Authentication in Ad hoc Networks: A Case Study[1]

Candelaria Hernández-Goya

Abstract: *In the cryptographic scenario authentication protocols play an important role since privacy and integrity are secondary when guaranteeing the identity of the correct addressee is not feasible. In this paper we will try to call attention to the importance of this kind of cryptographic tools in the emergent technology of ad hoc networks. The alternatives for authentication in this setting will be introduced and some of their weaknesses will be pointed out. Wireless networks may be considered as one of the last breakthrough in Computer Science. Nevertheless, we will point out the lack of robust procedures for security in this environment, particularly regarding node authentication. This area of research is at the moment one of the most dynamic in Cryptology.*

Key words: *Ad Hoc Networks, Cryptography, Authentication.*

INTRODUCTION

There is no great consensus when defining Mobile Ad hoc Networks (MANETs) but in this paper we will focus on short-term formed networks where the nodes collaboratively manage themselves. The set of restrictions associated to computational, communication and power supply resources present in this environment is the main barrier when providing them with security mechanisms.

Nevertheless, there are also other intrinsic features in this setting that increase this difficulty. The mobility of the nodes produce continuous nodes insertions and deletions and so, incessant instances of the authentication protocol are developed. As a result, designing scalable solutions [1] here is a must. Furthermore, it should be borne in mind that there is not any fixed infrastructure, so the security solutions should admit that legitimated nodes carry out all the required tasks, including routing and entity authentication, in a self-organized way. Other handicap to consider is related to the limitations on the network transmission range. Hence, to develop secure routing mechanisms is of vital importance [2] .

In [3] the authors include the following guidelines to take into account when designing ad hoc network protocols. First, the computational steps and their cost must be kept to a minimum in order to save battery power. Since it is assumed that there is certain homogeneity among the characteristics of the nodes it is also important to balance the computational burden among nodes. Finally and as may be expected, the number of messages exchanged and their length are parameters that should be chosen with proper care.

The rest of the paper is devoted to the description of different solutions for the ad hoc setting remarking their limitations and weaknesses. The paper ends with the conclusions and future work section.

AUTHENTICATION IN MANETs

It can be said that there are two main approaches to solve the authentication problem in ad hoc networks. These two groups of cryptographic techniques are defined using the basic classification used in Cryptology, which distinguishes between secret and public key methods.

[1] This work is partially supported by Spanish MEC under grant SEG2004-04352-C04-03 PROPRIETAS

The solutions included in the first group are not many and they are recommended for sensor networks as the devices forming these networks are even more constrained in their resources. Additionally, the problem of key distribution is difficult to overcome, being physical contact the most simple and extended solution [4]. Also, the authentication scheme implemented in the Bluetooth technology fells into the secret key class. Bluetooth is a short range wireless connectivity standard designed to allow wireless communication among diverse devices such as mobile phones, Palm, Pocket PC, etc. Here, the authentication is based on introducing a PIN in the devices and carry out a weak challenge-response protocol. Then, a shared key of length 128 bits is generated. The block cipher SAFER+ is used during authentication. Nonetheless it is catalogued as a non-scalable procedure for large environments. At the same time, the fact that only the device is authenticated but not the user is consider another drawback. The second approach, methods based on Public Key Infrastructure (PKI), are the most studied so far. The literature about the subject is mainly focused on how to use public key cryptography and how to manage public key certificates in this restricted ambience [5] [6, 7].

Among the available possibilities to implement PKI in ad hoc networks, the easiest way is to employ a globally trusted centralized Certification Authority (CA). Nevertheless, this approximation should be discarded as it will hinder scalability. The main obstacle is that the access to this entity may provoke a bottleneck, slowing down the communications among member of the network since it is compulsory connecting with the CA each time that to verify a certificate is needed. Jointly with the previous reasons, it should be considered the fact that having the certification service centralized may produce that the deployment of DoS attacks will be more effective and attractive. Mention should also be made of the complexity added to the routing process in the presence of this entity.

All things considered then, the most natural modification is to distribute the CA task among a set of nodes. In this sense, in [8] the authors put forward that the CA's functions will be developed by a set of special servers included in the network. These servers will sign the public key of the nodes trough a (t,n) threshold signature scheme [9]. In this way, each time a component of the network B wishes to communicate with one of his peers A, he should contact with t+1 servers in advance in order to obtain A's public key signed with the CA's secret key. In this proposal, the signature of the requested public key is generated by one of the servers involved in the previously mentioned coalition, playing the combiner's role. However, some difficulties still exist. First, the combiner figure and the servers acting as certification authorities produce system congestion as all the requests should be attended for them. Additionally, introducing special servers does not guarantee the eradication of vulnerabilities to DoS attacks. As for the storage requirements, it should be pointed out that the public keys of all the members of the network must be stored by the servers, which entail considerable memory needs. Another handicap to be faced by any user is the need to have t + 1 servers available in its transmission range. Apart from the aforementioned hindrance, the explanation of how the users are authenticated by the servers for the first time is not tackled in the paper.

The methods included in [10] and [1] solve some of the preceding problems through the removal of the servers. In both, any group of t+1 nodes without distinction may act as servers at the moment of issuing certificates. Consequently, one of the mayor advantages of this strategy is the balance in the distribution of the computational load among nodes. Although this characteristic has particular significance in MANETs, a number of remarks need to be made. Firstly, a distributor in charge of providing credentials to the first nodes

should be considered during the bootstrapping stage. Secondly, finding a valid coalition each time a certificate needs to be verified may result infeasible depending on the network actual topology and conditions. Besides, the methods in [10] do not provide any instrument to protect against malicious nodes when they send fakes shares.

A third alternative implementation of PKI was outlined in [7]. Here the authors deploy principles similar to the ones used by PGP. In this framework, each node B may sign the certificates associated to those peers with whom originally he share a trust relationship. From here on, each node generates a certificate repository that is merged with the repository corresponding to its neighbours when the authentication involves a user whose credentials are not included in B's repository. This combination will form trust chains among nodes in order to validate the public key. All this procedures are described using what the authors call certificate graph as model enabling in this way the use of graph algorithm in the construction of optimal trust chains.

To some extent it is true to say that it can be stated that this solution is the most robust so far, but there were factors which arguably may be considered as limitations. A first inconvenience regards the certificate repositories, their construction is not efficient, and they are expensive to create. As we have pointed out, the verification tasks are more complicated than the ones carried out in other approaches. On the other hand, when the community where the method is applied is limited (allowing to guarantee the truest relationships), this alternative turns out to be viable.

The proposal presented at [11] also makes use of PKI. The innovation is that the network is divided into trusted subgroup (members of the same group trust each other) and members of the same group share a pair of keys. A different key pair is shared among all the members of the network. In order to accomplish the authentication, it is essential the existence of a head group with greater computational capacities. Once more, it is considered a negative aspect since again it will produce an imbalance in the computational load of the nodes.

Assuming that the major deterrent regarding the use of PKI in ad hoc networks is certificate management, there are some works [12] where the use of PKI without using certificates is vindicate. So as to achieve it the public key of all the nodes involved should be exchanged through a location-limited channel, solution that is only applicable in small networks.

Given that none of the mentioned solution has been satisfactory, it is logical to think of hybrid methods where symmetric and asymmetric tools are combined. An exemplification of these methods may be found in [13, 14]. In this work, a protocol based on passwords is presented. Unfortunately, the operations to develop in this protocol are too heavy to be implemented in ad hoc networks**.**

After analyzing the authentication procedure proposed to date for MANETs, it can be deduced that the central barriers that still have not been solved are the following:

- Certain infrastructure is required in order to support the certificates associated to the nodes.
- The computational requirements are in general considerable.

- When an adversary is able to control a determined subset of nodes, the network is completely compromised.
- The reauthentication processes are almost as expensive as beginning the authentication again.

Trying to avoid these difficulties the use of advanced protocols such as Zero Knowledge Interactive Proofs is advisable. The application of these protocols in MANETs is still a novel research area, and it is considered as a promising one [15], [11], [16]. Nevertheless, there are no new published proposals specifically designed for this framework hitherto.

CONCLUSIONS AND FUTURE WORK

After the journey through authentication protocols and focusing in our case study: ad hoc networks, we found that there is not a satisfactory solution yet. More work is needed to address the problem of admission control in peer groups as well as in the design of advanced and low-cost protocols.

REFERENCES

1. Haiyun, L., et al. *Self-Securing Ad Hoc Wireless Networks*. in *Proceedings of the Seventh IEEE Symposium on Computers and Communications (ISCC '02)*. 2002.
2. Royer, E. and Toth, C.K., *A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks.* IEEE Personal Communications Magazine, 1999: p. 46-55.
3. Hoeper, K. and G. Gong, *Models of Authentications in Ad Hoc Networks and Their Related Network Properties*. 2004.
4. Stajano, F. and Anderson. R., *The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks*. in *Proceedings of the 7th International Workshop on Security Protocols*. 1999.
5. Luo, H. and Lu, S., *Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks*. 2000.
6. Capkun, S., Buttyan, L. and Hubaux, J.P., *Self-Organized Public-Key Management for Mobile Ad-Hoc Networks.* In IEEE Transactions on Mobile Computing, 2003.
7. Capkun, S., Buttyan, L., and Hubaux, J.P., *Self-Organized Public-Key Management for Mobile Ad-Hoc Networks*. 2003.
8. Zhou, L. and Haas, Z., *Securing Ad Hoc Networks.* IEEE Networks, 1999. **13**: p. 24--30.
9. R.Gennaro, et al., *Robust threshold {DSS} signatures*. Advances in Cryptology - EuroCrypt '96, ed. M. Ueli. 1996, Berlin. 354--371.
10. Kong, H., et al., *Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks,* in *International Conference on Network Protocols (ICNP)*. 2001. p. 251-260.
11. Sankar, K., *Securing Authentication and Privacy in Ad Hoc Partitioned Networks*. Symposium on Applications and the Internet Workshops {(SAINT'03} Workshops). 2003, Orlando, Florida. 354.
12. Balfanz, D., et al., *Talking To Strangers: Authentication in Ad-Hoc Wireless Networks*. In Symposium on Network and Distributed Systems Security {(NDSS} '02). 2002, San Diego, California.
13. Kaminsky, A., *Infrastructure for Distributed Applications in Ad Hoc Networks of Small Mobile Wireless Devices*. 2001.
14. Jonathan, K., Rafail, O. and Moti, Y., *Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords*. Advances in Cryptology - EUROCRYPT 2001. 2001.

15. Alan, K., *Infrastructure for Distributed Applications in Ad Hoc Networks of Small Mobile Wireless Devices*. 2001.
16. Pirzada, A.A. and McDonald, C., *Establishing Trust In Pure Ad-Hoc Networks*. 27th Australasian Computer Science Conference, Volume 26, ed. V. Estivill-Castro. 2004, Dunedin, New Zealand. 47 - 54.

ABOUT THE AUTHORS

Assoc. Lecturer. Candelaria Hernández-Goya, PhD, Department of Statistics, O.R. and Computing, Universidad de La Laguna, Phone: +34 922 318 637, ?-mail: mchgoya@ull.es