Enhancing Name Resolution Security in Mobile Ad Hoc Networks

Javad Pashaei Barbin[1] and Mohammad Masdari[2]

[1]*Computer Engineering Department, Islamic Azad University, Naghadeh Branch, Naghadeh, Iran*
[2]*Computer Engineering Department, Islamic Azad University, Urmia Branch, Urmia, Iran*
Javad.pashaei.barbin@gmail.com, m.masdari@iaurmia.ac.ir

Abstract

Name systems provide easy communication in large networks and relieve the network users and administrators from remembering long network addresses. But mobility, limited lifetime of user nodes and dynamic situations of MANETs make it impossible to use conventional NAME systems such as DNS on these kinds of networks. Numerous name systems are designed and proposed for MANETs, but most of these system are insecure and do not provide secure name services for upper layers. Name resolution is one of the main operations of that are conduct by client nodes to achieve the requested bindings from name systems. Vulnerability of MANETs to various security attacks, make it clear the need for a secure and reliable name resolution to protect the users against different security threats. In this paper, we present a solution to provide users with secure binding information that can use for secure name resolution. This solution is not dependent on any name systems and can be used with any previously designed naming scheme to enhance the security of name resolution even in offline state and link failures.

Keywords: *Name System, Authentication, Digital Signature, Resolver, Name Server*

1. Introduction

A mobile ad hoc network or MANET is a collection of mobile nodes that can dynamically form a network that does not rely on any infrastructure. In these networks each node has limited power and CPU resources and connects to other nodes by wireless links. Generally, a name system makes it possible to assign names to network's nodes and resources. Also, it makes the communication easier and provides various name management facilities. Internet uses DNS or domain name system for providing name resolution and other name related operations. However, it cannot be used in MANET, because DNS is designed for supporting large number of long-lived bindings in a hierarchical name space. But most MANETs may only need flat name space for supporting limited number of MANET nodes which may leave the network more frequently than Internet and other conventional networks. Thus MANETs require special type of name systems. However characteristics such as mobility, lack of any infrastructure and inherent problems of wireless communications, make it hard to implement and operate a complete and scalable name system. Numerous solutions have been proposed for managing user defined names in the MANETs. In the [1], we analyzed the naming solutions and classified them solutions according to their architecture into centralized, fully distributed and hybrid schemes. Each of these architectures exhibit name server nodes distribution over MANETs. For example, in centralized schemes there is one name server

node that provides name services to all MANET. Although, this method has availability problem and became single point of failure, it is efficient and has lower overhead than other schemes. In fully distributed method, there is no name server and every node is responsible for all of name related operations. Thus each node must register its own name, find name conflicts, answer name resolution requests and etc. The other kinds of name systems are partially distributed methods which uses multiple name servers that are distributed throughout the MANET. In these schemes, data distribution method is very important and affects the performance and availability of name to address bindings. Replication techniques are also used in these solutions to provide higher performance and availability, thus one binding may be in different parts of the network and users can access the bindings that are closer to them.

From security perspective, MANET name systems can be classified into secure and insecure categories. But although MANETs are very prone to security attacks, most of the proposed solutions are insecure [2-19] which do not support security options and only one secure scheme is designed by Jeong, *et al.*, [5]. In MANETs that lack any security protections, attacker can launch various attacks and prevent proper operation of MANET Applications. Name resolution process is one of the critical operations that attackers can use it to launch security attacks in all kinds of networks. For example an attacker can prevent normal communication between valid users by redirecting user requests to the wrong destinations. The main security problem of existing MANET name systems is that we cannot trust on the information that is supplied by other systems and they can be sent by anyone even attackers. In addition, although privacy is one of the important properties of every secure application, it is not needed in secure name resolution process and authentication of binding information source is enough for our purpose. This, requirement can be achieved by digitally signing the name resolution message by name servers.

In this paper, we briefly analyze the proposed secure name systems for MANET and present a solution for conducting secure name resolution in MANET. Although, it can be used in all kinds of networks, it is especially good for ad hoc networks which suffer from link failures and disconnections more often. The rest of this paper is organized as follows: in the Section 2, we describe the security problems of name resolution in MANET. Previous research related to name system security is described in Section 3 and in Section 4 classify insecure MANET name systems and propose security protocols for each of them in Section 5 and 6.

2. Related Work

Internet uses Domain Name System Security Extensions or DNSSEC protocol to protect the name resolution process in RFCs 4033, 4034, 4035. RFC 3833 specify some of the known threats to the DNS protocol and describe how DNSSEC responds to those threats. All answers in DNSSEC are digitally signed but not encrypted. By checking these signatures DNS resolvers can check that information is from the authoritative DNS server. But, DNSSEC not appropriate for MANET environments, because it requires online connections to the servers which can be guaranteed in MANETs.

For MANET, Jeong, *et al.*, [5] have presented a secure solution, called ANS or Ad Hoc Name Service System. It can provide secure name-to-address resolution and service discovery. As Figure 1 shows in ANS System, each node consists of ANS Responder that works as DNS name server and ANS Resolver.

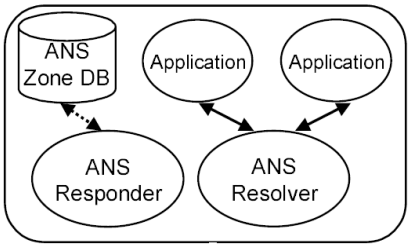

Figure 1. Name System Components in ANS

In this solution, Mobile node registers an AAAA type DNS Resource Record (RR) of combining its unicast address and host DNS name with DNS zone file of its ANS Responder. An application over mobile node that needs the name resolution can get the name service through ANS Resolver. ANS Resolver of mobile node A sends DNS query in ANS multicast address, which all ANS Responder should join for receiving DNS query. ANS Responder, after checking that is responsible for the query, decides to respond to it. Then it sends the appropriate response to ANS Resolver in unicast. But this scheme is limited to IPv6 protocol and is applicable only in small and connected MANETs.

Consequently, there is a need for special purpose name resolution solutions for MANET that be able to operate even in offline and disconnected states which may be caused by transient or permanent link failures.

Table 1. Acronyms and Abbreviations

Acronym	Expansion
NS	Name system
SBL	Secure Binding Lists
SNL	Secure Name Lists
DCA	Distributed Certificate Authority
IDS	Intrusion Detection System

3. Our Proposal

The main technique that we propose for secure name resolution is secure binding list. A secure binding list is a signed list of bindings that is produced by name system and can be published like CRLs or certificate revocation lists. This is an important solution that can be used in centralized and partially distributed name systems. In this scheme we public key cryptography and assume the existence of certificate authority system that issue the user requested certificates and manage them to support secure applications.

3.1. Distributed Certificate Authorities

In MANETs, a special type of certificate authority are used which called distributed certificate authorities or DCAs. Many schemes have been proposed for providing distributed Certificate Authority services in MANETs that we have analyzed them in [20, 21]. In Distributed Certificate Authorities or DCAs the CA's private key is distributed to a number of shareholding DCA nodes. However, the public key of the DCA will be known by all network's nodes and will be used to verify signatures of certificates issued by the DCA. In issuing or revoking digital certificates, threshold of available shareholding DCA nodes

participate to perform the required task. Distributed Certificate Authorities can be categorized as partially or fully Distributed Certificate Authorities. In Partially implemented DCA or PDCA, services of the certificate authority are performed by a set of specialized server nodes using secret sharing. Each of these nodes can generate partial certificates and a client can create a valid certificate by combining enough number of these partial certificates. In this case, these special server nodes must have high energy and the inherent heterogeneity of the nodes in network is utilized to choose the candidates for CA nodes. However, if all the nodes in MANET were identical, the nodes of the distributed CA might be chosen randomly. Implement and operating a Distributed Certificate Authority is an overhead that should be tolerated for using our solution. However, a Distributed Certificate Authority is one of main components of PKI and it is necessary for implementing other security dependent application. So, it overhead is divided among all application that uses it.

3.2. Secure Binding Lists

In this solution we propose that each name server produce a list of its binding and sign it with its private key. We call the produced list as Secure Binding List or SBL. Secure Binding Lists enable user nodes to conduct name resolution operation even at the presence of link failures, network partitioning and disconnection from name servers. As Figure 2 shows, our solution can be used to conduct hybrid name resolution. In this kind of name resolution, binding data are received as SBL from remote or other name servers to local name servers and resolver. Although, downloading these lists may consume bandwidth of network, but we can consider only special nodes for receiving these lists and publish name lists just to these nodes. These special nodes can decrease the name resolution traffic and relieve name server in high name resolution loads. After local name server checked the signature of remote name server's signature on SBL, it can respond to its users' requests by this information. For achieving higher performance, the communication between user nodes and local name server can be conducted in non-secure form. Generally, for using SBLs we must answer to these questions:

- Should SBLs be published or pulled by user requests?
- To which node they must be delivered? Must they be delivered to special MANET nodes or all of nodes can request it.
- How they must be updated? Should we use Delta SBLs or other methods?
- How nodes that receive SBL must distribute its content to other user nodes?
- Which methods can be used to increase SBLs scalability? Like Geographical SBL.

For the creation of Secure Binding Lists we have to consider the following issues:

- Who should create the SBLs?
- How they should be created? Should they be created by traffic patterns or they must be other technique.
- When should it be created?

For creation of SBLs we can have several options, as follows:

- In small MANETs these Lists can be created by name system itself.

- In Large MANETs they can be created by special security components which aid the name systems and we call them SBL Responders.
- In a hybrid method, when name severs have low processing loads then each of them produces these lists itself. But at the high loads, name server can determine one of its trusted neighbors for production of a name system.

For answering the second question we may have the following options:

- They may be created periodically.
- They may be created based on some events.
- They may be created periodically and based on some event.
- They may be created based on the number of Delta SBL that has been issued.

For example, when name servers can predict a network partitioning, they can produce new SBLs to support the offline and secure name resolution operations. But the question is that binding of which nodes must be added to the SBL?

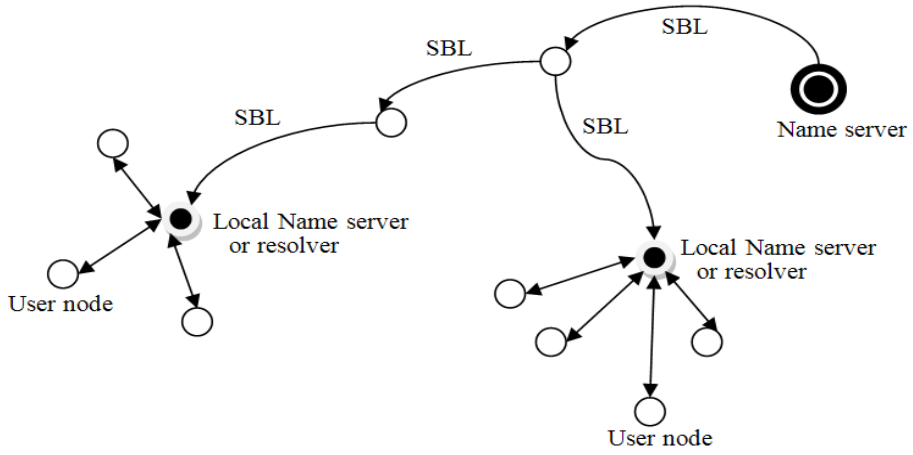

Figure 2. Hybrid Name Resolution in MANET

We may have the following options:

- Bindings of all MANET nodes.
- Bindings of all partitioned nodes.
- Setting some special bits that a partitioned has happened.

The structure of a Secure Binding List will include the following items:

- Reason of SBL's issuance.
- An Identification Number.
- Identity of issuer
- Name to address binding for each user node.
- Signature of name server that has issued the SBL on the SBL's hash.

In the Figure 3, structure of a SBL is shown. For providing other services to user nodes we can add other attributes to the SBLs. Although, this additional features increase the size of SBL, this will result in total decrease of messaging overheads. For example, in the applications that position of nodes is required, we can add users' geographical position to the SBLs.

When some nodes want to achieve a Secure Binding Lists, it must ask it by sending a request message that may contain the users queried names. For achieving more performance and reliability in SBL requesting process, we can send request to multiple name servers; however this method increases the name resolution overheads and should be used carefully.

In large scale MANETs SBLs may have large size.

After SBLs requested, they should be somehow transferred to the local name servers. Transferring large SBLs consume high amount of network bandwidth and for decreasing SBLs bandwidth overhead consumptions, we should consider the following items:

- A scheduling must be done so that distribution of SBLs does not interfere with other MANET activity.
- Name server must use transfer SBLs based on the path of requested nodes. Thus if multiple nodes have common path, then we send multiple SBL in one message.

3.3. Updating SBLs

A mobile ad hoc network is a dynamic network and nodes may join and leave the network more frequently than conventional network. Thus, SBL's information maybe stale very soon. Two approaches can be used to alleviate this problem. First for increasing validity period of binding lists entries we could specify some conditions for adding binding data to lists. For example, we can add stable node's bindings to SBLs. Second, we should update the SBLs by issuing Delta SBLs. Generally, after the SBL issuance, two types of events can be happened:

- Some node may join the MANET.
- Some node may leave the MANET.

These events must be detected and informed to the other network nodes. Thus for creation of Delta SBL we should consider the following items:

- How these events are detected?
- Who should detect these events?
- Who is responsible for the creation of these Delta SBLs?
- How these Delta SBLs must be deployed to the MANET nodes?
- Which information should be included in the Delta SBLs?
- When we should use different types of Delta SBLs?
- How these updates must be distributed?

First we deal with the events detection. Although, finding the new nodes is not so hard and a name system can detect them easily, detection of dead nodes is not easy and a name system must use a garbage collection method. In large scale MANET's, we can create two kinds of Delta SBLs, one for newly joined nodes and the other for nodes that have leaved the MANET. With this classification user nodes can obtain the information that they actually require them, this reduce bandwidth overhead and less information is transferred for node's operations. But,

in Small MANETs for decreasing the overhead of sending a Delta SBL we can combine both kinds of them. For deploying Delta SBL we can have the following options:

- We can publish it to all user nodes.
- We can publish it just for subscribed user nodes.
- Or user nodes may ask name system for each kind of Delta SBL.

Contents of these lists depend on the type of Delta SBLs. As mentioned in previous section, a Delta SBL can have the following data:

- Bindings of newly joined nodes.
- List of nodes that have leaved the MANET.
- Both of them.

Thus we must consider two special bits in the Delta SBL request messages to indicate the type of information that is placed at the Delta SBL. For receiving the Delta SBLs from name servers, a node must send a request to the name system. With Delta SBL, the secure name resolution can be conducted in two phase. In the first phase, some nodes request the SBL from name system and subscribe for the Delta SBLs. Then it receives the SBL from the name system. This node, verify the signature of name system on the SBL and the use it.

SBL ID	Identity of issuer	Reason of SBL's issuance	Name to address bindings	digital signature of name server on SBL

Figure 3. Structure of SBL

When any changes have been made to the base SBL, this node can receive the published Delta SBL. Some times before connecting some node, we want to examine its existence. This service can be achieved by the use of SNLs or Secure Name Lists that only contain the name of the network nodes and determine that such nodes are existed on MANET.

3.4. Increasing Security

For providing higher level of security, the monitoring and intrusion detection systems can be used in combination with name system. Then name servers can exclude the nodes that are added to the black lists. It is obvious that the communication between the name system and intrusion detection systems must be conduct in secure manner. This communication can be done in the SBLs and Delta SBLs creation phase.

The other operation which increases the security of our name resolution process is the checking validity of SBL's signing certificate. Generally, there are two main certificate verification methods that are used in the Internet and other networks. These methods are:

- OCSP (Online Certificate Status Protocol)
- CRL (Certificate Revocation Lists)

Each of these verification methods has its advantages and disadvantages. For example, OCSP based methods need online connections to OCSP responders and cannot operate in offline conditions. However, this problem is alleviated by using caching nodes in schemes such as ADPOT[xx]. Also, this method, consume little amount of network bandwidth because, it just need to achieve the status of just one certificate. In addition the security of OCSP based

methods is higher, because they provide more accurate information about status of some certificate. CRL based methods need more bandwidth and consume limited resource of MANET but it support offline states and can be even used in partitioned MANETs. For decreasing bandwidth overhead of this method, solutions such as delta CRL and xxx have been proposed. Because these methods cannot be used purely in MANET environments, many schemes have been proposed to adapt them to MANET characteristics.

3.5. Overheads

Secure name resolution process incurs the processing overheads, messaging overheads and storage overheads to MANET. Processing overheads are incurred to nodes which produce or use the SBLs and Delta SBLs and nodes that check the signature of SBLs and Delta SBLs. Also, storage overheads are created by storing the certificate of nodes and their related status. In this solution, we need storage for the following items:

- Secure Binding Lists
- Delta SBLs.
- Secure Name Lists

But messaging overheads are tolerated by all nodes which cooperate in forwarding these data structures. This is caused by increase of name resolution messages length, because a digital signature must be added to each name resolution messages. Also, additional messages must be sent for certificate status checking. The overhead of name resolution request which are transmitted between client node and local name server is computed by the following equation:

$$NR_{Req\_Size} * Dist_{Client\text{-}to\text{-}LNS}$$

Where NR_{Req_Size} is the size of name resolution request message and $Dist_{Client\text{-}to\text{-}LNS}$ is the distance between client node and local name server. When this request is received by local name server and there is not any binding for the requested name, then it create a SBL message and forward it the other name server that know. The overhead of this message can be computed from the following equation:

$$\frac{[(SBL_{reqheader} + \sum_{i=1}^{n} name_i) * dist * Reliability_{factor}]}{R}$$

Where $SBL_{reqheader}$ shows the size of SBL's header and *name* represents the users requested names. $Reliability_{factor}$ is the factor that shows the degree of redundancy in sending same request to multiple name server nodes and *dist* is the distance between name servers. Also, *R* is the request rate which is issued for bindings existed in the SBL and the overheads of SBL is divided among these requests. The SBL messages which are returned by name servers will have the following overhead:

$$\frac{[(SBL_{header} + \sum_{i=1}^{n} binding_i) * dist * Reliability_{factor}]}{R}$$

Where $binding_i$ is the size of *ith* binding in the SBL. After name servers receive the SBL can respond to the nodes:

$$NR_{Res\_Size} * Dist_{Client\text{-}to\text{-}LNS}$$

Where NR_{Res_Size} is the size of name resolution responses and $Dist_{Client\text{-}to\text{-}LNS}$ is the distance between nodes to name server.

One of the important parameters in the before mentioned equations is the $Reliability_{factor}$. In normal condition this factor is set to 1, but when we want to achieve some SBL more quickly, we can increase this factor. For example, assume that communication delay be Δt for contacting a name server. If we do not receive any response and try *n* other servers serially, then we will have $n*\Delta t$ delay. If the probability that first server had the requested binding be *P*, then we found the requested binding in the *nth* server with the following probability:

$$P * (1 - P)^n - 1$$

On the other hand, if we send n simultaneously request for SBL to n name servers, then the probability that we achieve some result increase and can be computed for the following equation:

$$\sum_{i=1}^{n} P_i$$

Although, this method increase the chance of getting a positive responses but it increase the messaging factor by $Reliability_{factor}$.

4. Conclusion

Security and availability are two main problems in MANETs. Conducting secure name resolution in such environment is challenging issue, because connection to name server maybe lost and numerous security attacks may be launched by internal and external attackers. In this paper, we proposed a solution for offline secure name resolution. This solution uses a data structure called SBL or Secure Binding Lists that are created by name servers. They can be downloaded from name servers and even at the absence of connection to the name servers, can be used for conducting secure name resolutions. SBLs decrease the loads of security related operations on the name servers and distribute loads on the other nodes.

References

[1] M. Masdari, M. Maleknasab and M. Bidaki, "A survey and taxonomy of name systems in mobile ad hoc networks", Journal of Network and Computer Applications, **(2012)** March.
[2] P. Engelstad, D. V. Thanh and T. E. Jonvik, "Name Resolution in Mobile Ad-hoc Networks", 10th International Conference on Telecommunications, **(2003)**, pp. 388 – 392.
[3] S. Ahn and Y. Lim, "A Modified Centralized DNS Approach for the Dynamic MANET Environment", 9th International Symposium on Communications and Information Technology, **(2009)**, pp. 1506 - 1510.
[4] M. Nazeeruddin, G. P. Parr and B. W. Scotney, "An efficient and robust name resolution protocol for dynamic MANETs", Ad Hoc Networks journal, vol. 8, Issue 8, **(2010)**, pp. 842-856.
[5] J. Jeong, J. Park and H. Kim, "DNS Name Service based on Secure Multicast DNS for IPv6 Mobile Ad Hoc Networks", the 6th International Conference on Advanced Communication Technology, vol. 1, **(2004)**, pp. 3–7.
[6] X. Hong, J. Liu and R. Smith, "Distributed Naming System for Mobile Ad-Hoc Networks", Proceedings of ICWN, **(2005)**, pp. 509-515.

[7] T. Zahn and J. Schiller, "MAPNaS: A Lightweight, Locality-Aware Peer-to-Peer Based Name Service for MANETs", the IEEE Conference on Local Computer Networks, **(2005)**, pp. 500-501.
[8] Y. M.Gottlieb, R. Chadha and K. E. Cheng, "MOSS: gathering names in networks of mobile nodes", IEEE Military Communications Conference, **(2008)**, pp. 1- 6.
[9] J. Jeong, J. Park and H. Kim, "Name Directory Service based on MAODV and Multicast DNS for IPv6 MANET", IEEE 60th Vehicular Technology Conference, vol. 7, **(2004)**, pp. 4750 – 4753.
[10] P. Hu, P. L. Hong and J. S. Li, "Name Resolution in On-demand MANET", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, **(2005)**, pp. 462 - 466.
[11] J. Jeong, J. Park and H. Kim, "Name Service in IPv6 Mobile Ad-hoc Network connected to the Internet", 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, **(2003)**, pp. 1351 – 1355.
[12] C. Jelger and C. Tschudin, "Underlay Fusion of DNS, ARP/ND, and Path Resolution in MANETs", 10th Scandinavian Workshop on Wireless Ad-hoc Networks, **(2011)**.
[13] J. H. Jeong, J. S. Park and H. J. Kim, "NDR: Name Directory Service in Mobile Ad-Hoc Network".
[14] M. Aoki, M. Saito, H. Aida and H. Tokuda, "ANARCH: A Name Resolution Scheme for Mobile Ad Hoc Network", Proceedings of the 17th International Conference on Advanced Information Networking and Applications, **(2003)**, pp. 723-730.
[15] R. Morera and A. McAuley, "Adapting DNS to Dynamic AD HOC Networks", IEEE Military Communications Conference, vol. 2, **(2005)**, pp. 1303 - 1308.
[16] P. Engelstad, D. V. Thanh and G. Egeland, "Name Resolution in On-Demand MANETs and over External IP Networks", IEEE International Conference on Communications, vol. 2, **(2003)**, pp. 1024–1032.
[17] A. Derhab and N. Badache, "Data replication protocols for mobile ad-hoc networks: a survey and taxonomy", IEEE Communications Surveys & Tutorials, **(2009)**, pp. 33 – 51.
[18] P. Padmanabhan, L. Gruenwald, A. Vallur and M. Atiquzzaman, "A survey of data replication techniques for mobile ad hoc network databases", VLDB Journal Springer, **(2008)**, pp. 1143–1164.
[19] S. Chesire and M. Krochmal, "Multicast DNS", Internet Draft, draft-chesirednsext-multicastdns-06.txt, **(2005)** June 7.
[20] M. Masdari, S. Jabbehdari, M. Ahmadi, S. M. Hashemi, J. Bagherzadeh and A. Khadem-Zadeh, "A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking, **(2011)**.
[21] M. Masdari and J. Pashaei, "Distributed Certificate Management in Mobile Ad Hoc Networks", International Journal of Applied Information Systems, **(2012)** November 6.