Effect of Network Traffic on Duplicate Address Detection in Wireless Ad Hoc Networks

Nkosinathi H. Zulu, Murimo B. Mutanga and Matthew O. Adigun
Department of Computer Science
University of ZULULAND, P. O. Box X1000, KwaDlangezwa 3886
Tel: +27 35 9026706
email: {nathiristo079, bethelmutanga, moadigun}@gmail.com

Abstract- While much effort has been put in the creation of IP address auto-configuration protocols, very little has been done in testing the different protocols in different network conditions like different network topologies and different types of traffic. IP auto-configuration in mobile ad hoc networks has attracted much attention. Efficient Duplicate Address Detection techniques are continuously being formulated to provide nodes with unique addresses. In this paper we present a Duplicate Address Detection mechanism for the DSDV routing protocol. A passive DAD procedure that makes use routing protocol packets to detect and solve duplicate IP addresses is proposed. The proposed mechanism will be tested in the presence of network traffic. We hope that our contribution will stimulate further research in this direction.

Index Terms— DAD, ad-hoc networks, routing protocol

I. INTRODUCTION

Providing unique IP addresses efficiently in ad-hoc networks is still an open research question. However in recent years, a lot of research in ad-hoc networks has concentrated on routing protocols. The same intensity has not been applied to IP interface addressing. Routing protocols typically rely on nodes having a unique address [1]. In general, nodes are often assumed to have addresses configured, but in ad-hoc networks this is not easily accomplished. Although routing protocols assume the existence of unique node addresses, the question of how to provide them is still open. A significant amount of IP address auto-configuration schemes have been proposed. The basic idea behind automatic configuration is reducing administration efforts by users [2]. Duplicate Address Detection (DAD) is one of the most important components of IP address auto-configuration protocols. Duplicate address detection is required when two networks merge or simply as a continuous process to resolve duplicate IP addresses that might arise as a result of erroneous address allocation.

Most IP address auto-configuration schemes in literature are independent of the routing protocol hence making it difficult to detect address conflicts and network mergers. Some of these proposals utilize routing protocol traffic to detect address duplicates. This method has been proved to significantly reduce communication overhead [3]. The applicability of these protocols is still debatable since most of them are tested without any other traffic on the network (application layer traffic). It is not clear how routing protocol traffic affect IP address auto-configuration despite the close relationship between routing protocols and IP address auto-configuration protocols.

In this work we investigate the effect of network traffic on Duplicate Address Detection in wireless ad hoc networks. We proposed a duplicate address detection mechanism for the Distance Sequenced-Distance Vector routing protocol [4]. The basic idea behind our proposal is analyzing routing protocol packets for hints that point to the existence of duplicate addresses. Using routing protocol information for the purposes of duplicate address detection is not an entirely new concept. The aim of this research therefore is to test the effect of network traffic on the duplicate address detection mechanism.

II. Literature Review

A lot of work has been done in the area of IP address auto-configuration. Most proposal are routing protocol independent [5] [6] and a few are integrated with routing protocols [3]. Generally IP address auto-configuration protocols are classified as either being stateless or stateful. Protocols following the stateless paradigm do not maintain an address allocation table. An address allocation table is a list of all IP addresses currently in use on the network at any given time. New nodes randomly generate their own IP addresses from the permitted range of IP addresses and check for possible conflicts through a DAD procedure, hence most of the research classified under this approach is aimed at coming up with the most efficient DAD procedure[6]. If a conflict is detected then the new node will repeat the process, thus making DAD the cornerstone of the stateless paradigm. On the other hand protocols that follow the stateful approach assume that the addresses that are going to be assigned are not being used by any node in the network. The network node responsible for allocating IP addresses are allocated disjoint address pools from which to allocate new nodes hence performing a DAD in this situation is not necessary. Another approach is to distribute the address allocation table to all nodes. This approach, however, requires that the address allocation tables be actively synchronized to avoid state inconsistencies.

III. Proposed DAD Mechanism For DSDV

Since DSDV is a pro-active routing protocol, the stateful approach can easily be adopted beacase it stores and update topology information. Proactive routing protocols, maintain an up-to-date view of the network by periodically broadcasting the link-state costs of its neighbouring nodes to all other nodes using a flooding strategy [7]. Stateful auto-configuration protocols also maintain state information i.e. the list of all the nodes that are in the network at any given time. The same information can be obtained from routing tables of proactive routing protocols. It then makes sense to use the same information rather than maintaining two separate states.

To detect duplicate addresses, nodes analyse the periodic routing protocol information that is disseminated by the routing protocol. The transmitted routing tables in DSDV [**4**] contain the hardware addresses, number of hops, sequence number etc. An analysis of this information can easily point out to the existence of duplicate addresses. The DSDV makes use of two types of topology dissemination messages, the full dump and incremental. If a new node joined the networks and is configured by its initiator, the initiator broadcasts an incremental reporting the topology changes to all its neighbors. This information will subsequently reach all the nodes in the network. All the other nodes check if their no other node in their routing tables that has a different hardware address and the same IP address with what is being advertised. If such an entry exists, a duplicate address is detected. If one of the conflicting nodes detects the address conflict, it checks the hardware address of in the received message. If it is higher than its own address, it changes its own IP address. This time there is no need for an initiator since it has a routing table with a list of all the nodes in the network. It simply selects an IP address from the ones that are currently free (according to its routing table). Soon after making this change, the node will broadcast an address change notification message. If any nodes receive the address change notification, they make relevant entries in their routing tables. If the hardware address is less that its own, it ignores the conflict. This is to make sure that only one node responds to an address conflict and also to reduce the amount of overhead. In essence there are no extra packets that are defined by this mechanism. Duplicate addresses are detected passively. Only one new message is defined.

III. SIMULATION EXPERIMENTS

To support our DAD mechanism, modifications of the DSDV routing protocol were made in Network Simulator-2 (ns-2) version 3.4 running on Ubuntu Linux 8.04 operating system with CMU extension of ns-2 to support ad-hoc networks [xx]. The link layer model used in the simulation is based on the IEEE 802.11 MAC protocol. All nodes will be preconfigured with IP addresses and the number duplicate addresses in the network were varied. Traffic will be generated using the scenario generator package. The same traffic file will be used for all experiments. The number of duplicate addresses will be varied to gain a compressive analysis. Traffic type and volume will also be varied.

IV. Conclusion

IP address auto-configuration has generated a lot of interest in recent years. So many IP address auto-configuration mechanisms have been proposed. Duplicate Address Detection is an important component of IP addressing schemes. This component uses routing protocol information to detect and resolve duplicate IP addresses. Despite all the work that has been done on this area, not much has been done in investigating how different components of the IP addressing schemes perform in a normal network. In this paper we presented a Duplicate Address Detection mechanism for the DSDV routing protocol. This mechanism will be tested under different types and volumes of network traffic.

References

1. Cavalli, A. and Orset, J. (2005). "Secure hosts auto-configuration in mobile ad-hoc networks", Ad-hoc Networks, Volume 3, Issue 5, pp: 656-667, September 2005.
2. Weniger, K. and Zitterbart, M. (2004). “Address Autoconfiguration in Mobile Ad-hoc Networks: Current Approaches and Future Directions”, EEE Network Magazine Special issue on 'Ad-hoc networking: data communications & topology control', Jul 2004.
3. Boudjit, S. Adjih, C. M¨uhlethaler, P. Laouiti, A. “Duplicate Address Detection and Autoconfiguration in OLSR” Journal of Universal Computer Science, vol. 13, no. 1 (2007), 4-31

4. Perkins, C.E. Bhagwat, P. “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers”, Proceedings of the conference on Communications architectures, protocols and applications, p.234-244, August 31-September 02, 1994, London, United Kingdom
5. Fazio, M. Villari, M. Puliafito, A. “AIPAC: Automatic IP address configuration in mobile ad hoc networks”, Computer Communications, Volume 29, Issue 8, pp 1189-1200, May 2006.
6. Mutanga, M.B. Nyandeni, T.C. Mudali, P. Xulu, S.S. Adigun, M.O. “Wise-DAD Auto-Configuration for Wireless Multi-hop Networks,” In the proceedings of the Southern African Telecommunications Conference, Sept 2008
7. Abolhasan, M. Wysocki, T. Dutkiewicz, E. “A review of routing protocols for mobile ad hoc networks”, Ad Hoc Networks, Volume 2, Issue 1, January 2004, Pages 1-22

Nkosinathi Zulu received his Hons degree in Computer Science 2009 from the University of ZULULAND and is presently studying towards his Master of Science degree at the same institution. His research interests include security in wireless ad hoc networks and automatic configuration in ad -hoc networks