Rethinking Self-organized Public-key Management for Mobile Ad-Hoc Networks *

Candelaria Hernández-Goya[1], Pino Caballero-Gil[1] and Amparo Fúster-Sabater[2]

[1] Dept. Statistics, O.R. and Computing, University of La Laguna
38206 La Laguna (Tenerife), Spain

[2] Institute of Applied Physics, C.S.I.C., 28006 Madrid, Spain

Abstract. In this paper, the self-organized public-key management scheme proposed for MANETs is considered in order to guarantee that all nodes play identical roles in the network. Our approach involves that the responsibility for creating, storing, distributing and revoking nodes' public-keys is on the nodes themselves. In particular, the methods here described and evaluated are aimed at improving the process of building the local certificate repositories associated to each node in the self-organised model. In order to do it, we face the problem by combining known authentication elements such as the web-of-trust concept, together with common ideas of routing protocols, such as the MultiPoint Relay technique used in the Optimized Link State Routing protocol. Our proposal leads to a significant improvement in the efficiency of the whole model and implies a good trade-off among security, overhead and flexibility. Results of experiments show an important reduction in resource consumption while undertaking the certificate verification process associated to the authentication.

1 Introduction

Lack of fixed infrastructure, highly dynamic topology, heavy constraints in node's capabilities jointly with they spontaneous nature are some of the characteristics of Mobile Ad-hoc Networks (MANETs) that hinder to provide them with security services. A particular example of this situation is the deployment of Public Key Infrastructure (PKI). The proposals in the bibliography related to the previous issue adopt two main approaches: using a distributed certification model or a self-organized scheme.

In the first case, the certification process is underpinned by distributed Certification Authorities (CAs), which use a threshold digital signature scheme and are in charge of issuing and renewing certificates associated to the members of the network. One of the first proposals under this approach was put forward in [1]. There, a group of special nodes, acting as a coalition, were responsible for certification tasks. The main drawbacks of this model are the computational intensive operations required by the threshold application when signing a certificate, and the definition of additional procedures such

* Research supported by the Spanish Ministerio de Ciencia e Innovación and FEDER funds under grant TIN2008-02236/TSI

Hernández-Goya C., Caballero Gil P. and Fúster-Sabater A. (2009).
Rethinking Self-organized Public-key Management for Mobile Ad-Hoc Networks.
In *Proceedings of the 7th International Workshop on Security in Information Systems*, pages 103-110
DOI: 10.5220/0002175401030110

as share refreshing [2]. Also, when dealing with certificate validation, nodes should locate a correct coalition but, depending on the actual network topology and conditions, it might result infeasible.

Consequently, the scalability of the proposal cannot be considered adequate since as network size increases, computational and communication overload increases too. Later on, in [3] and [4], nodes playing special roles are not considered since the CA's secret key used for signing certificates is distributed among all the nodes in the network.

In this paper the self-organised method for public-key management is chosen as base in order to guarantee identical roles for all the network nodes. This approach involves the relocation of the responsibility for creating, storing, distributing, and revoking their public keys to the members of the network.

The method here described and evaluated is aimed at improving the process of building the local certificate repository associated to each node in the self-organised model. This will lead to significant improvements in the efficiency of the whole model. Particularly, as it will be appreciated from the experiments, a reduction in resource consumption while undertaking the verification process associated to authentication is obtained. In order to achieve this aim, we face the problem by combining typical authentication elements with common ideas used in routing protocols in MANETs. In particular, the Optimised Link State Routing (OLSR) protocol from which some ideas regarding the use of the Multi-Point Relay (MPR) technique have been borrowed in order to design the algorithm for updating repositories.

The structure of this paper is as follows. Section 2 is devoted to the description of the MPR technique. Since our proposal is specifically designed to be deployed in the self-organised key management model, section 3 deals with the details of that approach, including the description of the method originally proposed to built such repositories called Maximum Degree Algorithm (MDA). Both the MPR technique described in section 2 together with the graph-based public-key certification protocol described in section 3 constitute the keystones of the proposal. A complete algorithmic description of the method is also provided here. Section 4 describes the results of several computational experiments carried out with the objective of comparing the MPR and MDA approaches. Some questions that deserve more research and the final conclusions are included in last section.

2 Preliminaries

In order to improve the construction of certificate repositories defined in the key management scheme when adopting the web of trust model and the self-organised approach to implement a Public-Key Infrastructure (PKI) we use certain elements of the proactive routing protocol known as OLSR protocol, one of the four basic protocols adopted for MANETs. This section contains an introductory description of this protocol, paying particular attention to the MPR technique embedded in such protocol.

OLSR belongs to the proactive set of protocols. In networks with high mobility these routing protocols have a good behaviour since the paths are re-calculated as soon as a link state change is detected. Building an accurated topological map of the network requires exchange of information among nodes on a regular basis, which can lead to certain network overloading on the network, unless network traffic is sporadic. On the other hand, when dealing with delay-sensitive networks (such as VANETs) the OLSR protocol outperfoms better [5].

Most proactive protocols consider techniques aimed at controlling overhead. In OLSR the technique used is MPR. An example of the important improvements obtained when introducing these procedures is the reduction on redundant packets. It may reach the 60% under some conditions [6].

It can be said that this technique allows determining the minimum number of nodes needed for reaching the whole network when it is recursively applied. This procedure is named as the MultiPoint Relay (MPR) technique. The way we will utilise the basics of this technique in the key management proposal as well as its relationship with Graph Theory problems are included below.

The MPR technique was originally deployed for reducing the duplicity of messages at local level when broadcasting information in a proactive MANET. In general, the number of redundant packets received by a node may be equal to the number of neighbours a node has. In the OLSR protocol, only a subset of nodes will be in charge of retransmitting the received packets. In this way, every node u must define among its direct neighbours a set of transmitters (here denoted by $MPR(u)$) that will be the only ones in charge of retransmitting the messages emitted by the initial node.

According to this method, the choice of the set MPR should guarantee that all the nodes in a two-hop distance of the initial node receive the messages. In order to fulfil this requirement every node in a two-hop distance of u must have a neighbour belonging to $MPR(u)$.

In routing models the network is usually represented with a graph whose vertex set $V = \{u_1, u_2, \ldots, u_n\}$ symbolizes the set of nodes of the network. In this way, for any node u, $N^i(u)$ denotes the set of u's neighbours in a i-hop distance from u. Consequently, $N^1(u)$ stands for u's direct neighbours. These sets are defined by using the shortest path and in such a way that $N^i(u)$ and $N^{i+1}(u)$ are disjoint sets.

With the notation previously introduced the MPR set for a vertex u may be defined as $MPR(u) \subseteq N^1(u) | \forall w \in N^2(u) \exists v \in MPR(u) | w \in N^1(v)$.

The MPR heuristic defined in the OLSR routing procedure uses a greedy approach handling the vertex degree as parameter. The idea is to select the neighbours of the original vertex u which cover the highest number of vertices in u's two-hop vicinity that have not been previously covered.

The greedy heuristic is composed by two main stages stages. In the first one those vertices w in $N^2(u)$ which have an only neighbour v in $N^1(u)$ are examined, in order two include in $MPR(u)$ the vertex v to which is connected. In case there are remaining nodes without covering in $N^2(u)$ those vertices in $N^1(u)$ which cover more vertices in that situation are also included in $MPR(u)$ in the second stage.

Analyzing the description of the problem from the Graph Theory point of view, it can be concluded that the node being examined and its MPR set must form a dominant set in its level 2 vicinity. A dominant set in a graph is a vertex subset such that any node in the corresponding graph has and edge linking it to a vertex in the dominant set.

3 Key Management in MANETs: Self-organized Model

In the bibliography we may find two main alternatives for the deployment of PKI in MANETs: distributed certification authorities, and self-organized public-key management model.

In this work we decided to follow the self-organized key management model based on the web of trust approach. Several are the reasons that justify the choice of this option. First, this model demands less maintenance overhead. Secondly, it is well worth remarking that on the one hand the self-organized approach eases the use of a simple bootstrap mechanism and on the other hand all the nodes perform equal roles.

The self-organized model in MANETs was initially described in [7]. Its authors put forward the substitution of the centralized certification authority by a self-organized scenario where certification is carried out through chains of certificates which are issued by the nodes themselves. Such a scheme is based on the information stored by each node and the trust relationship among neighbour nodes.

In this model public keys and certificates are represented as a directed graph $G = (V, A)$, known as *certificate graph*. Each vertex u in this graph defines a public key linked to a node, and each arc (u, v) symbolizes a certificate associated to v's public key, signed by using u's private key. Each node u has a public key, a private key, and two certificate repositories, the updated (G_u) and the non-updated repositories (G_u^N). Initially the updated certificate repository will contain the list of certificates on which each node trusts (out-bound list) and the list of certificates of all the nodes that trust on u (in-bound list).

When a certificate for a node u is issued by a node v the edge (v, u) is added to the certificate graph and each node u and v stores it in its in-bound and out-bound list, respectively.

In the original proposal two ways of building the updated certificate repository G_u of a node u were described:

1. Node u communicates with its neighbours in the certificate graph.
2. Node u applies over G_u^N an appropriate algorithm in order to generate G_u after checking the validity of every single certificate.

The selection of the certificates stored by each node in its repository should be done carefully in order to satisfy at the same time two requirements: limitation in storing requirements, and usefulness of the repository in terms of ability to find chains for the largest possible number of nodes.

The algorithm used in the construction of the updated repositories will influence in the efficiency of the scheme, so it should be carefully designed. The simplest algorithm for that construction is the so-called Maximum Degree Algorithm (MDA), where the criterion followed in the selection of certificates is the degree of the vertices in the certificate graph.

When using the MDA, every node u builds two subgraphs, the out-bound subgraph and the in-bound subgraph, which when joined generate the updated certificate repository G_u. The out-bound subgraph is formed by several disjoint paths with the same origin vertex u while in the in-bound subgraph u is the final vertex. The starting node is u and $deg^{+}(u)$, $deg^{-}(u)$ stands for the out-degree and the in-degree respectively of node u. The number of chains to be found is represented by c.

Note that the process to build the in-bound subgraph is equivalent to it except for the fact that in this case the edges to be chosen are always incoming edges.

In this paper it is proposed to substitute the MDA algorithm proposed for the updated repository construction by a new algorithm that uses the MPR. In this way, for each vertex in the certificate graph we have to define a re-transmitter set. Hence, the smallest number of vertices required for reaching the whole certificate graph will be obtained.

In order to extend the notation used in 2, which is required to be used in the certificate graph, we denote by $N_i(u)$ the set of predecessors of node u that may be found in an i-hop distance.

The algorithm proposed is an iterative scheme and it can be summarized as folllows. First, node u starts by calculating $MPR(u) = \{v_1, v_2, \ldots, k\}$. Then, these vertices are included in G_{out} together with the edges $(u, v_i), i = 1, 2, \ldots, k$. Henceforth, nodes v_i in $MPR(u)$ apply recursively the same procedure of retransmitting backwards the result $MPR(v_i)$.

The certificate chains required in the authentication are built by using the arcs $(u, MPR(u))$. After that, $\forall v \in MPR(u)$ and $\forall w \in MPR(v)$ the arcs (v, w) are also added after having checked that they have not been added in previous updates.

Note that the procedure every node $u \in G$ has to develop in order to build $MPR(u)$ takes $1 + ln(N^2(u))$ steps when no bound is defined on the length of the chains to be built. Otherwise, the number of iterations to be carried out is given by the number of hops to explore in the certificate graph. As for the definition of the aforementioned bound, it has to be remarked that such a parameter may be dynamically adjusted in function of the changes experienced by the certificate graph. This may be justified by the fact that as the network evolves, the information contained in each node's repository is more complete.

Thanks to this substitution the generated procedure is easier and more efficient, guaranteeing in this way that each node has a set of neighbours that allows it to reach the biggest number of public keys. One of the main advantages of the proposal is that all the information gathered for the construction of the chains is locally obtained by each node.

After obtaining the in-bound ($MPR_{G_{in}(u)}$) and out-bound ($MPR_{G_{out}(u)}$) subgraphs, both are merged and the initial repository (G_u) is generated. When a node u needs to check the validity of the public key of another node v, it has to find a certificate chain from itself to v in the graph that results from combining its own repository with v's repository. If this chain is not found there, the search is extended to $G_u \cup G_u^N$, what implies the inclusion of u's non-updated repository in the search. If this second exploration is successful, u should request the update of those certificates that belong exclusively to G_u^N. When no path is found, the authentication fails.

4 Experimental Results

This work proposes the application of the MPR technique in the computation of certificate repositories included in the self-organized public-key management model proposed by [7]. Our proposal is supported by the good results obtained when using the MPR procedure in the $OLSR$ routing algorithm in MANETs as well as computational experiments. A detailed description of the implementation and the results provided by it is presented in the current section. The main goal of the experiments was showing that applying the MPR technique when building certificate repositories in the self-organized approach instead of using the MDA heuristic provides the public-key management scheme with simplicity and efficiency.

4.1 Implementation Characteristics

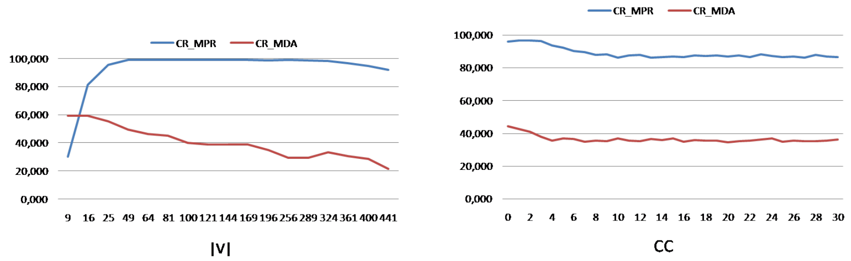
The implementation has been carried out using Java and the open source library JUNG 2.0 (Java Universal Network/Graph Framework) which provides the basic tools for representing and dealing with graphs. One of the reasons why JUNG was selected was having the possibility of working with random graphs with the small-world property. When a graph follows the small-world model, it is assumed that its paths have a small average length and a high Clustering Coefficient (CC). The CC corresponds with the average of the fraction of pairs of u's neighbors (taken over all the network nodes $u \in |V|$) which are at the same time direct neighbors of each other.

This characteristic is supported by certificate graphs as it was shown in [8]. When a graph holds this feature, most nodes may be reached by a small number of hops from any source node. This kind of graphs has received special attention in several scientific disciplines. The particular small-world model used in the simulation developed was proposed by Kleingberg [9]. When generating a graph with $|V| = n^2$ vertices according to this model, the first step is to create an nxn toroidal lattice. Then each node u is connected to four local neighbours, and in addition one long range connection to some node v, where v is chosen randomly, according to a probability proportional to $d^{-\alpha}$. d denotes the lattice distance between u and v and α stands for the CC. Generating the graphs following this model guarantees that the shortest paths may be determined using local information, what makes them particularly interesting for the networks we are dealing with.

4.2 Computational Results

The computational experience consisted of generating random graphs according to the Kleingberg's model where the size of the graphs $|V|$ ranges in the interval $[9, 441]$, the CC takes values between $[0, 30]$. For this parameters, the Certificate Rate obtained by MPR (CR_{MPR}) jointly with time consumption (t_{MPR}) expressed in seconds were measured.

For analyzing the MDA alternative, it is applied over the same input graphs using as specific parameters the maximum number of chains to built (n_{chains}) and their maximum length (C_l) is bounded by 7. In this case, the Certificate Rate in the repository (CR_{MDA}) and time consumption (t_{MDA}) were also obtained.



(a) $|V|$ (b) CC

Fig. 1. Comparing certificate rates.

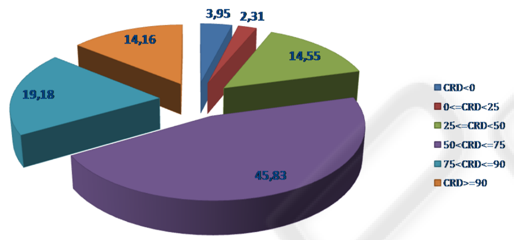


Fig. 2. Certificate Rate Difference.

From this experience, there are some general conclusions that may be remarked. The certificate rate CR_{MPR} finally contained in the local repository increases as the size of the graph increases. However the behavior of the certificate rate is not affected by the growth of the CC (). This phenomena may be better appreciated in figures 2(a) and 2(b), respectively. Additionally, the maximum length in the chains obtained by MPR are kept at reasonable values, what makes the chain verification process lighter.

Probably the most important fact when comparing the certificate rates CR_{MDA} and CR_{MPR} is that only in the 3.95% of the executions the MDA algorithm outperforms MPR, and it only occurs when the input certificate graph is small (see figure 2.(a)). Although, in the previous figure it seems that the difference between both certificates rates is reduced as the size of the graph increases, it should be taken in mind that MANETs have a limited number of nodes. Furthermore, in the the 45.83% percent of the problems the difference between the certificate rates CR_{MPR} and CR_{MDA} is in the interval $[50\%, 75\%]$.

Hence, it may be conclude that the repository built by MPR provides further information to facilitate the authentication process. Another result that illustrates the positive characteristics of MPR to solve the problem of updating the certificate repository is that in the 82.45% of the executions the repository built by MPR contains more than the 75% of the whole certificate set.

5 Conclusions

The application of the Multipoint Relay Technique in the process of building the updated certificate repository has been evaluated in the present work. For the assessment of this alternative several experiments over an implementation developed in JAVA have been carried out. According to these experiments the alternative presented outperforms the original one in several aspects. Probably the more relevant are the significantly higher certificate rate included in the repository when applying the MPR-based method as well as the generation of shorter chains. This first characteristic results in less interaction among nodes at the time of building an authentication chain. The second fact leads to a more efficient verification procedure.

Our immediate goal is to adapt the implementation developed to the network simulator NS2 in order evaluate the behaviour of the method with different mobility models.

References

1. Zhou, L., Haas, Z.: Securing ad hoc networks. IEEE Networks, 13 (1999) 24–30
2. Narasimha, M., Tsudik, G., Yi, J.: On the utility of distributed cryptography in P2P and MANETs: The case of membership control. In: Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP'03), IEEE (2003) 336–345
3. Luo, H., Lu, S.: Ubiquitous and robust authentication services for ad hoc wireless networks. Technical Report TR-200030, Dept. of Computer Science, UCLA (2000)
4. Kong, J., Zerfos, P., Luo, H., Lu, S., Zhang, L.: Providing robust and ubiquitous security support for mobile ad-hoc networks. In: International Conference on Network Protocols (ICNP). (2001) 251–260
5. Haerri, J., Filali, F., Bonne, C.: Performance comparison of AODV and OLSR in VANETs urban environments under realistic mobility patterns. In: Med-Hoc-Net 2006, 5th IFIP Mediterranean Ad-Hoc Networking Workshop, Lipari, Italy (2006)
6. Ni, S.Y., Tseng, Y.C., Chen, Y.S., Sheu, J.P.: The broadcast storm problem in a mobile ad hoc network. In: MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, New York, NY, USA, ACM (1999) 151–162
7. Capkun, S., Buttyan, L., Hubaux, J.P.: Self-organized public key management for mobile ad hoc networks. Mobile Computting and Communication Review, 6 (2002)
8. Capkun, S., Buttyan, L., Hubaux, J.P.: Small worlds in security systems: an analysis of the PGP certificate graph. In: Proceedings of The ACM New Security Paradigms Workshop 2002, Norfolk, Virginia Beach, USA (2002) 8
9. Kleinberg, J.: The small-world phenomenon: An algorithmic perspective. In: Proceedings of the 32nd ACM Symposium on Theory of Computing. (2000)