ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Name Management in Wireless Ad Hoc Networks: A Comprehensive Analysis

Javad Pashaei Barbin
Computer Engineering Department,
Islamic Azad University, Naghadeh Branch, Naghadeh, Iran,
Javad.pashaei.barbin@Afagh.ac.ir

***Abstract*:** Ever growing use of wireless devices has increased the demand for use of wireless ad hoc networks. Name systems provide easy communication for network users and many name related solutions have been designed and proposed to provide name services in different types of MANETs. In this paper, we analyze and discuss about the various proposed name systems for ad hoc networks. Then the properties, advantages and limitations of each name system are illuminated. This analysis is of high importance to understand the weakness of existing name systems and designing effective and complete name systems. Finally, we conclude with open research issues.

Keywords: Name System, Name Resolution, Replication, Name Server, Conflict Resolution.

I. INTRODUCTION

A Mobile Ad Hoc Networks or MANET is composed of a collection of mobile devices that use wireless links for multi-hop communications. Generally, MANETs have no predefined infrastructure and only rely on each device for routing and other network services. These kinds of networks have no centralized administration and are self-configuring and self-organizing. In addition, each mobile node has limited resources such as battery, processing power and storage. Over recent years, mobile ad hoc networks have attracted a lot of researches and many efforts have been made to provide easy and reliable communication in these kinds of networks. Name systems are one of the key elements that make access to various network resources and make it more transparent. Each network uses it to assign user friendly names to network's nodes and resources. They provide facilities for storing name to address bindings and the required software's for handling name related queries. After a name system has been installed and start to operate, user nodes and network applications can use

All network-based application needs name resolution for proper operation and presenting their services to network users and applications. Internet and other conventional network use DNS for registering, name resolution and name management schemes. It is an application layer protocol which uses a distributed database of name to address bindings that are spreaded all over the Internet. These bindings contain the IP addresses of important hosts which other user and network hosts need to access them. DNS can provide more scalability and reliability to network, by distributing the request loads on multiple replicas of sites and hosts. But, because of special characteristics of mobile ad hoc networks we cannot use DNS to provide name related services to network nodes. For example:

a. DNS uses special nodes as name servers that virtually have unlimited power, storage capacity and processing power but mobile ad hoc networks is a self-configuring, infrastructureless network of mobile devices and lacks any fixed servers and each node have limited capacity.
b. DNS name servers are always available in conventional networks but mobility of network nodes and other problems such as link failures and network partitioning disconnect the MANET and make the name server nodes often inaccessible.
c. DNS register bindings of servers that deliver services for a long time, but MANET users have short lived and may join and leave the network more frequently.
d. DNS maintain the requested bindings for long periods in its caches. The time for which a resolver caches a DNS response is determined by a value called the time to live or TTL that is associated with every record. But, in MANET node have short lifetime and caching the name resolution results may refer to dead nodes. Thus, setting the right value for TTL fields and detecting and clearing the invalid cached entries are a challenging problem.
e. DNS is supported by various security protocols such as DNSSEC [1-3] that guarantees the authenticity of bindings and other transferred data between DNS resolvers and servers. But MAENT's nodes are connected by wireless links which are more susceptible to security attacks and mobility of these nodes makes the situation even more severe. Also, these conditions cause attacks such as Sybil attacks that are nonexistent on internet.
f. DNS uses bindings that are unique and each binding has different name and IP address, unless we want to implement load balancing and redirecting users to different server for a domain name. However, selected names and IP Addresses can have conflict with each other and we cannot guarantee full uniqueness for names and IP Addresses at the presence of link failures and network partitioning.

Because of the above described features, special schemes are required for adaption to the dynamic situations of MANET. As a result, numerous schemes have been designed to implement name related services in ad hoc networks. This paper analyzes various solutions that are recently designed to present name services over wireless ad hoc networks. It provides a detailed discussion about the each category of naming schemes and their overheads and performances. Furthermore, it discusses about the security

and areas that can be subject to further research. Therefore, our aim is to provide a better understanding of the current research issues in this field which can be used in designing new name related solutions.

The remainder of the paper is organized as follows: the difference between Name Resolution and Name System is defined in section 2. Then desirable functions and capabilities of a complete MANET name system are described in section 3. Finally in section 4, we compare the various capabilities of each proposed name system and specify the advantages and disadvantages of each solution in detail.

II. NAME RESOLUTION VERSUS NAME SYSTEM

Each naming scheme presents different set of services for different kinds of MANET. Thus, we can classify them according to their capabilities and services. Therefore we may have the following categories:

a. Name resolution schemes
b. Name systems schemes

Name resolution schemes assume that network nodes have registered their names somehow and they present only a solution for translating hostnames to IP addresses. These schemes often use reactive routing protocols for conducting name resolution process. Therefore, overhead of name resolution operation are decreased by multipurpose broadcast. On the other hand, name systems are more sophisticated and support numerous name related operations and services. They also, handle various events and situation which can be occurred in dynamic environment of MANET and often combine with other MANET services to reduce their messaging and storage overheads.

On Internet and other conventional networks, client software which is called resolver is used for translating domain names to IP addresses. It is responsible for contacting the distributed database of DNS that ultimately lead to full resolution of requested the fully qualified domain. However, as we mentioned in section one, it cannot be used in Mobile Ad Hoc Networks. Therefore, some special purpose schemes have been designed for MANETs that have not the capabilities of registering and maintenance of name-to-address bindings, but perform name to address translations. In this section, we discuss about request and response distribution methods in name resolution schemes. In [4] masdari et al, classify the request distribution methods in name resolution schemes. Figure 1 shows this classification:

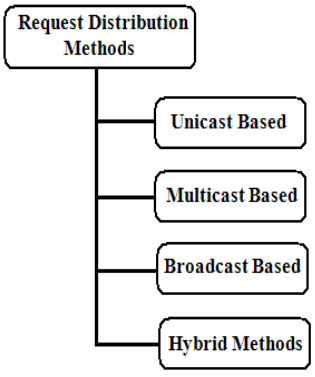

Figure 1: Name Resolution Request Distribution Methods

The easiest way for sending name resolution request is request broadcasting. Although this method has the highest probability of getting a response from network nodes, it has high messaging overhead. This overhead is increased when multiple users simultaneously try to resolve names and it may bring the network down. However, this method has the lowest response time. Schemes such as [5-7] use broadcast based request distribution method. Also, scheme [8] uses this method when it finds no name server and operates in hybrid mode. This method is not scalable and cannot be used in large scale MANETs. Therefore, some schemes propose to use limited flooding which has lower overheads. But it has the risk of finding no response, because the destination node may be out of the broadcast range. If the requested binding is founded in the limited broadcast range then it is obvious that overhead of limited broadcast is less than full broadcast, but as the degree of broadcast factors and retries are increased its overheads increases. In worst case, overhead of limited broadcast is more than the full broadcast. However, for using limited broadcast, the following issues should be considered:

a. How the broadcast limit should be determined for the first time? Should it be fixed or variable?
b. How much the broadcast factor should be increased in every step?
c. How the waiting window should be increased by increase of broadcast factor?
d. How many retries should be made for limited broadcasts?

Although some schemes proposed to use limited broadcast for name resolution process, none of them have presented a solution for the before mentioned questions and they can be considered in the future researches and works.

Scheme [8] is one of the schemes which use multiple methods for name resolution operation. In the best condition it uses unicast method for the request distribution method. As it fails to receive a response, it changes the request distribution method. Schemes such as [5], [6] and [7] can be considered as fully distributed systems. These schemes are on-demand name resolution systems that apply broadcast-based query distributions. Finally, the node that has authority on the requested name sends a unicast response. For decreasing the overheads of broadcasts, this approach is applied with reactive routing protocols such as AODV and DSR. So, each name query is piggybacked on the RREQ message and the corresponding response is piggybacked on a unicasted RREP. Almost in all name resolution schemes response messages are send as unicast message to requesting node. But because most of the proposed schemes send name queries in broadcast or multicast form, multiple unicasted messages may be received simultaneously at the source of name query. These response messages may cause high amount of collisions and traffics, the problem that is called response implosion. This problem worsens when some nodes send multiple name queries simultaneously to the MANET. This solution increases the response time of requests and does not guaranty to solve the situation at all.
The problem of response Implosion can be solved by the following two methods:

a. Random back off method
b. Data aggregation method

Random back off method uses the idea of random delays for prevention of high traffic and collisions. So when a node

wants to respond, it first waits for a random amount of time and then responds. However, it increases the delay of name resolution operation especially in link failures and interferences. The other solution of response implosion problem is data aggregation method, which combine the response of name resolution requests. However, it also may increase the delay of name resolution process and may not be effective in fully disjoint paths. But, in dense network which many links have been established between MANET nodes, aggregation methods decrease the traffic. Anyway, none of the proposed methods have used it for distribution of request and response messages. Thus, future studies are needed to prove the effectiveness of data aggregation methods on prevention of problems such as response implosion.

III. RESPONSE MESSAGES

When user nodes forward the name resolution responses, they can cache them for handling future requests. Caching of binding data increases the availability of name-to-address translations. It also increases the efficiency of name resolution operation and decreases its messaging overhead. Therefore, user requested bindings can be extracted from name owner node or the caches of other nodes. For example, when multiple responses are received by the response of name owner should be prioritized over the response of other nodes which cached that binding. Although, these two sources of binding data differ primarily, no proposed scheme differs between these two situations. The importance of this issue increases as the collision and conflict of name happens with network partitioning and link failures. Unfortunately, these problems are increased by increasing of cache size. Therefore, although we achieve more availability of binding data with more caches, more overhead of cache maintenance and response implosion are incurred to network. However, none of the proposed methods have studied on the effect of cache size on the network overheads. Also, none of the name related schemes present an optimal size for cache which can be considered as an open issue for future researches. DNS cache poisoning is a security or data integrity compromise in a Name System. It occurs when the bindings that are introduced into name broker's cache did not originate from authoritative nodes.

When a name broker received such non-authentic data and caches it for performance optimization, it is considered poisoned. It then supplies the non-authentic data to other nodes. On internet and other fixed networks, DNSSEC can prevent cache poisoning attacks with the help of digital signatures, nut it cannot be used in Mobile Ad Hoc Networks. Adaption of DNSSEC to MANET environment is an open issue and can be considered in future researches.

IV. NAME SYSTEM SCHEMES

Numerous name systems have been designed recently which are able to operate in different kinds of mobile ad hoc networks. Each of these systems tries to deliver their services with different solutions and approaches and have advantages and disadvantages. Generally, these systems can be categorized as centralized, fully distributed and partially distributed name systems [4]. Each of these architectures exhibits the distribution of name servers over network and is appropriate for different size of MANET. In this section, we illustrate these naming schemes and compare them.

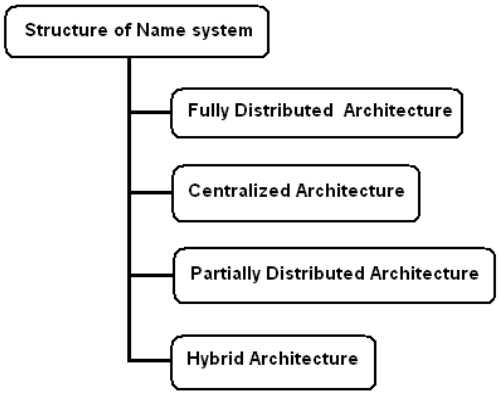

Figure 2: Structure of MANET Name systems

In centralized schemes, there is one name server node that provides name services to all MANET. This method is efficient and has lower overhead than others, but it has availability problem and became single point of failure. In addition, if an attacker can compromise this node, naming service in entire MANET will be affected. In [9] ahn et al., present a modified centralized dns called Manet DNS. It supports various name management operations and tolerates the merging and partitioning of ad hoc network. In this scheme when a node wants to acquire the DNS server address, it broadcasts a server solicitation message and then the DNS server or an intermediate node unicasts a DNS server advertisement message. Besides, each node registers its domain name to the discovered DNS server by sending a DNS register message.

In partially distributed methods, there are multiple name servers distributed throughout the MANET which often are called name brokers. Data distribution method is one the important factors that affects the performance and availability partial distributed name systems. In this method, we can use replication techniques to provide higher performance and availability. Thus one binding may be in different parts of the network and users can access the binding which is closer to them. Numerous partially distributed name systems have been proposed for MANETs, for example in [8] Nazeeruddin et al., have designed MANET Naming Service or MNS that is integrated with any statefull auto-configuration protocol and reuses the directory structure of autoconf protocol. In this scheme, resolver runs in basic and hybrid modes and interacts with external DNS servers for name resolutions of external hosts. Furthermore, in [10], Morera et al., present a method to adapt DNS to dynamic ad hoc networks that requires no change to the standard domain name space and existing DNS software.

The most radical change is to replace the static DNS roles and linkages with automatically configured ones. In addition, in [11] Hong et al., propose another partially distributed Name System that is called ADNS. It uses a redundant server structure to balances the registration and query load and provides service robustly in the presence of mobility and node failures. In ADNS, the name space is considered to be flat and different names have different subset of servers that are selected among the network members through clustering algorithms. Figure 3 shows the

name lookup operation in centralized and partially distributed name systems.

In fully distributed name systems, there is no name server and every node is responsible for all name related operations. Therefore each node must register its own name, find name conflicts, answer to name resolution requests and etc. Since these schemes use multicast or broadcasting in most of their operations, they are not scalable and cannot be used in large scale MANETs. Although flooding can be done in limited form, it has the risk of finding no response.

ANARCH is a distributed name system that is presented in [12] by Aoki et al and uses flat name space. It provides network nodes with unique user oriented names and exchanges control messages between nodes in one hop area that calls it core region. When a node starts joining the ANARCH, it propagates its name to the core region using a HELLO message, and collects HELLO messages sent by other nodes into an ANARCH Name Information List. These lists include mapped information between names, IP addresses, MAC addresses and hop numbers to the node.

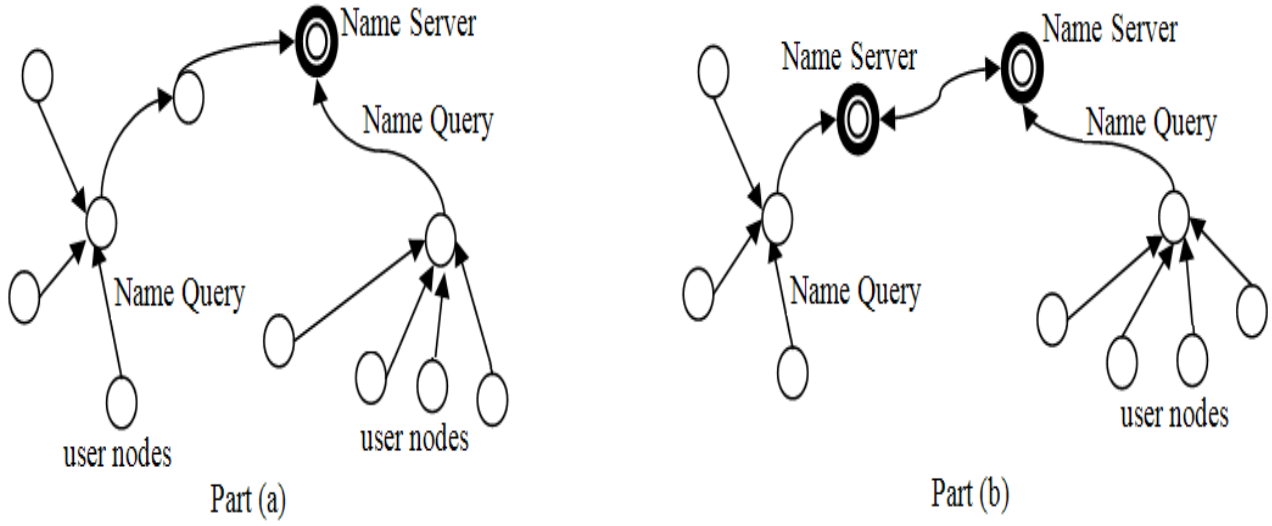

Figure 3: Part (a) Centralized name systems, Part (b) Partially distributed name systems

Also, in [13] Jelger et al., present a fully distributed name resolution scheme for MANET that uses IPv4 for operations such as name resolution, and IPv6 for neighbor discovery and routing path establishment. The other distributed scheme that is evaluated in this paper is MOSS. It is presented by Gottlieb et al in [14] and allows a set of nodes to provide name service which is resilient to node movement and reconfiguration. A MOSS-enabled node upon entering a network joins a multicast group responsible for resolving the node's name. Then the node can respond to DNS queries for its name. Every node in the network is both a server and a client and receives a query; it first checks to see if the name being resolved is its own then it responds with a unicast packet.

In [15] Jeong et al., propose another name service that supports IPv4 and IPv6, which is called name directory service or NDR. It can solve address conflict that may be caused by the repetitive partition and the merge of ad-hoc networks.

IV. NAME RESOLUTION IN NAME SYSTEMS

Address lookup is a user initiated operation that returns the IP address of user specified name. Because name systems distribute and manage the binding data themselves, they can use more effective methods for name resolution process. Figure xx shows various approaches which have been used for distributing name resolution requests. Each proposed name system applies different solutions for each of the operations that are specified in this figure.

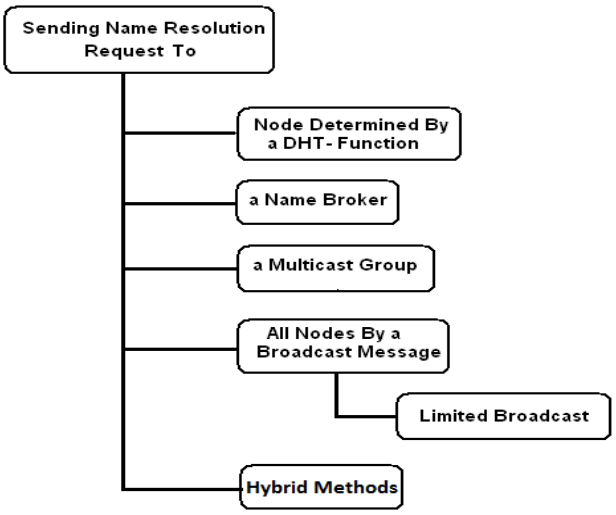

Figure 4: Request Distribution Methods

Figure 4 shows that some name systems use Dynamic Hash Tables for providing better performance in name resolution. DHT-based try to make the name resolution more efficient but

In [16], when source *A* wants to communicate with node *N*, it uses a hash function H to calculate the indexes of N's name servers. Then it uses the indexes to gather all of node *N*'s name servers and chooses the closest server and sends the query message. In case of a tie, i.e., more than one server has the same closest distance, *A* randomly picks one. Upon receiving a failure message or experiencing a query timeout, *A* turns to a less close server.

For example in [17] Zahn et al., propose MAPNaS or Mobile Ad-hoc Peer to Peer Name Service that runs on top

of MADPastry, a general-purpose DHT. In MAPNaS, every node keeps the network addresses of the resources that are identified by a unique resource key mapped into the logical MADPastry id space. In addition, each node advertises its own resources that must be shared through MAPNaS. When some node such as A wants to make a local resource available to other nodes, it assigns a hash key to that resource.

Large scale MANETs which are based on centralized or partially distributed architecture, rely on the name brokers for almost all name related operations. Each proposed name system uses different method to find these brokers. For example, in schemes such as [9] when a node wants to acquire the address of DNS server, it broadcasts a DNS server solicitation message, then the DNS server or an intermediate node unicasts a DNS server advertisement message back to the source node. Afterwards, it sends a DNS query message to the DNS server which provides the naming service by transmitting a DNS name response message. These name query and response are transmitted via unicast messages so they have less overhead than other methods. However, this scheme presents no efficient solution for selecting more appropriate node as name server for example node that has more power or more processing capacity. Thus, it can be investigated in future researches and studies.

In partially distributed schemes such as [11] and [8] that contain multiple name broker nodes, various policies can be used in partially distributed name systems for forwarding name queries. For example name queries can be forwarded to the closest broker or to the less busy brokers. In Addition, in partially distributed name systems with active replication, it is not enough to find just one name server instead, we should find specific number of servers.

In partial distributed systems such as [8], name system operates in Basic and Hybrid modes. In basic mode, the Resolver completely depends on the name server. Resolver first checks whether the requested name is in the local MNS cache. If the required name is found with a valid CLT then the Resolver immediately returns the IP address. Otherwise the Resolver forwards the request to its NS and starts a NRQ Timer. If a valid response is received from the NS, then the Resolver extracts the IP address from the response and forwards it to the requesting application. If the timer expires and no response is received, the Resolver re-sends the request to its name server until a response is received or the number of retries exceed a predefined number. If there is no response, the resolver forwards the request to the NSpid. If the NSpid also does not respond and the total number of retries exceeds rmax, the Resolver sends the error message to the application notifies autoconf module about the absence of NSpid and terminates the request process. In highly dynamic MANETs in which a node does not have any accessible NSs, hybrid mode is used. In table 4, we have specified the overheads of different name resolution operation.

Since fully distributed name systems do not have any special name server node, name resolution requests must be broadcasted until a cached result found or the node that own the name respond to this name resolution request. In other solutions such as MOSS [14], each node has a set of mappings between domain names and multicast addresses. The mappings define the addresses of the servers that are authoritative for a given domain and a node requires these mappings to use MOSS.

V. SECURITY ISSUES IN NAME RESOLUTION

Because of wireless communication properties, MANETs are susceptible to various security attacks.

Name resolution process is one of the critical operations that attackers can use it to launch security attacks on Internet and Mobile Ad Hoc Networks. For example an attacker can direct users to wrong destinations and prevent normal communication between valid users. The main security problem of existing name systems is that MANET nodes cannot trust on the bindings that are supplied by other nodes. The binding information that is received by a node can be sent by anyone even an attacker. Thus, we just need to ensure the integrity and authenticity of received bindings.

The following two methods can be used for securing the name resolution process:

a. Cryptographic-Based approaches
b. Trust-Based approaches

These methods use public key cryptography techniques for providing the required security. For example, ensuring authentication and integrity of received bindings only digitally signing of bindings is enough. However, these solutions incur the overhead of operating and maintaining a PKI solution in Mobile Ad Hoc Networks. Generally, for providing a Cryptographic-Based secure name service we require the following items:

a. A Certificate Authority for issuing, managing and revoking the public key certificates.
b. A Certificate validation method for verification of certificate status.

In Mobile Ad Hoc Networks a certificate authority can be implemented by the following methods:

a. Centralized CA
b. Distributed certificate authority
c. Fully distributed, Self-issuing certificates.

In these solutions, fully distributed method can be recommended for small MANETs. Centralize and distributed certificate authorities can be applied in larger and heterogeneous MANETs which may have some special nodes with high processing and bandwidth capacity. In [18, 19] masdari et al, have analyzed various DCA solutions that are designed for MANET. Distributed Certificate Authorities distribute the private key on multiple nodes and coalition of some nodes is required for all certificate authority operation. Therefore, they are more secure against attacks and compromise of members. In addition, its overhead is divided among all security dependent applications. Generally, cryptographic based name resolution schemes may have the following steps:

a. Name resolution
b. Checking the signature of response message with the corresponding certificate.
c. Checking the certificate status of node that has signed the message.

Although, these steps are necessary for almost every secure name resolution, their overheads can be decreased by using cached results and other techniques. Generally, in a secure name resolution protocol we have the following overheads:

a. Messaging overheads which are caused by adding digital signature to name resolution messages and

sending additional Certificate status checking messages.

b. Storage overheads that are caused by storing the certificate of nodes and their related status.

c. Processing overheads which are incurred to the Source and destination nodes for signing and checking the signature of bindings.

For implementing a trust-based name system, we need a trust or reputation management system. Numerous trust based security schemes are designed for Mobile Ad Hoc Networks. In [20] Cho et al, present a survey on the various trust management solutions for MANET. However, no scheme has been proposed to use trust and reputation factors for providing secure naming services. Therefore Trust-based name systems can be investigated in future studies and researches.

VI. CONCLUSION

In this paper, we analyzed various proposed name systems for mobile ad hoc networks. Although some studies have been done in the context of name resolution in MANETs, most of these schemes are designed for flat and small MANET and there is still lack of large scale name systems for large MANETs. In addition, security is one of the items that have not been considered in almost all of the schemes, so we have a lack of secure name service that can operate in hostile environments and provide secure name management service to upper layers and applications. Also, except dynamic hash tables, other data distribution methods and the impact of push based and hybrid methods on naming system have not been studied. Therefore, in our future works we will try to design a secure name system that tolerates various security attacks of malicious users.

VII. REFERENCES

[1]. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC 4033: DNS Security Introduction and Requirements, March 2005.

[2]. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC 4034: Resource Records for the DNS Security Extensions, March 2005.

[3]. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC 4035: Protocol Modifications for the DNS Security Extensions, March 2005.

[4]. M.Masdari, M.Maleknasab, M.Bidaki, A survey and taxonomy of name systems in mobile ad hoc networks, Journal of Network and Computer Applications, March 2012.

[5]. P.Engelstad, D.V.Thanh, T.E.Jonvik, Name Resolution in Mobile Ad-hoc Networks, 2003, 10th International Conference on Telecommunications, pp.388 – 392.

[6]. P.Hu, P.L.Hong, J.S.Li, Name Resolution in On-demand MANET, 2005, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 462 - 466.

[7]. P.Engelstad, D.V.Thanh, G.Egeland, Name Resolution in On-Demand MANETs and over External IP Networks, 2003, IEEE International Conference on Communications, volume 2, pp.1024–1032.

[8]. M. Nazeeruddin, G.P. Parr, B.W. Scotney, An efficient and robust name resolution protocol for dynamic MANETs, 2010, Ad Hoc Networks journal, Volume 8, Issue 8, pp.842-856.

[9]. S.Ahn, Y.Lim, A Modified Centralized DNS Approach for the Dynamic MANET Environment, 2009, 9th International Symposium on Communications and Information Technology, pp. 1506 - 1510.

[10]. R.Morera, A.McAuley, ADAPTING DNS TO DYNAMIC AD HOC NETWORKS, 2005, IEEE Military Communications Conference, Volume 2, pp.1303 - 1308.

[11]. X.Hong, J.Liu, R.Smith, Distributed Naming System for Mobile Ad-Hoc Networks, 2005, Proceedings of ICWN, pp.509-515.

[12]. M.Aoki, M.Saito,H.Aida, H.Tokuda, ANARCH: A Name Resolution Scheme for Mobile Ad Hoc Network, 2003, Proceedings of the17 th International Conference on Advanced Information Networking and Applications, pp.723-730.

[13]. C.Jelger, C.Tschudin, Underlay Fusion of DNS, ARP/ND, and Path Resolution in MANETs, 2011, 10th Scandinavian Workshop on Wireless Ad-hoc Networks.

[14]. Y.M.Gottlieb, R.Chadha, K.E.Cheng, MOSS: gathering names in networks of mobile nodes, 2008, IEEE Military Communications Conference, pp.1- 6.

[15]. J.H.Jeong, J.S.Park, H.J.Kim, NDR: Name Directory Service in Mobile Ad-Hoc Network.

[16]. J.Jeong, J.Park, H.Kim, Name Service in IPv6 Mobile Ad-hoc Network connected to the Internet, 2003, 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, pp.1351 – 1355.

[17]. T.Zahn, J.Schiller, MAPNaS: A Lightweight, Locality-Aware Peer-to-Peer Based Name Service for MANETs, 2005, the IEEE Conference on Local Computer Networks, pp.500-501.

[18]. M.Masdari, S.Jabbehdari, M.Ahmadi, S.M.Hashemi, J.Bagherzadeh, A.Khadem-Zadeh, A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks, 2011, EURASIP Journal on Wireless Communications and Networking.

[19]. M.Masdari, J.Pashaei, Distributed Certificate Management in Mobile Ad Hoc Networks, International Journal of Applied Information Systems, November 6, 2012.

[20]. J.H.Cho, A.Swami, I.R.Chen,A Survey on Trust Management for Mobile Ad Hoc Networks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2011,pp.562-583.