A Gateway Prototype for Coalition Tactical MANETs

Mazda Salmanian[1](✉), William Pase[2], J. David Brown[1],
and Chris McKenzie[3]

[1] Defence Research and Development Canada, Ottawa, Canada
{mazda.salmanian,david.brown}@drdc-rddc.gc.ca
[2] Armacode Inc., Ottawa, Canada
bill@armacode.com
[3] MIC, Ottawa, Canada
chris@mckenzieic.com

Abstract. Mobile ad hoc networks (MANETs) are well suited for tactical groups whose operations require that the network adapt to dynamic topology changes without the aid of centralized infrastructures. As more coalition forces deploy in tactical operations, their networks require inter-connectivity for sharing broadcast, multicast and unicast traffic from coalition applications such as situational awareness and sensor data. Inter-MANET connectivity, however, should not be at the cost of compromising a national MANET's sovereignty in terms of radio devices, subnet address space, and communication and routing protocols. In this paper, we describe our implementation of a gateway application that enables coalition tactical MANETs to inter-connect based on role names instead of IP addresses while keeping their national radios and networking sovereign and while protecting their private network addresses. We exhibit results and learned lessons from our laboratory experiments where we tested our gateway application in several MANET formations to ensure the functionality of relay connectivity, domain name service and network address translation features. The gateway application has potential to serve as a prototype for the future development of secure interoperability policies, service level agreements and standards at the tactical edge, e.g., for future NATO standardization agreements (STANAGs).

Keywords: MANET · Gateway · Interoperability · Domain name service · Network address translation · Wireless · Mobile ad hoc network Coalition networking

1 Introduction

As more national tactical forces are deployed in international coalition operations, they are expected to be interoperable to share basic application traffic such as situational awareness and sensor data. Future national forces are expected to take advantage of mobile ad hoc networking (MANET) technology, which adapts network topologies to tactical operations and enables dispersed nodes to pervasively inter-connect. The self-configuration benefits of MANET technology come from routing protocols that are

Y. Zhou and T. Kunz (Eds.): ADHOCNETS 2016, LNICST 184, pp. 330–341, 2017.
DOI: 10.1007/978-3-319-51204-4_27

used in conjunction with wireless radios and networking protocols. In a coalition deployment, national forces deploy with their own tactical radios and networking protocols and require gateways to share common application data with other nations who may not be equipped with the same radios and protocols. Currently, NATO's (North Atlantic Treaty Organization) protected core networking (PCN) concept relies on gateways in strategic enterprise networks [1] to facilitate quality of service (QoS) and policy negotiations; however, its approach is not yet relevant at the tactical edge due to the dynamic inter-networking challenges of MANETs. The authors in [2] present an architecture for secure interoperability between coalition tactical MANETs that promotes keeping national tactical radios and networking protocols sovereign. The architecture includes a gateway node designed for national MANETs that inter-connects with peer coalition gateways for secure information exchange.

In this paper, we describe such a prototype gateway application constructed on an Android device using two IEEE 802.11 (WiFi) radios, one internal and one external to the Android device. The gateway application is designed to relay the traffic between the two radios, connecting intra-MANET traffic flows on a national radio to inter-MANET traffic shared between the gateways on the coalition radio, e.g., NATO narrowband waveform (NBWF) [3–5]. In other words, each nation's MANET connects to another nation's MANET by its own gateway and without changing its service set identification (SSID) or subnet address. The implementation also includes domain name service (DNS) functions that enable role-based connectivity between national MANET nodes, simplifying the prerequisite requirement of possessing the internet protocol (IP) addresses of a destination node before information sharing. In addition, the gateway application protects the private network addresses of a national MANET by mapping them to designated public network addresses via network address translation (NAT).

We present results from our laboratory experiments where we tested our gateway application in several MANET formations with WiFi radios. We demonstrate that our prototype application inter-connects autonomous MANETs using sovereign radios and networking protocols, including frequency assignments, routing protocols and network addresses.

The rest of the paper is organized as follows. We present the basic inter-connectivity and networking of MANETs under several scenarios in Sect. 2 where we recommend a frequency assignment scheme for gateway radios given our measured metrics. In Sect. 3, we present results and learned lessons from our DNS testing trials. We present similar results in Sect. 4 for testing the NAT function. We provide a summary in Sect. 5.

2 Basic Connectivity

In this section, we describe experiments we conducted to examine the inter-connectivity and networking of MANETs across gateways with three scenarios. In the first scenario, a MANET from nation A (MANET-A) and a MANET from nation B (MANET-B) inter-connect using gateways. In the second scenario, MANET-B connects MANET-A and MANET-C (from nation C), acting as a relay network between nations A and C. In the third scenario, the MANETs of the three nations inter-connect using their own local gateways while the gateways form a MANET of their own.

As mentioned earlier, the gateway application on a node routes the traffic between the two radios on the gateway: one used for inter-MANET connections and one for intra-MANET traffic. We use the internal WiFi radio of the Android device (with the gateway application) to connect to the local intra-MANET side of the gateway. We enable the gateway device to also drive an external radio tuned to a shared gateway channel that connects to the inter-MANET side of the gateway. The operation of the second radio is made possible by a customized Android operating system, Cyanogenmod 12.1 with a modified Kali Linux Nethunter kernel made for Nexus 5 (phone) and Nexus 7 (tablet) devices [6]. The external radio used throughout our experiments is the TP-Link™ [7].

To simplify the experiments, we assign different radio frequency (RF) channels to represent different nations; the national subnet address and the MANET's SSID are other distinguishing features. We use the non-overlapping North American channel selection i.e., channels 1, 6 and 11 in accordance with [8].

Our experiments were performed in a laboratory under controlled static conditions. Mobility trials are planned for future work. The MANETs use the optimized link state routing protocol (OLSR) [9] for multi-hop connectivity. To enforce multi-hop connections and to avoid cross-talk between co-channel non-adjacent nodes, we used a separate customized application that generates 'iptables' commands and creates firewall rules. These rules permit testing of topologies that would otherwise require physically separating devices to restrict connectivity.

We used an iPerf [10] application to generate TCP and UDP (transmission control and user datagram protocols) traffic for the experiments and measured throughput to evaluate the effects of network changes in the scenarios.

Given an SSID, a common WiFi channel (via TP-Link) and a shared subnet address, the gateways discover one another as nodes of a MANET using the OLSR signaling. While gateway assignment is pre-determined in our experiments, future MANETs could use algorithms such as [11] to dynamically assign the gateway role to a node.

A gateway's primary task is to relay traffic from one of its radios to another, serving two SSIDs and subnets. The relay function in our gateway application is implemented by configuration settings of 'iptables' commands and OLSR routing table instructions. The gateway nodes are equipped with two OLSR instances, one for each RF interface; there is no cross-talk between the two OLSR instances.

Scenario 1. In this first scenario, depicted in Fig. 1, commander of nation A (CMDR-A) connects to commander of nation B (CMDR-B) under several cases, detailed in Table 1. In this stage of the experiment (basic connectivity) we assume that the commanders know one another's IP addresses. As shown in the figure, MANET-A is on subnet 192.168.11.xx and MANET-B is on subnet 192.168.12.xx.

The two phones in Fig. 2, which represent nodes 1 and 6 of Fig. 1, are CMDR-A and CMDR-B, respectively with addresses 192.168.11.10 and 192.168.12.11. The two tablets in Fig. 2 represent nodes 3 and 4[1] of Fig. 1 as GW-A (gateway of MANET-A) and GW-B (gateway of MANET-B), respectively, each with two radios, one internal

[1] Notations for nodes 2 and 5 are reserved for multi-hop configurations of this scenario.

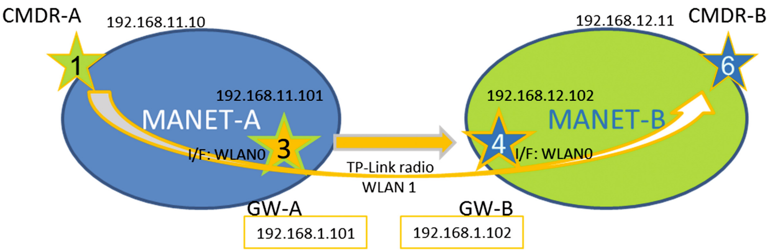


Fig. 1. The configuration of two MANETs in Scenario 1. Nodes 3 and 4 are gateways with two radios tuned according to use cases in Table 1. The internal radio interface (I/F) is denoted WLAN0, while the external radio interface is denoted WLAN1. MANETs are partitioned with three parameters: The MANET's SSID, the operating WiFi channel and the subnet address. The subnet address of the gateway MANET is 192.169.1.xx.

Table 1. Channel assignments of the radios in Scenario 1.

Use case	MANET-A	GW-A	GW-B	MANET-B	Description
0	11	11/11	11/11	11	One flat MANET, base measure
1	11	11/11	11/11	11	Two MANETs, two GWs, all @ Ch.11
2	11	11/11	11/06	06	Two MANETs, one GW @ Ch.11/06
3	01	01/11	11/06	06	Two MANETs & GWs, Ch. 01/11/06

and one TP-Link external to the tablet. The external radios for inter-gateway communication share subnet 192.168.1.x. Traffic packets are generated by the iPerf application at CMDR-A node destined for CMDR-B's IP address. The packets are sent to GW-A by default due to their unknown destination subnet address in MANET-A; every MANET node is assigned a default gateway. The packets are then forwarded to GW-B where their subnet addresses are recognized and where they are forwarded to CMDR-B.

The use cases tabulated in Table 1 differ in the RF channels assigned to the MANET radios and to the gateways. For example in use case 3, GW-A is assigned channel 01 (intra-MANET radio) and channel 11 (inter-MANET radio). In addition:

- Case 0 also differs from the other use cases in its network address assignments. In this use case we make a baseline measure of throughput from a flat (same subnet) multi-hop network. Here, we expect co-channel interference to contribute to collisions and loss of packets.
- Case 1 examines the potential overhead of the gateway application and its introduction to two MANETs separated by subnet addresses but not by radio frequency. All nodes, including the gateways' internal and external radios, are tuned to channel

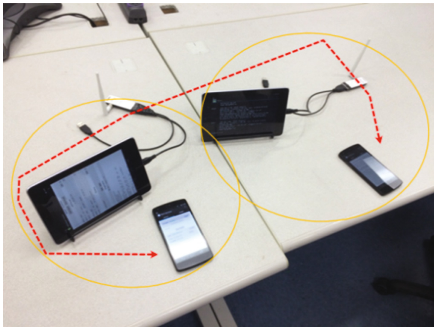


Fig. 2. The laboratory configuration of two MANETs in Scenario 1. The two MANETs are depicted in yellow ellipses. The two tablets (representing nodes 3 and 4 of Fig. 2) are gateways with two radios, one internal and one external to the tablet. The external radio is the TP-Link. (Color figure online)

11, as they were in case 0. The subnet addresses of the two MANETs are 192.168.11.xx and 192.168.12.xx, and that of the gateway MANET is 192.168.1.xx.

- Case 2 is designed to measure the effect of reduced co-channel interference. One MANET is assigned to operate on channel 6; its gateway's internal radio is also tuned to channel 6 while the rest of the nodes operate on channel 11.
- Case 3 offers the environment in which we measure potential improvements in throughput by dedicating channel 11 to inter-gateway communication. Both gateways' external radios are tuned to channel 11 while the MANETs are tuned to channels 1 and 6, respectively.

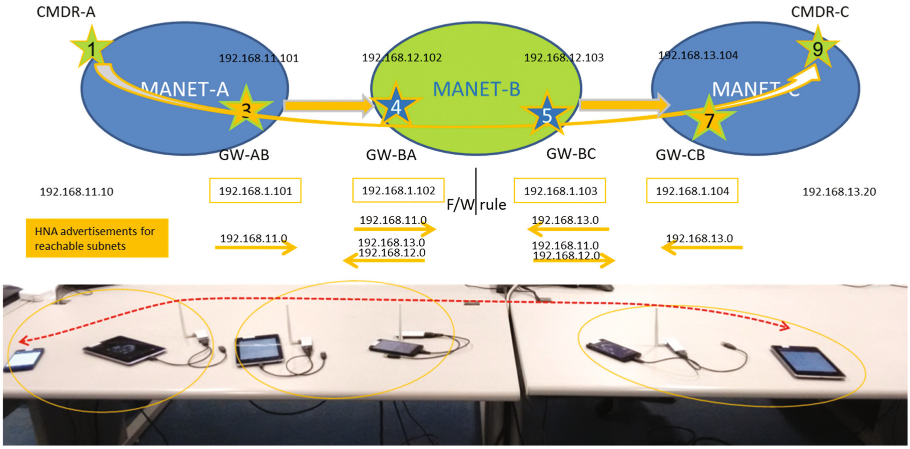


Fig. 3. The configuration of three MANETs in Scenario 2. Nodes 4 and 5 are gateways of MANET-B depicted in our laboratory experiment with a Nexus 7 tablet and a Nexus 5 phone, respectively. Their external radios are the TP-Link.

Scenario 2. In Scenario 2 (single use case), MANET-B provides connectivity between MANETs A and C so that CMDR-A establishes a multi-hop connection to CMDR-C. This scenario is depicted in Fig. 3.

Scenario 2 continues the theme of minimizing co-channel interference; MANETs A, B and C are assigned to operate on channels 1, 6 and 1 respectively, while the gateways operate on one common channel 11. This test ensures that an iPerf-generated packet destined from CMDR-A to CMDR-C is relayed correctly through the gateways in MANET-B, leaving subnet 192.168.11.x through 192.168.12.x for 192.168.13.x. MANET-B has two gateways: a firewall rule forces them to establish their peer-to-peer connection via their internal radios under subnet 192.168.12.x, leaving their TP-Links on channel 11 under subnet 192.168.1.x to serve connections to each of their neighbouring MANETs. In this scenario, the OLSR on the gateway nodes is configured (via our gateway application) to advertise host network association (HNA) messages so that subnets can be found for route discovery. The HNA messages advertise network routes (subnet IDs) in the same way topology control (TC) messages advertise host routes. We avoid (and recommend against) using multiple interface declaration (MID) messages that advertise all the internal routes to other subnets; this ensures that internal routes are kept private on a multi-national scenario.

Scenario 3. In Scenario 3, the traffic flow is from CMDR-A to CMDR-C. This scenario configuration is depicted in Fig. 4.

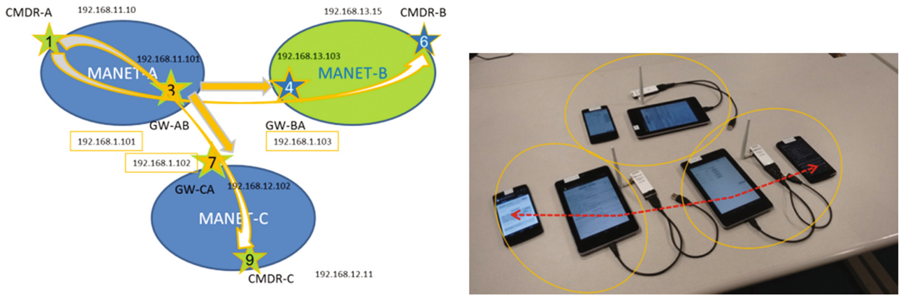


Fig. 4. The configuration of three MANETs in Scenario 3. Nodes 3, 7 and 4 are gateways that form a MANET of their own; these gateways are depicted in our laboratory experiment with Nexus 7 tablets. Their external radios are the TP-Link.

Scenario 3 is similar to Scenario 2 in that MANETs A, B and C are assigned to operate on channels 1, 6 and 1 respectively, while the gateways operate on one common channel 11. In Scenario 3, however, each MANET is assigned one gateway whereas in Scenario 2, MANET-B had two gateways.

Laboratory Results. We present our experimental results and summarize learned lessons of our three scenarios. To put the throughput results in perspective, we first present the commercial specifications of our link connections. The specifications are:

- TP-Link to the tablet/phone connection is USB 2.0 (universal serial bus) with maximum data rate up to 480 Mbps.

- Internal radios of the tablets are (802.11b/g/n) rated up to 150 Mbps.
- Internal radios of the phones are (802.11a/b/g/n/ac) rated up to 300 Mbps.
- TP-Link to TP-Link connection (802.11n) is rated up to 150 Mbps; this is the main inter-gateway connection common for interoperability in our scenarios and the relative bottleneck among the links.

The TCP and UDP throughput results are presented in Figs. 5 and 6, respectively. Each scenario (and use case) is run ten times; each time (i.e., every point on the graph) is an averaged value over a 30-second iPerf transmission. The TCP packets are transmitted at the highest possible rate for assured reception; the iPerf UDP packets are transmitted at 50 Mbps load.

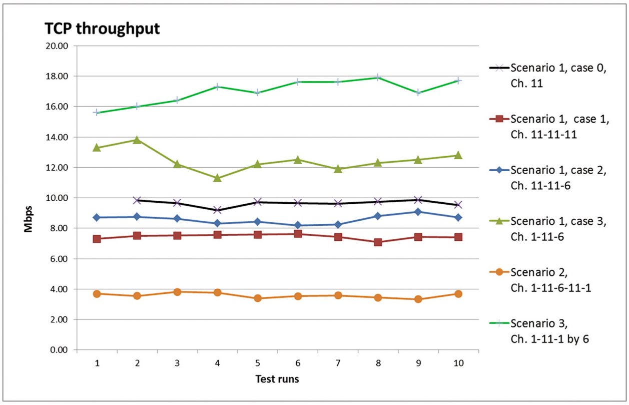


Fig. 5. TCP throughput results of Scenarios 1 to 3.

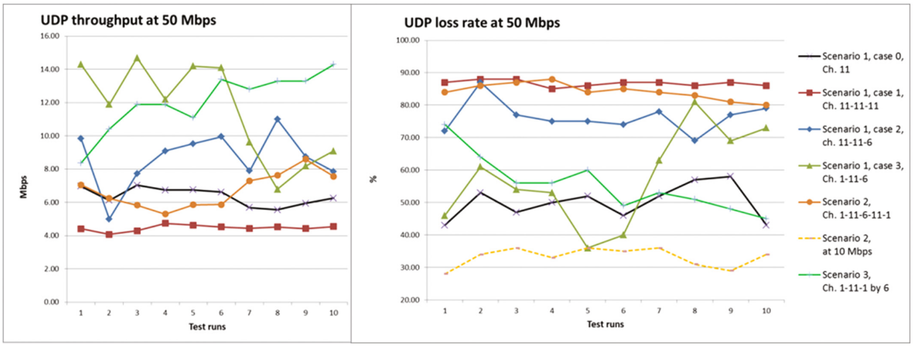


Fig. 6. UDP throughput and loss rate results of Scenarios 1 to 3.

The TCP throughput increases of Scenario 1 cases 1 to 3 are well noted and result from the reduction of co-channel interference. The throughput of Scenario 1 case 0, however, is higher than those of cases 1 and 2. The MANET in Scenario 1 case 0 is a flat merged network using channel 11; with no gateway, it presumably has the most co-channel interference among the scenarios. This throughput observation indicates that there is overhead associated with the gateway application managing a connection in a two-MANET formation partitioned by subnet addresses (Scenario 1 cases 1 and 2). We also presume that the carrier sense multiple access (CSMA) of the 802.11 radios had the opportunity to optimize access time to channel 11.

The channel transition of the iPerf traffic for Scenario 1 case 3 is 1-11-6 whereas that of Scenario 3 is 1-11-1 next to a MANET operating on channel 6. Our results show that Scenario 3 produced higher average throughput than Scenario 1 case 3. It is possible that co-channel sensing of CSMA influences transmission times such that optimum throughput performance may be achieved, e.g., by performing bulk acknowledgements.

In the UDP throughput results shown in Fig. 6, we note that the data points are not as stable as those of TCP in Fig. 5 because UDP is a connectionless protocol and does not re-transmit lost or erroneous packets. Here, the throughput of Scenario 1 case 1 is lower than Scenario 2; both have similar loss rates. This observation indicates that co-channel interference in Scenario 1 case 1 reduces the throughput of UDP packets such that it is lower than hopping over two additional gateways in Scenario 2 where there is no co-channel interference.

The HNA feature of OLSR is implemented per (radio) interface in order to enforce control over the direction of advertised subnets and to avoid circular routes. This allows us to dedicate a gateway to a neighbouring MANET – the external radio of the gateway that connects to the neighbour MANET advertises a specific subnet.

A MANET providing a connection service between two MANETs (e.g., Scenario 2) must advertise subnet addresses inside its network as well as outside. Every MANET node is assigned a default gateway; these internal HNA advertisements help the default gateway of a node route the message to the subnet of the destination address. These internal HNA messages are not needed in a MANET that has only one gateway serving multiple neighbours, such as the formation in Scenario 3.

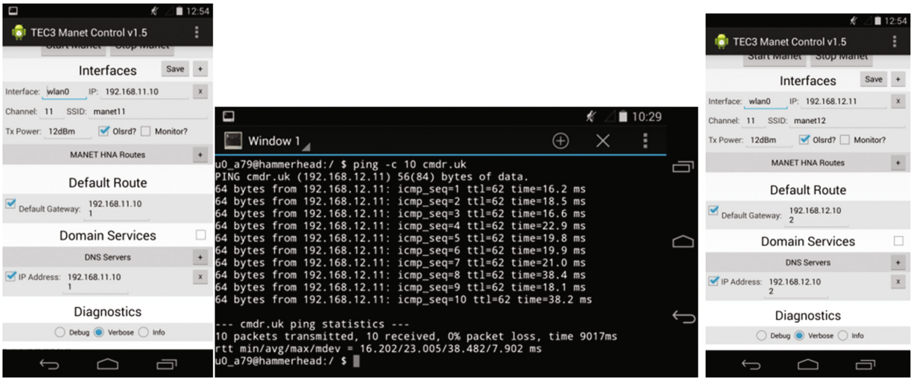
3 Domain Name Service

Domain name service (DNS) is an Internet standard protocol made of a collection of request for comments (RFC) documents [12] published by the Internet Engineering Task Force. The messaging exchange in the protocol allows a node to address its destination by a name, instead of by the numerical representation of the IP destination address. In this work, we use the role name of a MANET node such as CMDR. Earlier, in the basic connectivity section, we had assumed that the two commanders in Fig. 1 were in possession of one another's IP addresses. Now, the IP address of the destination does not have to be known a priori at the source. With the DNS feature, CMDR-A can address CMDR-B by its role name and its domain name, e.g., cmdr.b representing the commander's role name in MANET-B domain.

The DNS protocol message flow and its trigger by CMDR-A are explained below with reference to Fig. 1. A traffic message is formed with cmdr.b as the destination address. The message is queued until DNS software resolves the 'RoleName.domain' and maps it to an IP address. A DNS signaling message is sent to GW-A, the default gateway of the source node, CMDR-A. The DNS signaling message is forwarded to

GW-B because domain '.b' is identified with GW-B in GW-A. At GW-B, the DNS software resolves the 'RoleName.domain' to the IP address mapping of CMDR-B. GW-B responds to GW-A with the IP address for CMDR-B. Then, GW-A forwards the signaling message to CMDR-A's queue where the original traffic message is stored. Subsequently, the traffic message is sent from 192.168.11.10 to 192.168.12.11.

In Fig. 7, we present a screen shot of our DNS experiment where cmdr.ca generates a 'ping' command to cmdr.uk whose address is successfully resolved to 192.168.12.11. In the experiment, the '.ca' and '.uk' represent Canada and United Kingdom domains, respectively replacing CMDR-A and CMDR-B. The DNS query (signaling message) is triggered per 'traffic flow', i.e., as needed. The result of a query is cached for a configurable time-to-live (TTL). In our Android implementation, we use a Linux DNS server (DNSmasq) and replace the Android default DNS, i.e., Google, because it requires connection to the Internet[2]. The DNS server is currently implemented on the gateway nodes; however, it can be implemented on any node in the MANET, so long as a traffic source can route DNS queries to the DNS server node.



Interfaces

Interface: wlan0 IP: 192.168.11.10

Channel: 11 SSID: manet11

Tx Power: 12dBm ☑ Olsrd? □ Monitor?

MANET HNA Routes

Default Route

☑ Default Gateway: 192.168.11.10
1

Domain Services □

DNS Servers

☑ IP Address: 192.168.11.10
1

Diagnostics

○ Debug ● Verbose ○ Info

```
u0_a79@hammerhead:/ $ ping -c 10 cmdr.uk
PING cmdr.uk (192.168.12.11) 56(84) bytes of data.
64 bytes from 192.168.12.11: icmp_seq=1 ttl=62 time=16.2 ms
64 bytes from 192.168.12.11: icmp_seq=2 ttl=62 time=18.5 ms
64 bytes from 192.168.12.11: icmp_seq=3 ttl=62 time=16.6 ms
64 bytes from 192.168.12.11: icmp_seq=4 ttl=62 time=22.9 ms
64 bytes from 192.168.12.11: icmp_seq=5 ttl=62 time=19.8 ms
64 bytes from 192.168.12.11: icmp_seq=6 ttl=62 time=19.9 ms
64 bytes from 192.168.12.11: icmp_seq=7 ttl=62 time=21.0 ms
64 bytes from 192.168.12.11: icmp_seq=8 ttl=62 time=38.4 ms
64 bytes from 192.168.12.11: icmp_seq=9 ttl=62 time=18.1 ms
64 bytes from 192.168.12.11: icmp_seq=10 ttl=62 time=38.2 ms

--- cmdr.uk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 16.202/23.005/38.482/7.902 ms
u0_a79@hammerhead:/ $
```

Interfaces

Interface: wlan0 IP: 192.168.12.11

Channel: 11 SSID: manet12

Tx Power: 12dBm ☑ Olsrd? □ Monitor?

MANET HNA Routes

Default Route

☑ Default Gateway: 192.168.12.10
2

Domain Services □

DNS Servers

☑ IP Address: 192.168.12.10
2

Diagnostics

○ Debug ● Verbose ○ Info

Fig. 7. A 'ping' command from cmdr.ca (CMDR-A in Fig. 1) is translated to cmdr.uk's IP address (CMDR-B) via the DNS server implemented on GW-A and GW-B. Screen shots of our customized application on Nexus 5 phones representing CMDR-A (left) and CMDR-B (right) show the CMDRs' default gateway and DNS server addresses as 192.168.11.101 and 192.168.12.102, respectively.

Figure 7 also shows screen shots of our customized application on Nexus 5 phones representing CMDR-A (left) and CMDR-B (right) of Fig. 1. As mentioned earlier, in our customized application, every node is assigned a default gateway, and now, in this stage, a default DNS server. It is this customized application that enables a node to control its radio interfaces, act as or assign a gateway or a DNS server. The screen shots of CMDR nodes show the CMDRs' default gateway and DNS server addresses as 192.168.11.101 and 192.168.12.102, respectively. In our experiments, we successfully

[2] DNSmasq allows us local control to add and to resolve domain names.

performed end-to-end ‘ping’ and ‘traceroute’ commands on Scenarios 1, 2, and 3, testing the DNS function in all aforementioned MANET configurations, but for brevity we do not show their screen captures here.

4 Network Address Translation

We extend the features of our custom application to include network address translation (NAT) such that the DNS query response returns a configurable public IP address of a MANET node’s RoleName (in the query) not its actual private IP address. The private IP address of the destination node is not only kept sovereign within its MANET domain, it is further protected by the NAT feature such that it is not shared outside of the MANET domain.

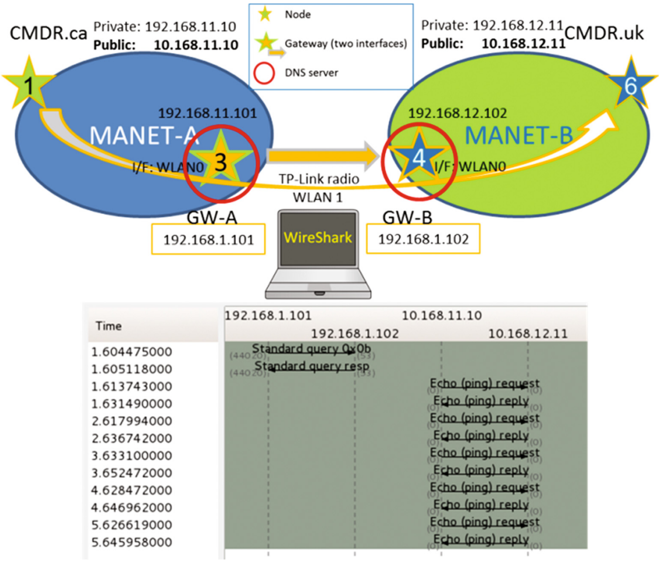
We have chosen to implement this feature on the gateway node which is at the edge of the MANET as the final trusted node that releases traffic packets to external domains. An outgoing traffic packet from a source node is sent with a private source IP address and a public destination IP address, acquired by the DNS protocol. When this packet arrives at the default gateway (of the source node), its private source IP address is mapped to a public source IP address. This process is referred to as a source NAT.

Analogously, an incoming traffic packet that arrives at the gateway carries public source and destination IP addresses. At the gateway, by a process referred to as a destination NAT, the packet’s public destination IP address is mapped to a private destination IP address.

We present Fig. 8 as evidence of our NAT implementation. The Wireshark$^{\text{TM}}$ flow capture of Fig. 1 configuration is shown where cmdr.ca (CMDR-A) generates a ‘ping’ command to cmdr.uk (CMDR-B) whose address is successfully resolved to 10.168.12.11. This address is the public address of cmdr.uk as it is in 10.x.x.x network address space, not the 192.x.x.x network address space where the private address resides. The flow capture shows the implementation of both source and destination NATs as the private addresses are protected and hidden.

Source and destination NAT techniques are employed and executed in the Linux kernel. We use the Netfilter feature of the Linux kernel to implement NAT in our application. The application generates source and destination NAT rules, S-NAT and D-NAT respectively, such that the IP Table gets reconfigured with ‘iptables’ commands.

It is important to note that the gateway node itself, as a member of the MANET, must subject its internal (radio) traffic to the NAT rules. It is also important to note that with our scheme, the subnet address space of the public domain becomes limited as the number of nodes increases and their addresses are mapped to a public address. In a coalition operation, the public subnet addresses must be managed and even pre-assigned to the participating nations.



```
Time           192.168.1.101              10.168.11.10
                             192.168.1.102              10.168.12.11
1.604475000   (44020) Standard query 0x0b (53)
1.605118000   (44020) Standard query resp (53)
1.613743000                                  (0) Echo (ping) request (0)
1.631490000                                  (0) Echo (ping) reply (0)
2.617994000                                  (0) Echo (ping) request (0)
2.636742000                                  (0) Echo (ping) reply (0)
3.633100000                                  (0) Echo (ping) request (0)
3.652472000                                  (0) Echo (ping) reply (0)
4.628472000                                  (0) Echo (ping) request (0)
4.646962000                                  (0) Echo (ping) reply (0)
5.626619000                                  (0) Echo (ping) request (0)
5.645958000                                  (0) Echo (ping) reply (0)
```

Fig. 8. A ‘ping’ command from cmdr.ca is translated to cmdr.uk’s public IP address via the DNS server and NAT implemented on GW-A and GW-B. Screen shot of Wireshark captured messages shows the gateway addresses as 192.168.1.101 and 192.168.1.102, and the public addresses of the two commanders as 10.168.11.10 and 10.168.12.11, respectively in subnet 10.x.x.x. not 192.x.x.x.

5 Summary

Gateways provide traffic relay service between two autonomous MANETs. In this work we presented experimental results performed on three MANET scenarios. We have shown that even though a gateway is an extra relay in the MANET, there is a noticeable improvement in throughput when the frequency assignments are managed in a coalition deployment such that co-channel interference is reduced. Frequency management, however, should be weighed against the inevitable exposure to jamming as more frequency allocations (different channels) mean more targets.

We implemented the relay functionality along with DNS and NAT in a customized Android application. We implemented the gateway discovery function by taking advantage of the OLSR protocol and its HNA messages. The gateway application manages configuration settings such that MANETs can be partitioned by RF radio channels, subnet addresses and SSIDs.

From a security perspective, we showed that MANETs can operate using sovereign private subnet addresses and only share their assigned public subnet addresses. The public address space assignments in a coalition deployment, however, require careful planning to avoid public-address collisions between network gateways.

In this work, we have realized the architecture that was detailed in [2]. For brevity, we have omitted the prototyping results of the encryption strategy as they are out of scope of this work.

In a MANET, there is no “physical” way to ensure that a high-assurance mobile exchange point is connected to the perimeter of the network. Appropriate architectures and algorithms may employ multiple exchange points or allow for a single mobile exchange point to serve as the “logical” gateway between two networks. Along that theme, we are considering the following areas in our future research: policy enforcement at the tactical edge, distributed DNS and load balancing between multiple gateways. These new architectures will ensure that network connectivity between two partners will be more robust (i.e., survivable) despite mobility and changes to topology.

Acknowledgment. The authors wish to thank Ms. Susan Watson for her valuable time and suggestions for this work.

References

1. Lies, M., Dahlberg, D., Steinmetz, P., Hallingstad, G., Calvez, P.: The Protected Core Networking (PCN) Interoperability Specification (ISPEC), NATO Communications and Information Agency. Technical report 2013/SPW008905/13 (2013)
2. Salmanian, M., Brown, J.D., Watson, S., Song, R., Tang, H., Simmelink, D.: An architecture for secure interoperability between coalition tactical MANETs. In: 2015 IEEE Military Communications Conference, MILCOM 2015 (2015)
3. North Atlantic Treaty Organization (NATO), Standardization Aggrement (STANAG) 5631/AComP-5631, Narrowband Waveform Physical Layer, 1 edn. Ratification Draft (2015)
4. North Atlantic Treaty Organization (NATO), Standardization Aggrement (STANAG) 5632/AComP-5632, Narrowband Waveform Link Layer, 1 edn. Ratification Draft (2015)
5. North Atlantic Treaty Organization (NATO), Standardization Aggrement (STANAG) 5633/AComP-5633, Narrowband Waveform Network Layer, 1 edn. Ratification Draft (2015)
6. Kali NetHunter Documentation (2016). https://github.com/offensive-security/kali-nethunter/wiki
7. TP-Link. http://www.tp-link.com/en/products/details/TL-WN722N.html
8. IEEE Computer Society, IEEE Standard for information technology - telecommunications and information exchange between systems local and metropolitan area networks - specific requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11™ (2012)
9. Clausen, T., Jacquet, P.: Optimized Link State Routing Protocol (OLSR), RFC 3626, IETF (2003)
10. iPerf - The network bandwidth measurement tool (2016). https://iperf.fr/
11. Wong, S.H.Y., Chau, C.K., Lee, K.W.: Managing interoperation in multi-organization MANETs by dynamic gateway assignment. In: 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops (2011)
12. Domain Name System (2016). https://en.wikipedia.org/wiki/Domain_Name_System