LOCALISED AD HOC ADDRESS AUTOCONFIGURATION VIA CLUSTERING IN NOMADIC AD HOC NETWORKS

George Metaxas, David Hutchison and Nicholas J.P. Race
Computing Department, InfoLab21
Lancaster University, Lancaster LA1 4WA, UK

Keywords: Address Autoconfiguration, Nomadic Ad hoc Networks, Wireless Networking, IPv6.

Abstract: Densely populated urban environments provide unique nomadic movement patterns. People tend to move in groups across predefined paths, with low intra-group movement, giving rise to Nomadic Ad hoc Networks (NANETs). NANETs, which are a constrained subset of Mobile Ad hoc Networks (MANETs) in terms of mobility, concentrate on civilian-style usage and are sufficiently dynamic in nature to present significant challenges in the design of even the most common tasks such as packet routing or name resolution. An intriguing issue relates to the automatic configuration of IP addresses to constituent nodes that will allow data exchange. The underlying physical group structure can be utilised in the network layer as a basis for an address autoconfiguration mechanism, which would yield low and localised signalling traffic overhead coupled with a subnet optimisation. This paper proposes and discusses the AALM IPv6 address autoconfiguration mechanism, which has been developed to provide the aforementioned characteristics.

1 INTRODUCTION

Nomadic Ad hoc Networks (NANETs), first explored in (Prince, 2005), provide a relatively fresh view to the generic field of **Mobile Ad hoc Networks (MANETs)**. The inherent nomadic nature constrains the movement patterns of constituent nodes to a tacit model found in densely populated urban environments. People tend to move in groups across predetermined paths, pausing at places of interest for an undetermined amount of time. Intra-group mobility is considered low, whereas group mobility in respect to the environment may be high. NANETs present an environment found in crowded city centres, university campuses and shopping centres, which are typical civilian-style rather than military or emergency response scenarios.

Although constrained in relation to MANETs, NANETs are still highly dynamic ad hoc networks and exhibit several MANET traits, such as lack of a centralised infrastructure. Consequently, basic tasks such as packet routing, name resolution and automatic address configuration require cooperative approaches. The most widely researched subject is associated with packet routing. Several experimental standards have been produced by the IETF MANET Working Group, which is responsible for engineering such solutions.

Aside from packet routing, address autoconfiguration provides an area of significant challenges. In wired and wireless infrastructure networks, this is supported by infrastructure means, such as address pool servers. In a MANET, it is impossible and unwise to presume the presence of infrastructure support. Therefore, address autoconfiguration requires node cooperation and the design of distributed algorithms capable of rapidly adapting to environmental conditions. The constrained and specialised nature of mobility in NANETs, can be exploited to provide better solutions and reveal issues, otherwise hidden due to unconstrained and unnatural movement patterns.

This paper proposes an address autoconfiguration mechanism for NANETs, which has been fundamentally designed to operate in partitioned networks, by localising signalling traffic, through the use of clustering concepts. The added advantage of this approach is the subnet optimisation which minimises routing table size. The remainder of this paper is organised as follows. Section 2 discusses related work in the field of address autoconfiguration mechanisms for MANETs and details various physical layer issues. Section 3 presents the design of the proposed mechanism. Section 4 provides an evaluation of the mecha-

Metaxas G., Hutchison D. and J.P. Race N. (2006).
LOCALISED AD HOC ADDRESS AUTOCONFIGURATION VIA CLUSTERING IN NOMADIC AD HOC NETWORKS.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 121-128

nism through extensive simulations. Finally, Section 5 concludes the paper and discusses future work.

2 RELATED WORK

Address autoconfiguration mechanisms became a requirement in wired networks as a result of the growth and popularity of the Internet. They are classified in two categories, statefull and stateless. The former requires the presence of a centralised server for distributing addresses, as in DHCP (Droms, 1997). The latter achieves address configuration per node atomically, without contacting a centralised server. The IPv6 **Stateless Address Autoconfiguration (SAA)**, defined in (Thomson and Narten, 1998), is such a mechanism. Nodes are equipped with link local and global addresses. SAA requires a router advertising a unique subnet prefix in every subnet. A link local address is formed by converting the MAC address of a network interface to a 64-bit identifier and appending it to the link local prefix (FE80::). Address uniqueness on the link is verified through a broadcast message, which initiates the **Duplicate Address Detection (DAD)** process. A reply signals duplication causing the repetition of the procedure. Otherwise, the address is considered unique and a global address is formed by appending the unique interface identifier to the subnet prefix.

Pure ad hoc networks require stateless approaches, which are classified in three categories, conflict avoidance, conflict detection and hybrid. In conflict avoidance mechanisms, addresses are acquired through a configured neighbour which possesses an unallocated address pool. In contrast, nodes atomically acquire addresses in conflict detection mechanisms and attempt to detect and resolve possible duplications. Hybrid solutions provide a fusion of the above approaches. Several ad hoc address autoconfiguration mechanisms are presented in Section 2.1.

At present, software solutions developed for use in ad hoc networks are impeded by various physical layer issues. These issues are mainly concerned with scalability and partition formation. They are inherent in two of the most popular wireless technologies used for constructing ad hoc networks, IEEE 802.11 and Bluetooth. Section 2.2 discusses some of these issues.

2.1 Address Autoconfiguration In Ad Hoc Networks

An initial attempt to provide a MANET address autoconfiguration mechanism, similar to the IPv6 SAA is described in (Perkins et al., 2000). An unconfigured node selects a random IPv4 address from a specific range, broadcasts a message requesting a route to the generated address and sets a timer. If the timer expires and no replies are received, the process is repeated up to a pre-specified number of times. Further lack of replies, is assumed to reveal that the address is unallocated and can be assigned to the node. Otherwise the address is in use and the process is repeated.

(Vaidya, 2002) terms the above idea as **Strong DAD** and argues that it fails if message delay between any pair of nodes is unbounded. The proposed **Weak DAD** technique allows routing protocols to correctly deliver packets even in the presence of duplicate addresses. This is achieved by associating a predefined unique key with each node, such as an IMEI[1], distributed and stored alongside IP addresses to enable unique node identification when required.

(Zhou et al., 2003) uses a common address pool which is drawn from the results of a carefully chosen function that generates sequences with a low probability of producing the same numbers. The first initialised node chooses the function and the seed to be used. It is called a *prophet* as a result of its ability to predict all generated addresses. Unconfigured nodes request the help of their closest configured neighbour, which creates an address using the selected function and returns it, along with the seed and the function in use, to the requester.

Another technique called **Passive Duplicate Address Detection (PDAD)** is discussed in (Weniger, 2003) and (Weniger, 2005). It is a passive approach, involving no explicit signalling traffic transmission, deriving its decisions from routing protocol traffic investigation. Nodes are configured with addresses that are unlikely to be duplicate, deriving their decisions through a probabilistic algorithm, which is aided by an *Address Allocation* table maintained per node.

A common issue in MANETs is the occurrence of partitions, which are collections of nodes separating from or merging into the network. Address autoconfiguration mechanisms handle partitions by associating them with identifiers and providing duplicate address resolution in case of partition merge, as in (Sun and Belding-Royer, 2003), (Nesargi and Prakash, 2002), (Zhou et al., 2003) and (Toner and O'Mahony, 2003). A node is chosen to create, distribute, maintain and advertise the partition identifier. Partition splits and mergers are identified by the lack of partition identifier advertisements or the reception of multiple different advertisements respectively. This approach is cumbersome, generates excessive signalling traffic and does not resolve address duplications across multi-hop partitions. Moreover, partition identifiers are unrelated to the network operation and introduce additional bandwidth and routing

[1] A pre-configured unique 15-digit number used in GSM networks

table size overheads.

2.2 Physical Layer Issues

One of the major issues inhibiting the wide deployment of MANETs are the inherent physical layer issues in the most popular underlying networking technologies. These issues result in the creation of partitions and impact the scalability of the resulting networks. Partitions are mainly manifested when several nodes become separated from the rest of the network, as a result of physical movement or due to wireless channel conditions. The existence of partitions prohibits proper operation of distributed algorithms due to the lack of routing paths. Even though partitions can be treated as separate networks, the presence of mobility and freedom of movement leads to partition merging and splitting.

Wireless channel conditions are the most important contributer to partitioning, apart from physical node movement. This is especially evident in the IEEE 802.11 protocol. (Lundgren et al., 2002) reports the problem of *gray zones*, which are areas where nodes are able to exchange routing information but no data. The problem of *unidirectional links* discussed in (Prakash, 1999), can also lead to partitions, especially if such a link exists between key routing paths in the network. Even the number of people impacts the channel quality as discussed in (Mathur et al., 2004).

Ad hoc networks are also plagued by scalability problems impeding their multihop ability, as a result of various physical layer issues. (Tschudin et al., 2003) and (Tschudin et al., 2004) discuss the *Ad hoc Horizon* problem which exists in IEEE 802.11. It dictates that beyond two to three hops, routing information becomes useless, route maintenance and discovery inhibit network operation and TCP performance becomes unacceptable. Bluetooth is known for its difficulty in scaling due to oversights in its specification, as discussed in (Guerin et al., 2002), regarding the scatternet formation procedure used for creating larger Bluetooth networks. A number of research studies propose different algorithms for this purpose, such as for example (Zaruba et al., 2001) and (Law and Siu, 2001). However, it is doubtful whether Bluetooth is scalable, due to the increased overhead required for scatternet creation, as discussed in (Miklós et al., 2000) and (Vergetis et al., 2005).

3 THE AALM MECHANISM

Partitioning is a natural tendency of MANETs and NANETs due to physical movement and wireless channel conditions. Especially in the case of NANETs, the existence of partitions is a highly likely occurrence due to the underlying nomadic behaviour. However, current address autoconfiguration proposals treat partitioning as a special case and consider generic MANET movement scenarios, which are mostly unrealistic and do not reflect civilian-style scenarios. The **Ad hoc Address autoconfiguration Localisation Mechanism (AALM)** is a novel approach in the field. It has been designed around IPv6, reuses the ICMPv6 signalling mechanisms and attempts to tailor the SAA procedure for use in partitioned NANETs.

Partitioning is fundamental to the design of AALM, which combats this issue and provides a scalable, low overhead solution. This is achieved through the use of Network layer clusters, or groups as they are referred to in this paper, which are at most two hops in diameter. This technique also achieves increased scalability by reducing the required routing table size, as groups are considered to be small scale subnets. Address uniqueness is highly localised in small regions, up to a maximum of six hops. Consequently, the impact of address duplications and partition creations is localised to a very small network part, thereby minimising the signalling traffic overhead. This *localisation* of signalling traffic governs all aspects of address generation and maintenance. All packets are transmitted with a hop count of one unless otherwise stated.

3.1 Assumptions

Several assumptions are required in the design of the AALM mechanism. The underlying environment is assumed to be constrained in terms of mobility and node movement, following the nomadic model, where nodes move in groups and intra-group mobility is considered low. NANETs concentrate on civilian-style scenarios found in settings such as city centres. Therefore, it is assumed that group movement with respect to the environment and other groups is considered low. Low mobility is similar to the walking speed of people. Constituent devices are considered to be small mobile devices, such as mobile phones, PDAs or laptops.

Each device must be equipped with one wireless ad hoc interface and one wireless infrastructure interface[2]. The interface operating in infrastructure mode is assumed to be assigned a globally unique IPv6 address which remains unchanged. Furthermore, each ad hoc interface is associated with a unique MAC address. For the remainder of this paper, the abbreviations NSOL, NAD, RAD and RSOL specify the ICMPv6 Neighbour Solicitation, Neighbour Adver-

[2]For example IEEE 802.11 and GPRS, found in some mobile phone models

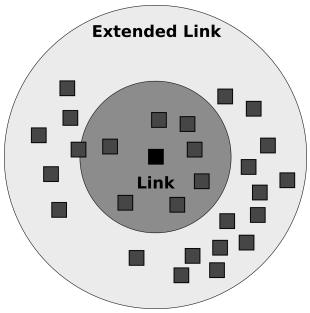

Figure 1: The link and extended link concepts.

tisement, Router Advertisement and Router Solicitation messages respectively.

3.2 Founding Concepts of AALM

AALM defines two neighbour sets, the *link* and the *extended link*. A link is: **the set of all one hop neighbours of a node**, whereas an extended link is: **the set of all one hop neighbours of a node plus their one hop neighbours**. The link definition resembles the corresponding definition used in wired networks. An extended link represents a node's two hop neighbourhood. Nodes acquire unique link local addresses that are cooperatively maintained in their extended link. Precise knowledge of the extended link is not required, but provides a safety zone for link local address uniqueness. Figure 1 shows the difference between the two constructs.

The SAA specification requires nodes to *defend* themselves in case of address duplication in their link. Reception of a message on a specific multicast address, after the completion of the SAA procedure, permits the receiver to defend its address by transmitting an appropriate NAD. Nodes using the AALM mechanism are also required to respond to any potential duplications, but also defend their link neighbours. This is necessary due to a node's partial perception of the network topology. Maintaining address uniqueness in a node's link requires neighbour cooperation, as their link is part of the defended node's extended link. All address defence messages are transmitted to the **All Nodes in Link Multicast** (FF02::1) address.

There are two address types assigned by the AALM mechanism, link local and site local. Link local addresses are of limited scope, valid for one hop communications only. Their uniqueness is maintained in a node's extended link through regular beaconing and neighbour cooperation. This cooperation is enforced by transmitting all beaconing, address acquisition and maintenance related messages to the IPv6 broadcast address, for inspection by all neighbours. All such messages are transmitted with a hop count of one.

Upon acquiring link local addresses, group formation is initiated to equip nodes with site local addresses. AALM uses the term group rather than cluster to differentiate from clustering algorithms, which are usually implemented at the MAC layer. Each group is associated with a 32-bit *Group Identifier (GID)* that is embedded in the site local addresses of group members. GID uniqueness is maintained across neighbouring groups. There are three group member types, a leader, gateways and ordinary nodes. Groups are centred around a leader and all group members are one hop neighbours of a leader. Therefore, all group members are at most two hops away. Nodes record neighbour information in their Neighbour Cache and group information in their Prefix and Router Caches.

3.3 Link Local Address Acquisition

The link local address acquisition procedure, is similar to the DAD procedure of SAA, although there are several distinct features associated with the AALM mechanism. The 64-bit interface identifier is randomly generated, rather than being associated with the MAC address, for enhancing privacy. The NSOL carrying the generated address is transmitted to the **All Nodes in Link Multicast** address (FF02::1) to promote cooperation among neighbours in the configuration procedure. Receiving nodes must record this information in their Neighbour Cache, unless a duplication is detected. The initial NSOL is transmitted exactly once and the node must also set a timer to signal the end of the DAD procedure. This event is followed by the initialisation of a pseudo-periodic beaconing service to advertise a node's link local address, which in AALM terms has been *acquired* by the node that is now considered to be configured.

MAC address comparison is used for resolving duplications, with the lowest one favoured. The preferred node is also determined by whether either of the offending nodes has acquired the address. If both or none have acquired the address, only MAC address comparison is performed. Otherwise, the node which is configured or presumed to be configured is allowed to maintain ownership of the address, irrespective of MAC address comparison. Furthermore, if address duplication occurs after group formation, involving a leader and a non leader node, the leader is favoured. All signalling and data traffic containing link local addresses are searched in the Neighbour Cache for duplications.

The favoured node is not defended immediately, unless it is also the one detecting the duplication. In all other cases an appropriate reply packet is created and queued for future transmission. The queueing interval is random for each node, but does not exceed one hundred milliseconds. Reception of a similar reply packet, causes the receiving node to cancel its

queued transmission if it is in agreement with the provided information. Otherwise, it re-evaluates its decision and proceeds to update the contents of its queued packet, but not the scheduled transmission time. This procedure minimises the number of defence packets transmitted and reduces wireless channel contention and the number of dropped packets. Assuming two conflicting nodes, only one packet is necessary to resolve a duplication.

3.4 Group Formation and Site Local Address Acquisition

The group formation procedure is based on the **Lowest-ID** and **Least Cluster Change (LCC)** clustering algorithms, discussed in (Ephremides, 1988) and (Chiang, 1997) respectively. Lowest-ID is used in leader election, whereas LCC is used as a means to increase group stability by not destroying groups whenever a member with a lowest identifier from the leader becomes a group member. As previously mentioned, the Prefix and Router Caches record information about groups. The former stores prefixes advertised by group leaders or gateways, whereas the latter stores leaders addresses. Prior to the group formation procedure, nodes investigate their Prefix and Router Caches to identify groups in the vicinity, in which case they associate themselves with such a group, becoming members. Otherwise, group formation is initiated by investigating the contents of the Neighbour Cache for identifying the node possessing the lowest MAC address, which is designated as a *potential leader*. All other nodes set a timer and await for a leader to make its presence known. This is required in case a potential leader does not claim its leadership due to the existence of a node with an even lower MAC address in its link.

The potential leader picks a random GID, by first investigating the contents of the Prefix Cache, and generates its *leader specific* site local address as: FEC0:0000:HIGH-GID:LOW-GID::1[3]. To verify the GID uniqueness, the newly introduced **Duplicate Group Identifier Detection (DGID)** procedure is initiated. A NSOL sourced from the leader's link local address is transmitted to the All Nodes In Link Multicast address, containing the leader specific site local address. The hop count of the message is set to one and an option specifying the leader's wireless infrastructure address, which uniquely distinguishes every node in the network, is included. A timer is set to signal the end of the DGID procedure.

Neighbouring nodes receiving the NSOL investigate their Prefix Caches for the included prefix. If one is found, a duplicate GID may have been detected which is resolved by comparing the associated wireless infrastructure addresses, with the lowest being favoured. In GID duplications it is also important to check if they involve established groups. If both groups are established or are not established, then comparison of the leaders wireless infrastructure addresses resolves the duplication. Otherwise, the established group is favoured. The result of the resolution is transmitted by either RADs or NADs, depending on whether the detecting node is a leader or not. Only leaders are allowed to immediately transmit a reply. All other nodes are required to queue their packet for a random time interval of up to one hundred milliseconds and follow a similar procedure to link local address defence, to transmit or cancel the packet accordingly.

If a potential leader receives a NAD signifying duplication, it picks a new GID and restarts the DGID procedure. However, if a RAD is received, an established leader is in the link of the potential leader which must stop the group formation procedure and join the existing group. If no messages are received by the potential leader and its timer expires, the GID is assumed unique, no other leaders are found in the link and the group can be established. Its NAD beaconing service is replaced by pseudo-periodically transmitted RADs. All such packets are transmitted from the leader's link local address and contain options signifying the prefix advertised, the leader's link layer address and its wireless infrastructure address.

All nodes receiving the group creation NSOL message insert appropriate entries in their Prefix and Router Caches and generate a site local address. This is achieved by appending the interface identifier from their link local address to the prefix included. The resulting address is associated with a tentative status, as the group is not yet established. Permanent status is only assigned after reception of a valid RAD from the same leader which advertised the address prefix. Nodes receiving RADs from multiple leaders become gateways and create site local addresses per group. One group is selected as the primary group of each node.

AALM attempts to maintain GID uniqueness among neighbouring groups. There are two types of neighbouring groups, direct and indirect. Two groups are direct neighbours of each other when there exists a gateway node, in other words a one hop neighbour of both leaders. In contrast, two groups are indirect neighbours when they have no gateways among them, but there are member nodes in each group which are one hop neighbours of each other. Neighbouring groups of a group are responsible for maintaining GID uniqueness by prohibiting any of their neighbours to use the same GID. This process guarantees site local address uniqueness across a maximum of

[3]HIGH-GID and LOW-GID represent the high and low order 16 bits of the GID respectively

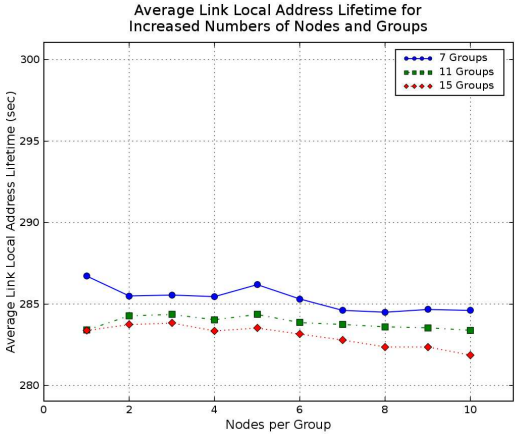

Figure 2: Average lifetime of link local addresses.

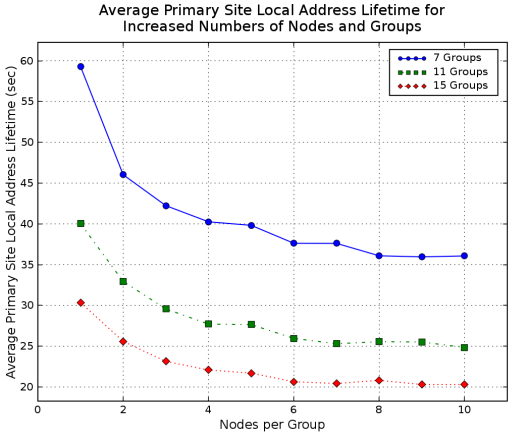

Figure 3: Average lifetime of primary site local addresses.

six hops. It is augmented by the newly introduced **Group Multicast Information Exchange Mechanism (GMIEM)** which uses a **Group Multicast Address (GMA)**, as well as a newly defined ICMPv6 Group Information option. Each group leader maintains knowledge about neighbouring groups proactively and is able to resolve possible GID duplications.

The Group Information option is a new ICMPv6 option for the exchange of group information. It contains a GID and the associated wireless infrastructure address of the leader, together with a flag signifying whether the information belongs to the transmitter's primary group. These options are inserted by all group members in their beacons. Each leader includes the complete contents of its Prefix Cache in all transmitted RADs. This provides group members with an up-to-date view of all known neighbouring groups and are qualified for resolving possible GID duplications.

Member nodes passively register to the GMA of each group they are members of. The GMA is a multicast address of the form: FF02:FF02:HIGH-GID:LOW-GID::1. All traffic transmitted to the GMA is received by some of the members of the associated group. It is provided as a means to filter out certain nodes from receiving packets. Only a leader may be able to reach all group members. The GMA is used in the GMIEM, to assist member nodes in informing their group neighbours and especially their respective leaders about newly discovered groups and propagate this information through the packet queueing mechanism.

Nodes regularly monitor GMA traffic to identify information identical to their queued packets, resulting in the cancellation of their own packets. Duplications are resolved through wireless infrastructure address comparison of the conflicting group leaders, with the lowest one being favoured. A reply is immediately transmitted, if the transmitter is a leader, and forwarded to the affected group as a NAD.

Table 1: Summary of Simulation Scenarios.

No of Groups	Total Nodes
7	7 to 70 increments of 7
11	11 to 110 increments of 11
15	15 to 150 increments of 15

4 EVALUATION

The AALM mechanism has been evaluated through extensive simulations using the ns-2 simulator. The characteristics investigated are the amount of signalling traffic generated, the lifetime of addresses and the impact of increasing numbers of physical groups and nodes in the simulation. The simulated scenarios are produced by the *rpgm* tool, kindly provided by the authors of (Camp et al., 2002), which implements the **Reference Point Group Mobility Model**. The exact node and group configuration parameters of the simulations are shown in Table 1. For each node and group increment, twenty scenarios are generated and simulated with 100 different seeds. The simulator has been configured with the standard IEEE 802.11 implementation, using the Two Ray Ground propagation model. There exists no other traffic in the network apart from AALM signalling traffic. The simulated area is 300 metres wide by 300 metres long and the transmission range is set to 60 metres. The simulated scenario time is fixed at 300 seconds. The allowed address space used, is constrained. The interface identifier values are restricted from 0 to 4 times the number of nodes in the simulation, which is also applied to GIDs. Fi-

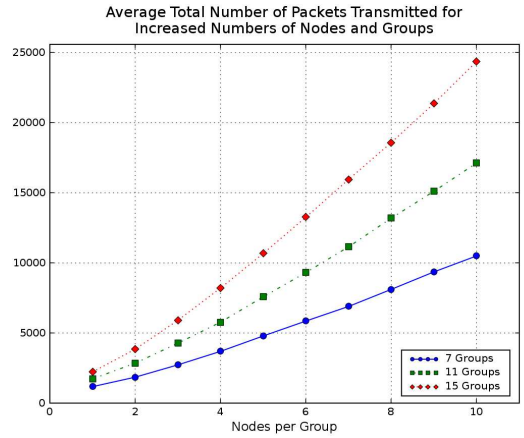

Figure 4: Average total number of packets transmitted per simulation.

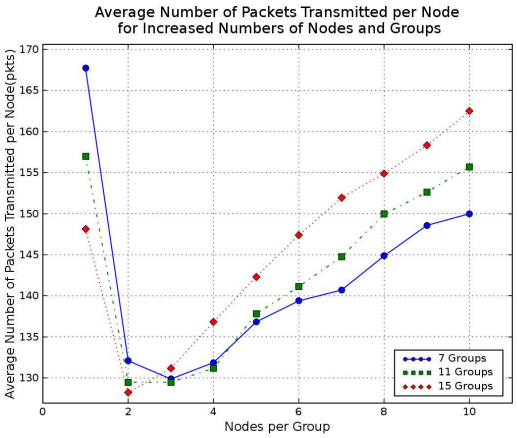

Figure 5: Average number of packets transmitted per node.

nally, the beaconing interval for all nodes is set to 2 seconds, apart from leaders which advertise their presence every 1.5 seconds.

The results acquired regarding the lifetime of link local addresses are highly positive. As shown in Figure 2 the average lifetime is high, with a lowest value of about 282 seconds. The graph demonstrates a minimal decrease in the link local address lifetime as the number of nodes per group increases. Increased numbers of physical groups in the simulation result in slightly decreased lifetime values. The decreased trends observed are mainly related with the number of physical groups, rather than nodes per group. Inserting more groups in the network increases the number of nodes in the simulation which are beyond a node's extended link. Therefore, the existence of a duplicate address somewhere in the simulation area, which is not resolved, is more probable.

Figure 3 shows the results obtained regarding the average lifetime of primary site local addresses, in other words the address associated with a node's primary group. It is evident that increased numbers of nodes per group results in decreased address lifetime values. The same applies to increased numbers of physical groups. Another important observation is that as the number of physical groups increases, the differences in the results obtained for increased numbers of nodes per group are decreased. For example, for 15 physical groups, the average primary site local address lifetime for 1 node per group is about 30 seconds, whereas it is 20 seconds for 10 nodes per group, a difference of 10 seconds. On the other hand, for 7 groups the corresponding values are 60 and 36, which is a difference of 24 seconds. The obtained values are suitable for HTTP-type traffic, where the amount of data exchanged is relatively low. They are unsuitable for multimedia-type traffic and large data exchanges, due to the requirement for a mechanism capable of maintaining connections after address changes. Although such mechanisms exist in wired networks (MIPv6), which have been somewhat adapted to operate in an ad hoc context, there exists no mechanism at present to operate in a pure ad hoc networking environment. The lifetime of primary site local addresses is dependent on group and link local address lifetime. Whenever a link local address is removed, for any reason, all site local addresses are also removed. Furthermore, upon group destruction, nodes must pick a new primary site local address, if another group is present, or initiate the group formation process. The achieved results point to reduced group lifetimes. This is one aspect of the proposed mechanism which requires further investigation and improvement.

The graphs shown in Figure 4 show the signalling traffic footprint of the mechanism. Clearly as the number of nodes and nodes per group increases, so does the number of transmitted packets. This increase is almost linear in nature. It is observed that increasing the total number of nodes in the simulation by 40 results in about 7000 extra packets. Figure 5 shows the average number of packets transmitted per node. In this figure, it is interesting to note that for the most part, increasing the number of nodes per group, results in an increased average number of packets transmitted per node. The only exception is for 1 node per group. The initial high values are attributed to the greater number of leaders in respect to ordinary nodes per group, which transmit packets at a lower interval (1.5 seconds for leaders versus 2 seconds for ordinary nodes). Furthermore, increasing the number of groups results in slightly increased values. The average number of packets transmitted per node and the one hop nature of these packets indicates the scalability of the mechanism.

5 CONCLUSION

This paper has presented a novel address autoconfiguration mechanism for NANETs, which are a subset of MANETs and are associated with civilian-style scenarios. The mechanism has been fundamentally designed to address the problem of partitioning, utilising underlying environmental characteristics to impose a Network layer subnet structure. Furthermore, the structure is maintained through signalling traffic localisation, thereby reducing the effects of partitioning and probable address duplications.

The evaluation of the proposed AALM mechanism, through extensive simulations, has demonstrated its effectiveness to facilitate short lived HTTP-type traffic, in regards to signalling traffic overhead and link local addresses lifetime. It is an efficient approach for assigning addresses usable for one hop data exchange, although requires further improvement regarding long-lived connectivity in respect to the lifetime of site local addresses. Future work should also concentrate on improving the design of AALM in order to provide a more generic solution applicable to a wider range of MANETs.

REFERENCES

Camp, T., Boleng, J., and Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502.

Chiang, C. C. (1997). Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. In *IEEE Singapore International Conference on Networks (IEEE SICON '97)*, pages 197–211.

Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol.

Ephremides, A. (1988). A design concept for reliable mobile radio networks with frequency-hopping signaling. *NASA STI/Recon Technical Report N*, 89:17772–+.

Guerin, R., Kim, E., and Sakar, S. (2002). Bluetooth Technology: Key Challenges and Initial Research. In *Conference on Network and Distributed Simulations*.

Law, C. and Siu, K. Y. (2001). A Bluetooth scatternet formation algorithm. In *IEEE Symposium on Ad Hoc Wireless Networks 2001*.

Lundgren, H., Nordström, E., and Tschudin, C. F. (2002). Coping with communication gray zones in IEEE 802.11b based ad hoc networks. Technical Report 2002-022, Department of Information Technology, Uppsala University.

Mathur, R., Klepal, M., McGibney, A., and Pesch, D. (2004). Influence of People Shadowing on Bit Error Rate of IEEE802.11 2.4GHZ Channel. In *1st IEEE International Symposium on Wireless Communication Systems, ISWCS04*.

Miklós, G., Rácz, A., Turányi, Z., Valkó, A., and Johansson, P. (2000). Performance aspects of Bluetooth scatternet formation. In *MobiHoc '00: 1st ACM international symposium on Mobile Ad hoc Networking & Computing*, pages 147–148, Piscataway, NJ, USA. IEEE Press.

Nesargi, S. and Prakash, R. (2002). MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network. In *Proceedings of IEEE INFOCOM*.

Perkins, C., Royer, E., and Das, S. (2000). IP Address Autoconfiguration for Ad Hoc Networks. Internet Draft, IETF.

Prakash, R. (1999). Unidirectional links prove costly in wireless ad hoc networks. In *DIALM '99: 3rd International Workshop on Discrete algorithms and methods for mobile computing and communications*, pages 15–22, New York, NY, USA. ACM Press.

Prince, D. (2005). *Dynamic Service Deployment through Consensus Negotiation in Programmable Ad hoc Networks*. PhD thesis, Lancaster University.

Sun, Y. and Belding-Royer, E. M. (2003). Dynamic address configuration in mobile ad hoc networks. *UCSB Technical Report 2003-11*.

Thomson, S. and Narten, T. (1998). IPv6 Stateless Address Autoconfiguration. RFC 2462.

Toner, S. and O'Mahony, D. (2003). Self-organising node address management in ad-hoc networks. *Lecture notes in Computer Science 2775*, pages 476–483.

Tschudin, C. F., Gold, R., Rensfelt, O., and Wibling, O. (2004). LUNAR: a Lightweight Underlay Network Ad-hoc Routing Protocol and Implementation. In *Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN'04), St. Petersburg*.

Tschudin, C. F., Lundgren, H., and Nordström, E. (2003). Embedding MANETs in the Real World. In *Personal Wireless Communications (PWC)*, pages 578–589.

Vaidya, N. H. (2002). Weak duplicate address detection in mobile ad hoc networks. In *MobiHoc '02: 3rd ACM international symposium on Mobile ad hoc networking & computing*, pages 206–216, New York, NY, USA. ACM Press.

Vergetis, E., Guerin, R., Sarkar, S., and Rank, J. (2005). Can Bluetooth succeed as a large-scale ad hoc networking technology? *IEEE Journal on Selected Areas in Communications (JSAC) Special Issue*, 23:644–656.

Weniger, K. (2003). Passive Duplicate Address Detection in Mobile Ad Hoc Networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*.

Weniger, K. (2005). PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks. *IEEE Journal on Selected Areas in Communications (JSAC) Special Issue*.

Zaruba, G., Basagni, S., and Chlamtac, I. (2001). Bluetrees - scatternet formation to enable bluetooth based ad hoc networks. In *IEEE International Conference on Communications(ICC)*.

Zhou, H., Ni, L. M., and Mutka, M. W. (2003). Prophet address allocation for large scale MANETs. *Ad Hoc Networks*, 1(4):423–434.