Study of Various IP Auto-configuration Techniques

Jagrati Nagdiya, Shweta Yadav

Abstract

Mobile Ad Hoc Networks (MANETs) are without a fixed infrastructure. All nodes have self organizing capabilities. One of the most important issues is the set of IP addresses that are assigned to the ad-hoc network. IP addressing and address auto-configuration have attracted much attention in MANETs. Some papers have proposed solutions to provide an auto-configuration of nodes. But they do not absolutely support security aspects in auto-configuration techniques. Thus, security is also a main issue in address allocation. In this paper we are proposing a model for secure IP- auto-configuration using public key cryptography.

Keywords: mobile ad-hoc networks, MANET, research trend, IP- auto-configuration, authentication and security.

1 Introduction

In contrast to infrastructure-based networks, MANET's support autonomous and spontaneous networking and, thus, should be capable of self-organization and self-configuration. An Ad hoc network is a group of mobile and wireless computers which communicate between each participant can, at any moment, act as a router to ensure a communication between two other distant nodes. Those networks are thus based on the cooperation between nodes without the assistance of any infrastructure. MANET applications include supporting battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room, and other security-sensitive computing environments. The ad-hoc networking technology has stimulated substantial research activities in the past years.

Before proper routing of data packets in a network, all nodes must be configured with unique IP address. Preconfiguring is not possible always as well as it has some drawbacks. Thus, an auto-configuration protocol is required to enable address assignment of nodes dynamically. The main task of an address auto-configuration protocol is to manage the resource address space. It must be able to select, allocate, and assign unique address to an unconfigured node.

Many research issues are deployed involving widespread situations for MANETs. If the researchers start to study the mobile ad-hoc network, they require spending a lot of time for collecting and arranging related literature. MANET research issues are here presented and classified. Aspects of MANETs are identified and grouped into fifteen categories [1]. These issues have the potential to significantly increase MANET survivability:

(1) Routing: Routing is an essential protocol in this field, because changes in network topology occur frequently. An efficient routing protocol is required to cope with highly fluid network conditions.

(2) Multicasting/ Broadcasting: Multicast service supports users communicating with other members in a multicast group. Broadcast service supports users communicating with all members on a network.

(3) Location Service: Location information uses the Global Positioning System (GPS) or the network-based geo-location technique to obtain the physical position of a destination.

(4) Clustering: Clustering is a method to partition the hosts into several clusters and provide a convenient framework for resource management, routing and virtual circuit support.

(5) Mobility Management: In the ad-hoc network environment, mobile hosts can move unrestricted from place to place. Mobility management handles the storage, maintenance and retrieval of the mobile node position information.

(6) TCP/ UDP: TCP and UDP are the standard protocols used in the Internet. Data applications running over MANETs, such as http and real audio need transport layer protocols like TCP and UDP to send packets over the links.

(7) IP Addressing: One of the most important issues is the set of IP addresses that are assigned to the ad-hoc network. IP addressing and address auto-configuration have attracted much attention in MANETs.

(8) Multiple Access: A major issue is to develop efficient medium access protocols that optimize spectral reuse, and hence, maximize aggregate channel utilization in MANETs.

(9) Radio Interface: Mobile nodes rely on the radio interface or antenna to transmit packets. Packet forwarding or receiving via radio interface or antenna techniques in MANETs are useful investigations.

(10) Bandwidth Management: Bandwidth management in MANETs is a typical characterization. Because the bandwidth is usually limited, effectively managing and using it is a very important issue.

(11) Power Management: A power management approach would help reducing power consumption and Hence prolonging the battery life of mobile nodes. Because most devices operate on batteries, power management becomes an important issue.

(12) Security: The mobile nodes in MANETs are highly susceptible to malicious damage. Security issues are important in MANETs to prevent potential attacks, threats and system vulnerabilities.

(13) Fault Tolerance: This issue involves detecting and correcting faults when network failures occur. Fault tolerance techniques are brought in for maintenance when a failure occurs during node movement, joining, or leaving the network.

(14) QoS/ Multimedia: Quality of Service (QoS) and Multimedia require high bandwidth, low delay, and high reliability.

(15) Standards/ Products: The standards and products issues that allow the development of small scale is emerging for this field. For instance, Bluetooth is a low-cost technology for short-range communications techniques.

The research trends from 1998 to 2003 are introduced first. The research trends for different issues are shown via a statistical graph.

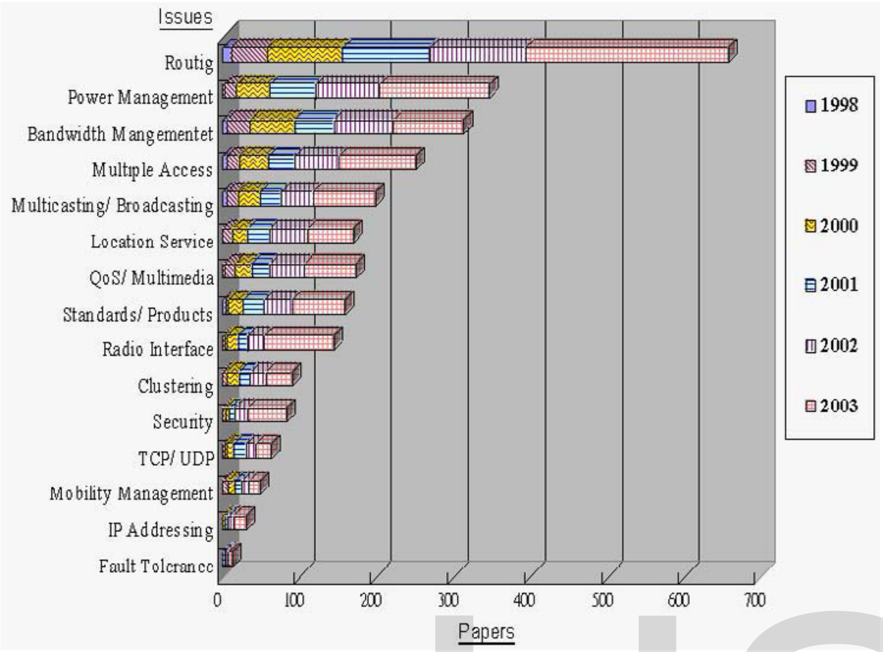

Figure 1 Trends of the issues in 1998 to 2003

1.1 Motivation

According to analysis results [1], the routing and power management issues have grown very fast and were the most popular in recent years. Although the IP addressing and fault tolerance issues have not been discussed very often, they will have potential study value in the future. As well as security is main issue in MANETs.

Before proper routing of data packets in a network, all nodes must be configured with unique IP address. Preconfiguring is not possible always as well as it has some drawbacks. Thus, an auto-configuration protocol is required to enable address assignment of nodes dynamically. The main task of an address auto-configuration protocol is to manage the resource address space. It must be able to select, allocate, and assign unique address to an unconfigured node.

Some papers have proposed solutions to provide an auto-configuration of nodes. But they do not absolutely support security aspects in auto-configuration techniques .Thus, Security is also a main issue in address allocation.

2 Related work

Several work has been done on MANET address auto-configuration like DHCPV6 based, Dynamic Configuration and Distribution Protocol (DCDP), Basic User Registration Protocol (BURP), Dynamic Mobility Agent (DMA), MANETconf, BOleng, Prophet, Buddy, CAC, Perkins, HCQC, PACMAN. In [2] presented Auto-configuration, Registration, and Mobility Management for Pervasive Computing. They explained that to face the future challenges, we must enhance many existing network protocols. Here, we have argued about the types of enhancements needed to IP-layer auto-configuration, user-to-network registration, and mobility management solutions. The manual configuration of individual hosts and nodes is impractical in future networks, characterized by a significantly larger number of networked nodes and considerably more dynamic topologies. Dynamic Configuration Distribution Protocol (DCDP) for auto configuring large networks with IP addresses and other information. While the protocols presented here significantly enhance the capabilities of future pervasive networks, several additional problems, such as security, still need to be completely worked out.

In [3] authors explained that some papers proposed solutions to allow an automatic configuration of nodes, i.e. without human intervention. Unfortunately these processes, often inspired of the traditional wired networks, are not always well adapted to the MANET model and appear relatively resources greedy. Moreover, they apply only to ideal networks in which all nodes can trust each other. In this manner, they do absolutely not consider the security aspects and are thus not adapted to a real use. One of the main threats against the security of MANET routing protocols is the identity usurpation (spoofing). Protocol intended to achieve automatic nodes configuration and addresses authentication. It uses the concept of recursive binary trees to efficiently provide addresses to the nodes and that of inter-certification in order to guarantee the origin of the forwarding packets. It can be used in a complementary way with algorithms especially dedicated to the securization of the routing process.

Auto-configuration protocols for conventional networks can be classified in protocols utilizing either stateless or stateful approaches [4]. DHCP is not applicable to a MANET with its highly dynamic topology is that the node running the DHCP sever may not be permanently reachable by all nodes. In contrast, protocols utilizing stateless approaches allow the nodes to select an address by themselves and verify its uniqueness in a distributed manner with the so-called, duplicatc address detection (DAD). Hybrid protocols combine elements of both stateful and stateless approaches. This can lead to more robust protocols, but may result in higher complexity and higher protocol overhead. Two such protocols are-presented in-the following: HCQA and PACMAN.

Kilian Weniger [5] presented research on PACMAN: Passive Auto-configuration for Mobile Ad Hoc Networks. Passive auto-configuration for mobile ad hoc network (PACMAN), a novel approach for the efficient distributed address auto-configuration of mobile ad hoc networks. Special features of PACMAN are the support for frequent network partitioning and merging, and very low protocol overhead. This PACMAN follows a hybrid approach and massively uses cross layer information from ongoing routing protocol traffic to provide an efficient address assignment and DAD, including support for frequent network partitioning and merging.

In [6] a new auto-configuration protocol for MANET (APM) is proposed. The solution is designed to perform node configurations in direct way and ensure continuity in the configuration service by introducing a special node called the configuration node (Nc). The APM considers node arrivals, node departures, and network partitioning and merge. Theoretical computation and simulation results show that APM has low latency and low overhead compared to most configuration methods based on conflict detection.

Maid Taghiloo and et. al [7] presented research on A SURVEY OF SECURE ADDRESS AUTO-CONFIGURATION IN MANET. They explained that providing security for IP address auto-configuration in MANET is still an open problem. Existing solutions for IP address auto-configuration in MANET do not address security issues. A centralized or hierarchical network security solution does not work well. Optimistic approaches can provide a better trade off between security and performance.

In [8] and [11] discussed about VASM. The scheme uses virtual address space for addressing new nodes joining a network. The aim is to map one point from virtual address sheet to exactly one new node. The reason for using the term “virtual” is that the whole corresponding address space is a 2D flat sheet and each point of this sheet is virtually mapped to a node in MANET. The protocol uses coordinate values for generating addresses. Basic idea is to dynamically distribute virtual address space among the dynamically selected Allocator nodes [8].

In [11] a security mechanism is added to VASM. It used a hash function that has very low running time. So this scheme is very light-weight. This approach uses cryptography functions (one-way hash function and symmetric cryptography) to encountering of the all possible address auto-configuration attacks. The key management and distribution is not explained here. The protocol assumes each node has pre-distributed secret key.
Hongbo Zhou and et. al [13] presented a secure auto-configuration and public-key distribution algorithm to achieve uniqueness of address allocation and secure public-key distribution. When a new node joins a MANET, which provides the bootstrapping for building a distributed certificate authority (DCA) in the network where a trust relationship is absent.

In [10], [12] and [14] presented security aspects for secure address allocation in MANET. [10] presented an authentication based dynamic IP configuration scheme that can securely allocate IP addresses to the authenticated hosts for a MANET without broadcasting over the entire network. Each host in the MANET can generate new unique IP address from its own IP address for a new authenticated host. This scheme provides authentication for address configuration with the help of a trusted third party and as such capable of handling the security threats associated with dynamic IP configuration. This addressing scheme has less addressing latency, low control overhead and low complexity. Robustness and security is also good in comparison to other schemes.[12] presented an ID based dynamic IP configuration scheme that can securely allocate IP addresses to the authorized hosts for a mobile ad hoc network without broadcasting over the entire network. The proposed scheme provides authentication for address configuration without the help of a trusted third party without compromising the security-threats associated with dynamic IP configuration. Each host can assign a unique IP address for a new host and the node is identified by a unique tuple_node id, IP address, the DAD broadcasting is not required. The scheme can also handle network partitions and mergers efficiently and securely. Further, it has low complexity, low overhead, is robust and more secure in comparison to the existing addressing schemes for the MANET. In [14], authors proposed a novel signature scheme that authenticates and lessens the security threats associated with dynamic IP configuration. This scheme is secure against any forgery attack. Therefore it eliminates the need of flooding messages all over the MANET during address allocation procedure, which saves considerable bandwidth. This scheme based bilinear pairing that ensures only authorized host will be configured in the MANET. Simulation results show that proposed addressing scheme has fairly good latency, low overhead in comparison to the similar existing dynamic addressing schemes for the MANET.

3 Problem definition

To develop a framework for Auto and secure Assignment of IP address to new node entered in mobile ad-hoc network using Public key cryptography. Expected output of the framework offer security in address auto-configuration in the absence of any static configuration or central sever. This approach uses public key cryptography “Rabin algorithm” to provide security in auto-configuration.

4 Proposed approach

For this purpose, consider a mobile ad hoc network. Nodes are classified into four categories:

- Allocator: Maintain the address space. They allocate new addresses for joining nodes.
- Initiator: An intermediate node between Allocators and Requester node that exchange all messages between them.
- Requester: new node that needs to get IP address in order to join the network.
- Normal: all other nodes are in this category.

Each Allocator in the network contains a disjoint address space. Therefore, address space overlap between allocators is none.

For creating network among the above mentioned nodes, an algorithm of IP auto-configuration is used. Here we are using public key cryptography to provide security in IP auto-configuration. According to this algorithm, at the beginning, requester broadcast a message to get the public key and public key certificate of allocator. This message (intended only for initiator and allocator) is received by initiator and remaining nodes discard it. With this message requester sends its own MAC address also. If initiator receives this message then forward it to allocator.

In reply allocator sends a message that contains public key and public key certificate to requester via initiator.

New node encrypts a message using the allocator's public key. This encrypted message contains request for IP allocation and its own MAC address. Requester sends message to allocator via initiator. As well as new now node calculates its own private key and public key.

Allocator decrypts the received message using requester's public key. Allocator gets the request for IP allocation and does the matching with the MAC address that was sent at the beginning. If match is found then allocator assign any one of available IP addresses to the requester as well as it maintains a record that map between requester's MAC address and allotted IP address. Now allocator encrypts the allotted IP address using requester's public key and send it to requester via initiator.

Requester decrypts the message by using its own private key and gets the allotted IP. Requester gets itself configured into the Mobile Ad hoc Network in secure manner.

5 Conclusion

In this paper we discussed the major issues in the MANETs. IP auto-configuration and security are two major issues among all. We proposed an algorithm that can provide IP address to new node (requester) in secure way. For security purpose we can use public key cryptography. Public key cryptography has its own advantages over secret key cryptography. IP address can be assigned in secure manner to the requester when it enters in range of MANET.

6 References

[1]C. R. Dow, P. J. Lin, S. C. Chen, J. H. Lin, and S. F. Hwang," A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks", in Proceedings of the 19th International Conference on Advanced Information Networking and Applications,2005 IEEE

[2] Archan Misra, Subir Das, and Anthony McAuley "Auto-configuration, Registration, and
Mobility Management for Pervasive Computing", IEEE Personal Communications, pp.24-31, 2001 IEEE

[3] Ana Cavalli and Jean-Marie Orset," Secure Hosts Auto-configuration in Mobile Ad hoc Networks", 2004 IEEE

[4] Kilian Weniger and MaHina Zitterbatt," Address Auto-configuration in Mobile Ad Hoc, Networks: Current Approaches and Future Directions", IEEE Network, pp. 6-11, 2004

[5] Kilian Weniger," PACMAN: Passive Auto-configuration for Mobile Ad Hoc Networks", AREAS IN COMMUNICATIONS, VOL. 23, NO. 3, pp. 507-519, 2005

[6] Abdellatif Ezzouhairi, Alejandro Quintero, Samuel Pierre." IP configuration in Ad Hoc Networks", IEEE, pp.1-7, 2005

[7] Majid Taghiloo1, 2, Jamshid Taghiloo3, Mehdi Dehghan1," A SURVEY OF SECURE ADDRESS AUTO-CONFIGURATION IN MANET", IEEE, 2006

[8] Majid Taghiloo1, Mehdi Dehghan2, Jamshid Taghiloo3, Maria Fazio4," New Approach for Address Auto-Configuration in MANET Based on Virtual Address Space Mapping (VASM)", IEEE, 2008

[9] Tomasz Mrugalski, Krzysztof Nowicki, and Krzysztof Wnuk," Next generation automatic IP configuration deployment issues", IEEE, 2008

[10] Uttam Ghosh and Raja Datta," An Authenticated Dynamic IP Configuration Scheme for Mobile Ad Hoc Networks", IEEE, 2009

[11] Majid Tajamolian, Majid Taghiloo, Mahnaz Tajamolian," Lightweight Secure IP Address Auto-Configuration Based On VASM", Advanced Information Networking and Applications, pp. 176-180, IEEE, 2009

[12] Uttam Ghosh∗ and Raja Datta," IDDIP: An ID Based Secure Dynamic IP Configuration Scheme for Mobile Ad Hoc Networks", pp. 1-5, IEEE, 2009

[13] Hongbo Zhou, Matt W. Mutak, Lionel M. Ni "Secure Auto-configuration and Public-key Distribution for Mobile Ad-hoc Networks", pp. 256-263, IEEE, 2009

[14] Uttam Ghosh and Raja Datta," A Novel Signature Scheme to Secure Distributed Dynamic Address Configuration Protocol in Mobile Ad Hoc Networks", pp.2700-2705, IEEE, 2012