systems*, pages 57-66
DOI: 10.5220/0002578800570066

MN does not require any physical infrastructure and nodes can move freely because there is no central communication point.

Ad Hoc WLAN are mostly used in situations where it cannot or does not make any sense, install a fixed wired network, such as disaster situations, hurricanes, earthquakes, where rescue teams needs coordination and communication. Soldiers in a battlefield exchanging tactical information, businessman receiving information in business meetings, students using laptops in classrooms. In a near future, Ad Hoc networks shall have an important paper in wearable computers interconnection, sort of future computer that can be attached to human body, for example, a computer jacket.

An Ad Hoc WLAN can operate isolated or it can be an extension of some wired network already installed, which, in this case, needs a communication gateway to connect each other.

As advantages of MANET it has quickly installation (can be installed in areas with no previous infrastructure because it needs no fixed base to route messages), fault tolerant (any malfunction or disconnection of a station can be easily solved with dynamic reconfiguring of the network), connectivity (if two stations are inside the same area where there is reach of radio waves, there is a communication channel), mobility and others.

Based in RFC 2501 [5], some characteristics and fragilities are important in these networks. These characteristics and fragilities are related to dynamic topologies, restricted bandwidth and variable links capacity, power save consumption operation and limited physical security.

Due to these problems, MANET needs proper specifications related to certification, authentication, configuration and routing.

In this paper some proposals related to certification and auto configuration with routing considerations are presented and fundamented in [1] and [2] developed work. Besides that, some problems are emphasized and possible solutions are shown as considerations and possible solutions related to auto configuration and distributed Certification Authority (CA).

2 MANET routing protocols

Routing protocols are responsible for finding, establishing and keeping routes between MN that wishes to communicate. It is very important that routing protocols in MANET creates very few messages as possible, avoiding network overhead and thus not consuming network bandwidth. These factors are directly connected with the velocity that network routes are established and the frequency that they are updated. Different techniques were developed creating protocols that can create and establish routes faster than others. Others can consume less bandwidth but takes more time to establish a specific route.

According to IETF MANET workgroup (IEEE, 2004), there is a desirable quality list that routing protocols are required to supply with: (a) distributed operation, (b) no routing loops, (c) under demand operations, (d) pro-active operation, (e) security, (f) inactivity period operation and (g) unidirectional link support.

Basically MANET routing protocols can be classified as reactive and pro-active. Pro-active are routing protocols that keep information about routes to every MN in the network. Reactive protocols only create a route when it is requested by origin node.

Four routing protocols are specified by IETF with drafts RFC: (a) TBRPF [6], (b) OLSR [7], (c) AODV [8] and (d) DSR [9]. Where (a) and (b) are considered pro-active routing protocols and (c) and (d) are considered as reactive routing protocols.

Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) creates per hop routing by the shortest path for each destination. Each MN running TBRPF generates a topology information tree based in information topology that is saved in a topology table. To minimize network processing, each MN reports only a few portion of is topology table to neighbor MN. TBRFP uses different combinations and periodical updates to keep every MN informed about its own topology tree. To reach and keep robustness in highly mobile environments in the protocol, each MN can send additional information (complete topology tree) to its neighbors.

Differentiated HELLO messages are used to neighbor discovery that contains only information about neighbor change. This modified message results in shorter messages based in link state algorithm.

TBRPF can be divided into two main modules. The first module is called “neighbor discovery” and the second is called “routing” which does the topology discovery and computes the routes to every destination.

Optimized Link State Routing Protocol (OLSR) has as key concept the use of multipoint relays (MPRs). MPRs are MN selected to forward broadcast messages in the routing protocol flooding mechanism. MPRs are spread throughout MANET to provide every MN the partial information about the necessary topology that computes the best route to every MN in the network. MPRs combined with local duplicity avoidance are used to minimize the number of control packets that should be sent in the network.

OLSR is projected to work in high scalable networks where traffic is sporadic and randomly among specifics MN. As a pro-active protocol, it is also adequate to scenarios where pairs of MN changes very often, but no additional control packet is generated in the network since the routes are kept and known by all possible destination.

Ad hoc On-Demand Distance Vector Routing (AODV) is based in Destination-Sequenced Distance Vector Routing Algorithm (DSDV) protocol. In general AOADV tries to cut off the need of broadcast routing messages, which limits its own scalability. Another important AODV point is that it tries to minimize the latency when new routes are required.

AODV is classified as distance-vector algorithm and is considered as a reactive protocol because only one route is created if it is necessary. In general, AODV tries to eliminate the broadcast routing messages flooding, which limits its own scalability. AODV also tries to minimize latency when new routes are requested. It functions is similar to traditional algorithms what can facilitate the interconnection with wired networks. Even though working very closed to traditional protocols, AODV allows multicast and unicast traffic, however the protocol shows only one route to every destination what cannot be a good characteristic.

Dynamic Source Routing (DSR) is a simple and efficient routing protocol designed to multi-hop MANET with up to 200 MN and supports high mobility rates.

It allows the network to organize and auto configure itself without the network infrastructure administration.

DSR is divided into two main modules: “routing discovery” and “routing maintenance” that work together to permit that MN discover and keep updated routes. All aspects of the protocol work under demand, thus not sending periodical messages to routing exchange information. This characteristic of the protocol allows low network bandwidth consumption and power saving.

DSR also permit multiple routes to a specific destination and that every sender selects and control the used routes to forward its packets. Other advantage of the protocol is that is provides loop-free routing information, supports unidirectional links and fast convergence when the network topology changes.

3 MANET routing protocols

To avoid malfunction in MANET it is necessary security in message routing. Besides in [3, 4] and [11] an authentication service for routing protocols is proposed, where Manet Authentication Extension (MAE) is used and attached to every message in the routing protocol. All necessary information to authentication are included in MAE. The main focus of the proposed model was to keep the routing packets and its messages unchanged. MAE format is shown in Fig. 1.

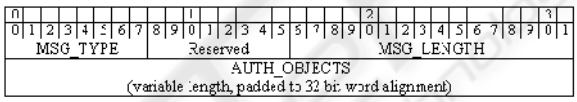

Fig. 1. Mae Syntax

MSG_TYPE field is used to differentiate MAE messages from other routing protocol messages. MSG_LENGTH field indicates the size of MAE in bytes and AUTH_OBJECTS has the objects that have authentication information.

4 Distributed Certification

In MANET, due to its characteristics, is heavily not recommended any centralized service. In [12], [13] and [1] approach a distributed certification model is proposed.

The model proposed uses threshold cryptography theory and pro-active secret key update based in Shamir [14] schema.

In the system point of view, the whole architecture is fully distributed and the service is localized using a coalition approach and the cryptographic system is fully based in RSA model.

It is considered a MANET where every NM v_i has a personal RSA key pair $\{sk_i, pk_i\}$, where $sk_i =< d_i, n_i >$ is the private key and $pk_i =< e_i, n_i >$ is the public key that are used in point-to-point transactions.

A Certification Authority (CA) has a key pair $\{SK, PK\}$, where $SK =< d, n >$ is used to sign all MN certificates. Any certificate in this approach can be verified by the system public key SK, that is know by ever MN in the network.

According to threshold cryptography, SK is divided in the network. Every MN v_i, besides its own key pair, has the partial key P_{vi}. Any subgroup k of n MN can work as a CA. However it is not possible to any MN to know SK, but in the system initialization.

Threshold cryptography is indicated in MANET due to some of its proprieties: (a) the distribution and decentralized control of the keys fits the profile of Ad Hoc networks, (b) security omnipresence is guaranteed since the secret is fully distributed in the network and intrusion detection is more practical and efficient, (c) the limit k is the balance between the service availability and intrusion tolerance. In other words, a group of adversaries need to destroy $(n-k+1)$ partial key holders to bring the system down (once it would block one auto configuration) and at least break k partial keys to steal SK secret.

System is initialization is a very careful step to k choosing. As lower the k value the greater the facility of break SK secret. In other hand the greater the value of k the higher the system security, which reduces fault tolerance at the same time. After all, the most close k is from n, the probability of $(n-k+1)$ MN leaving the network raises, which would forbid the service.

Certificates generated by a CA formed by a subgroup of k MN have the finality of certificate, as in a normal cryptographic system, the public key of every MN. Therefore, every MN has its own $cert_i$ certificate that must be signed by SK, in $< v_i, pk_i, T_{sign}, T_{expire} >$ format, where v_i is the MN identifier, pk_i is its public key, T_{sign} is the signature date and T_{expire} is the expiration certificate date.

To control the certificate validity are used to methods: (a) Implicit certificate revocation that defines that every MN must renew its certificate at least ever period T_{renew} where $T_{expire} \leq T_{sign} + T_{renew}$, (b) explicit certificate revocation where a certificate is assumed by Certificate Revocation List (CRL) is not valid anymore even its T_{expire} is valid. This implies directly that only revoked certificates that did not expire must be in CRL.

This model was implemented in [1] which involves only subgroups, k size, of partial key holders. The basic operations include: (a) secret key negotiation, where the secret key can be obtained by on MN with the system initialization or with the auto configuration service. In the first case, both keys and certificates are distributed to MN by a central negotiator before MANET formation. In the second case, an auto initialization algorithm where k MN can provide a partial key to new MN in the network, (b) the secret key update, instead of changing the system key from time to time, only changes the partial key with the main purpose of protecting the secret key from being broken. The system supports until $k-1$ partial secret breaks because SK is obtained with k keys. If in a update situation there is less than k discovered keys, SK is protected and does not need to be changed, (c) the certification service permits, that when a MN requests using the certification service, one subgroup of k (coalition) partial secret key holders is created and every MN v_i generates a partial signed certificate to the requesting MN. MN then generates its certificate by grouping k received certificates that represents a signed certificate from SK. This service includes emission, renovation and revocation of certificates, besides, even before the MANET formation, a security policy for each step should be defined.

5 Auto Configuration

A MN to communicate in a network must have a unique identifier, usually the IP address. However, in MANET the topology changes dynamically thus creating a difficult environment for centralized administration that can distribute IP address or any other identifier. This situation leads to a distributed, dynamically and automatic service.

Together with security and routing protocols, auto configuration provides a service that can became MANET more efficient and robust. Even though there are many approaches related to auto configuration, none has been standardized.

In [14] is proposed an auto configuration model that uses message authentication considering the distributed CA model in [12, 13] and [1]. In [2] approach a protocol for auto configuration is developed considering a distributed CA, which avoids that any intruder MN can produce messages or even change the messages already created with the purpose to break the protocol or get the service unavailable. To reach this situation in MANET, according to [2], the MN where already configured with a valid certificate before they can request and join the auto configuration service.

Therefore to a MN request an IP address or even respond to MN client solicitation, MN must have a valid certificate. The authentication service of the auto configuration mechanism is supplied by MAE, which has all the necessary information to guarantee authenticity, integrity, non-repudiation in all MAE protected messages.

MAE used for the proposed auto configuration model is the same proposed to protect the routing messages in MANET routing protocols.

As referenced before MAE has authentication objects which includes Digital Signature (DS) that is mandatory and authenticate all non-mutable fields of auto configuration messages. MAE should have one more object, that can be the certificate. The message sender must use DS with its private key because the certificate that goes with MAE has the sender public key that can be used to certify the message sender. If the MN certificate is not locally available, MAE can have a CERT object, which carries with the message the certificate that created and signed MAE. Additional objects are used to provide additional services that are beyond the protocol auto configuration approach.

Every NM that is valid and trustable belonging to MANET has an IP address identifying its interfaces and a subset of free IP address (FIA) to offer to MN clients that wishes do associate to the network.

Inside an individual MANET, A MN FIA must be distinguished from others MN FIA thus avoiding that the same IP address can be distributed by more than one MN, besides that, every MANET has a unique identifier defined as partition ID (PID), which, in this situation permits that to MN that has the same PID are in the same MANET. PID also helps distinguishing different MANET in a specific area and also helps different MANET to be brought together.

Dynamic Configuration Distribution Protocol (DCDP) is used to distribute network configuration information such as IP address, network mask and default gateway, which uses binary division to provide to MN different IP address in the network. Binary division assures that all MN receives distinguished IP address, thus avoiding IP address conflicts even in a MANET join situation.

In [2] to obtain and associate an IP address the MN must have received its valid certificate. When a MN wishes to join a MANET so it can obtain an IP address, it sends an ADDR_REQ message in broadcast using its MAC address as source address.

Any MN belonging to the MANET answers the message with ADDR_REP that contains FIA with the biggest free IP quantity because a MN can have more than one FIA with different quantities. The MN can receive more than one answer from different other MN and then selects the MN that has the biggest FIA sending a SERVER_POOL message directly to the chosen MN server, discarding all other received messages.

The SERVER_POOL message confirms the MN intention of getting an IP address. The elected MN server then divides its FIA, sending one half to the MN that requested it and keeping the other half so it can answer future requests. The MN that received the FIA throughout IP_ASSIGNED message assigns the free IP address in its own FIA. The first IP address the MN uses for itself associating it with its interface and using all the rest as FIA to answers MN client requests.

If a MN has more than on FIA, for security and implementation facility reasons, the MN must mark in which FIA is its own address. The process is finished using an IP_ASSIGNEMENT_OK message to the server MN.

6 Related problems and proposed solutions

In [1] a MANET distributed CA was created and implemented. The proposed model relies in k size. This implies directly that k MN must be reached so a MN can have its certificate signed. If k MN are not reached, the MN cannot join MANET because it cannot sign its certificate. A routing protocol should then be used to reach k MN thus permitting the certificate signature.

Another problem related to k is that it has a fixed value that is defined considering a relative size so that k cannot have a big value (close to the total amount of MN in the MANET) and neither very short size (related to the quantity of MN in MANET). However the size of MANET is highly variable thus implying that an adequate defined k value may become inadequate considering that a MN can leave or join the MANET at anytime.

An initial solution is that k may vary in function of the size of the percentage of the network, but alter k is important define maximum and minimum values (both related to a percentage of the size of the network) of MN in function of the security necessity of the network and these values should be monitored as the quantity of MN in the MANET raise or reduce, thus implying directly that if a minimum or a maximum value is overpast is necessary a redefinition of k. According to the analyses of the results obtained in [1], the value of k can be defined as an average of the maximum and the minimum size.

Considering that k may vary from time to time, the model needs improvements in the CRL because the number of revoked certificates would be much bigger because

the certificates are fully dependent on k. At this point we have the relation that the most k varies the most will be the emission of revoked certificates and the most will be the emission and requests of new certificates. This generates more traffic in the network and thus forcing the MN to process new certificates raising power consumption. Besides the variation of k, as MN enter and leaves the network, the certificates are automatically revoked but new certificates needs a new CA initialization. But according to [1] the process of CA initialization is centralized, contradicting the MANET's necessity.

In [1] model approach, to solve out this problem here presented is necessary the creation of a model of distributed CA initialization that implies in new mathematical models to the generation of a distributed key.

In other hand if k MN has to be reached, these MN can be reached using routing protocols to the signature of a previous requested certificate. This problems requires that a MN can work as a proxy, asking in the MN's name that others $k-1$ MN sign the certificate request. Considering that the proxy MN already has a valid configuration in the network related to IP address it could request the certificate to be signed using routing measures if $k-1$ could not be reached for itself.

Another approach considers that it could be used a temporary IP address to request the certificate signature. This implies that a topology change is required because of the temporary IP chosen by the MN. To solve out this problem a range of IP network address (even in CIDR) could be allocated and announced in the network informing that if a MN wishes to sign a certificate so it can join MANET, it then should use an IP address range reserved to that finality.

Considering this situation OLSR could be used as routing protocols because of its pro-active characteristic, besides the information messages to the reserved IP range could be announced by MPRs. A time-to-live (TTL) should be limited to 2 or 3 hops because is highly probable that $k-1$ nodes could be reached by routing. Another consideration is that it would limit the traffic related to certification signatures.

Another point is that any pro-active routing protocol could be used in this situation because the routing information would be easily created because the IP range would be well-known in the network.

In [2] the distributed CA approach implemented in [1] was used and the routing considerations where not applied limiting the reach of the auto configuration model proposed. This returns to the considered approach pointed herein because in (BUIATI, 2004) is assumed that the MN already has a valid signed certificate. So the proposed solution to [1] can be easily applied in [2].

Another problem in [2] is that the auto configuration model relies in that every message sent in the network is broadcast messages. This process makes the proposed auto configuration model not scalable because in huge MANET the amount of messages would increase significantly creating problems related to unnecessary bandwidth consumption and increasing power consumption by the MN.

To solve out this specific problem the protocol should be changed so that only the first message is broadcasted to reach all close MN. In this message the MAC address of the MN goes with the frame. As the MN server receives the sender MAC address

the other messages in the communication process can be done in the unicast approach thus avoiding the flooding of the network.

7 Conclusions

MANET is increasing highly but some problems should be fixed out due to its characteristics. Related problems about auto configuration, routing measures, distributed CA are increasing as MANET standards are developed.

The approach studied in this paper is related to the problems found in [1] and [2] and the proposed solutions considering routing and others protocol modifications so both models can be more heavily developed and studied.

In [1] approach the proposed solution relies in static k, but in MANET the number o MN cannot be easily predicted. In other hand k is defined considering n. As n increases or reduces, k cannot vary because the whole process needs an initialization to secret key creation that is centralized. This approach was not considered in the implemented model and thus pointed herein to future researches in this subject. The initial proposed solution is based in new idea that relies in a fully distributed CA initialization approach so k can vary according to the necessity of MANET. It is important to say that this model should be heavily studied to validate the proposed solution.

In [1] the routing measures to reach k is not considered because it assumes that k are close of the requesting MN, which in MANET may not be true due to its mobility. An initial proposed solution considers that routing protocols can be used as proxy to reach k MN in order to produce a signed certificate.

In [2] the model is based in broadcasts messages during the whole auto configuration process. This paper proposes that the protocol should be changed in order to avoid unnecessary bandwidth consumption and thus avoiding power consumption. Once the first message is sent the MAC address of the sender can be easily obtained and the consequent communication process can be done using unicast approach.

Both [1] and [2] are heavily fundamented and very well work were developed permitting that new approaches and researches could be conducted using both proposed models in order to allow secure auto configuration and distributed CA in MANET.

References

1. SILVEIRA, F. AND HANASHIRO, M., *Serviços de Certificação para Redes Móveis Ad Hoc*. UnB, Brazil, 2003.
2. BUIATI, F.M., *Protocolo Seguro para Autoconfiguração de Endereços de Redes Móveis Ad Hoc*, UnB, Brazil, 2004.

3. PUTTINI, R.S., ME, L., e SOUZA, R. T. de, *Certification and Authentication for Securing MANET Routing Protocols*.
4. IEEE Standard 802.11, *Wireless LAN media access control (MAC) and physical layer (PHY) specifications*, First edition, 1999-08-20
5. CORSON, S. e MARKER, J., *Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation consideration*. RFC 2501 (informational), IETF, 1999.
6. OGIER, R., LEWIS, M., TEMPLIN, F. e BELLUR, B., *Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), INTERNET DRAFT, MANET working group*, <draft-ietf-manet-tbrpf-06.txt>, November 2002.
7. CLAUSEN, T. e JACQUET, P. *Optimized Link State Routing Protocol, IETF Internet Draft*, MANET working group, version 11, Jul. 2003.
8. PERKINS,C. E., ROYER, E. M. e DAS, S. R.. *Ad hoc on-demand distance vector (AODV) routing*. *IETF INTERNET DRAFT*, MANET working group, Jan. 2002. draftietfmanetaodv10.txt.
9. JOHNSON, D. B. et al, *The dynamic source routing protocol for mobile ad hoc networks (DSR), INTERNET DRAFT*, MANET working group, < draft-ietf-manet-dsr-07.txt>, Feb. 2002.
10. PUTTINI, R.S., ME, L., e SOUZA, R. T. de, *An Authentication Protocol to MANET*.
11. BUIATI, F.M., PUTTINI, R.S. e SOUZA, R.T.J. de, *Secure Autoconfiguration for Móbile Ad Hoc*, 2nd International Information and telecommunication Technologies Symposium I2TS 2003.
12. LUO, H. AND LU, S. *Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks*. Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.
13. KONG, J., ZERFOS, P., LUO, H., LU, S. AND ZHANG, L., *Providing robust and ubiquitous security support for MANET*, IEEE ICNP 2001, 2001.
14. SHAMIR, A. *How to Share a Secret*. Communications of the ACM, 22(11):612-613, 1979.