Alternatives to Binary Routing Policies Applied to a Military MANET Coalition

Florian Grandhomme
DGA-IP
France
florian.grandhomme@intradef.gouv.fr

Gilles Guette
IRISA, Université de Rennes 1
France
gilles.guette@irisa.fr

Adlen Ksentini
Eurecom
France
adlen.ksentini@eurecom.fr

Thierry Plesse
DGA-MI
France
thierry.plesse@intradef.gouv.fr

Abstract - New generation radio equipment, used by soldiers and vehicles on the battlefield, form ad hoc networks and specifically, Mobile Ad hoc NETworks (MANET). The battlefields where these equipment are deployed include a majority of coalition communication. Each group on the battleground may communicate with other members of the coalition and establish inter-MANET links. These inter-MANET links are governed by routing policies that can be summarized as *Allowed* or *Denied* link. However, if more than two groups form a coalition, blocked multi-hop communications and non-desired transmissions due to these restrictive policies would appear. In this paper, we present these blocking cases and theoretically evaluate their apparition frequency. Then, we present two alternatives to extend the binary policies and decrease the number of blocking cases. Finally, we describe an experimental scenario containing a blocking case and evaluate our propositions and their performance. ***Keywords*—ad hoc, inter-domain, routing, policy**

I. Introduction

On the battleground, several nations or entities can collaborate to fight against one or several enemies. These elements, sharing the same goal, can be grouped under a coalition. However, each entity of the coalition would keep control on its transmitted data. This can be done by using routing policies which define the level of data each group would share with the others. On wired networks, BGP (Border Gateway Protocol) [10] ensures these functions and allows network operators to collaborate in order to build the Internet network. Traffic engineering can be done to promote some domains and reject some others. In military environments, the exchanged data can be very sensitive leading that these routing policies can simply be summarized as "permitted" or "denied" (*i.e.* binary policies). Due to soldiers mobility, allies can be distant (not in direct range communication) requiring multi-hop communication. If a denied member of the coalition is on the route between two allies, this communication would be interrupted. In the same way, once you transmit your routing data to a trusted neighbor, routing protocol naturally send information to other neighbors, that can be untrusted members, creating non-desired transmission. Consequently, it is necessary to provide solutions to avoid the above-mentioned cases, and hence establish these communications. In this paper, we first evaluate the amount of blocked communications and non-desired transmitted information due to binary policies. Then, we propose two methods to extend these routing policies. Finally, we apply our propositions in a network example and evaluate their performance.

II. Current limitations of binary policies

In this section, we evaluate the limitations of the policy model of our previous work ITMAN [6][1]. Two aspects will be handled. The blocked communications between distant allies, and the non-desired transmissions.

A. Multi-hop blocked communications

Due to the binary policies, distant allies would be unable to communicate. In Figure 1, we illustrate this situation by an example. Groups A and C, that are distant and allowed to communicate, are blocked by the denied policy between B and C on the route. Usually, we consider the following situation as a blocking case. Two groups, that are allowed to communicate, not directly connected and other groups are part of the data route. However, if two adjacent groups of the data route have a deny policy between them, they will block the communication which should be established between the two allowed distant groups.

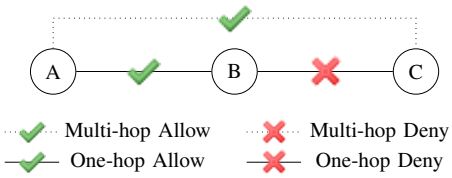


Figure 1: Example of a blocking case

These blocking cases are evaluated by using two matrices: the connectivity matrix (M_c) of the groups, and the policy matrix (M_p) applied between the groups. M_c and M_p are two square matrices of size n, where n is the number of groups in the coalition. Each group is designed by a number from 1 to n. We use the topology of Figure 2a as example. The matrix representation of the connections in this coalition, illustrated in Figure 2b, is done as follows:

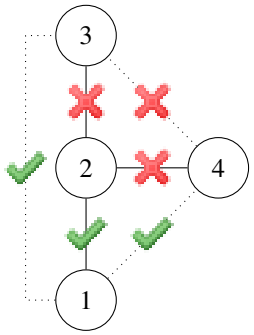
- $M_c[i][j] = M_c[j][i]$: links are symmetric,

[1]Reading this article is recommended to understand the whole issues aimed in this paper.

- $M_c[i][j]$ = 1: groups i and j are directly connected (for $i \neq j$),
- $M_c[i][j]$ = 0: groups i and j are not directly connected (for $i \neq j$),
- $M_c[i][i]$ = 2: not valuable connection (for $i = j$).

The matrix representation of the policies applied in the coalition, illustrated by Figure 2c is done as follows:

- $M_p[i][j] = M_c[j][i]$: policy is symmetric,
- $M_p[i][j]$ = 1: groups i and j are allowed to exchange data (for $i \neq j$),
- $M_p[i][j]$ = 0: groups i and j are not allowed to exchange data (for $i \neq j$),
- $M_p[i][i]$ = 2: not valuable policy (for $i = j$).



(a) An example of Ad Hoc topology and associate policies

$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{bmatrix}$$

(b) Matrix representation of the topology (M_c)

$$\begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 2 \end{bmatrix}$$

(c) Matrix representation of the inter-domain policy (M_p)

Figure 2: Topology and policy representations for a given topology

In this evaluation, we will compute all possible topologies for various number of groups. If four groups form the coalition, then 64 possible topologies will result. For a sake of simplification, we consider that all links are symmetric, if group 1 is connected to group 2, then, group 2 is also connected to group 1. Furthermore, the number of nodes in groups is not important in our case. Our objective is to evaluate inter-group blocking cases, which is independent of the number of nodes in groups. On each possible topology for a fixed number of groups, we apply all the possible combination of policies. Thus, to evaluate the amount of cases for a four-group coalition, we compute all the 4.096 topology/policy combinations (64 policy combinations applied on the 64 possible topologies).

For each couple of topology/policy, represented by M_c and M_p, we calculate two routing tables on each group of the network. The first is made with the Dijkstra algorithm, to calculate the shortest path to other groups. The second one is calculated with a variation of the Dijkstra algorithm to have a routing table influenced by the policies. This variation is about the link cost calculation. If two groups are adjacent but their policy do not allow them to communicate, the cost link is considered as infinite (*i.e.* the groups are not in range).

Once the two routing tables have been computed, we check the following criteria to determine if the current network and its topology/policy combination have blocked communications:

- Groups A and B are allowed to communicate,
- Groups A and B are not connected directly,
- Group A can reach group B via the basic routing table, and reciprocally,
- Group A can not reach group B via the policy table, and reciprocally.

The amount of blocking cases is evaluated from two point of views:

(i) the network view,
(ii) the group view.

Considering the example of Figure 2a, communications between groups 1 and 3 are blocked, as there is the group 2 on the route, which does not want to communicate with the group 3. Even if other couples of groups are able to exchange data, we consider the network as blocked. In networks with more than three groups, this case would nearly appear at least once for each combination of topology/policy. For this reason, we decided to evaluate the blocking cases from the group view. If a couple is blocked, we continue the computation for the other couple of groups. For the example of Figure 2a, there are six group couples to study (1-2 ; 1-3 ; 1-4 ; 2-3 ; 2-4 ; 3-4), mainly due to the symmetric links and policies. Couples 1-4 and 1-3 satisfy the blocking conditions that have been listed previously. Considering this network from the group point of view, the blocking rate is about 33.33%.

Figure 3 presents the amount of blocking cases depending on the number of groups in the coalition. As presented previously, it is computed on the network and group views.

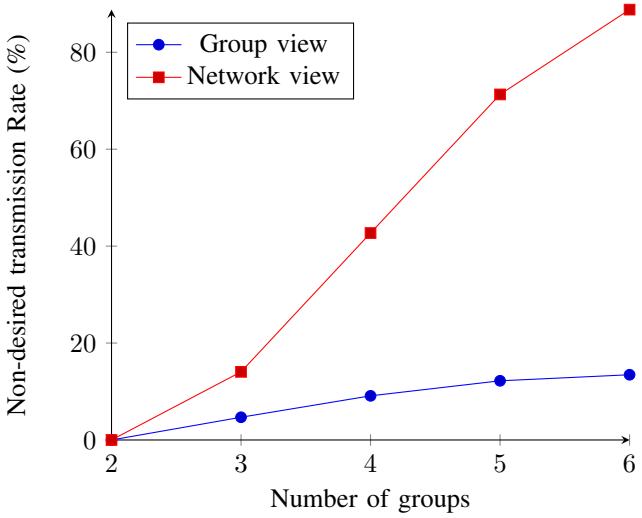


Figure 3: Theoretical blocked communications rates

These results show that from the group point of view, there is a small rate of blocked communications due to binary policies. However, the probability to have at least one blocking case in the whole network fastly increases in comparison to the number of groups. This result means that in a coalition network, if restricted policies are applied, some information

would not be transmitted in more than half of the cases. Consequently, there is a need to extend these policies in order to improve the communication rate.

B. Non-desired transmission

The other problem that can occur due to binaries policies is the non-desired transmission of routing information. Once you send your routing data to a trusted neighbor, nothing prevents him from sending your data to a distant group. However, the original sender do not want them to be received by an untrusted group, from its policy view. The example of Figure 4 illustrates this situation.

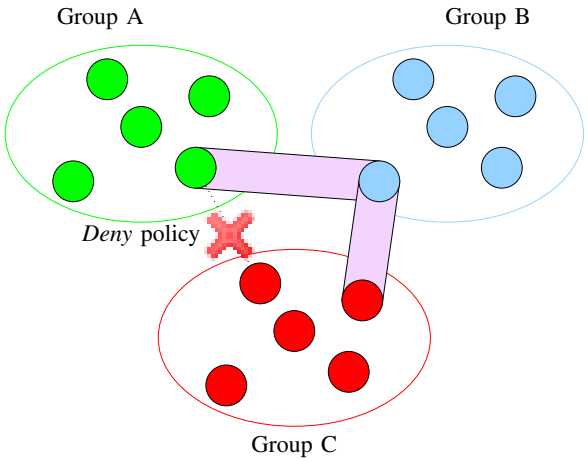


Figure 4: Representation of non-desired transmission issue

On the same matrix representation, we compute all possible topologies and policies. On each network, for each couple of groups, we check the following criteria to evaluate the amount of non-desired transmission:

- Groups A and B are not allowed to communicate,
- Group A can reach group B via the basic routing table, and reciprocally,
- All reachable groups via Group A policy table are selected,
- If at least one of them can reach Group B, there is a non-desired transmission.

Figure 5 presents the amount of non-desired transmission cases depending on the number of groups in the coalition. As presented for the blocked communications, it is computed on the network and group views.

In a network where several domains are interconnected, a significant rate of routing information are leaked by other groups. In large coalition, more than a half of the communications can be transmitted against the will of the source.

After the theoretical evaluation of blocked or non-desired communications, we pointed out that a need to improve the routing policy in inter-domain communications to improve global performance. In the next section, we propose two algorithms to soften the binary policies.

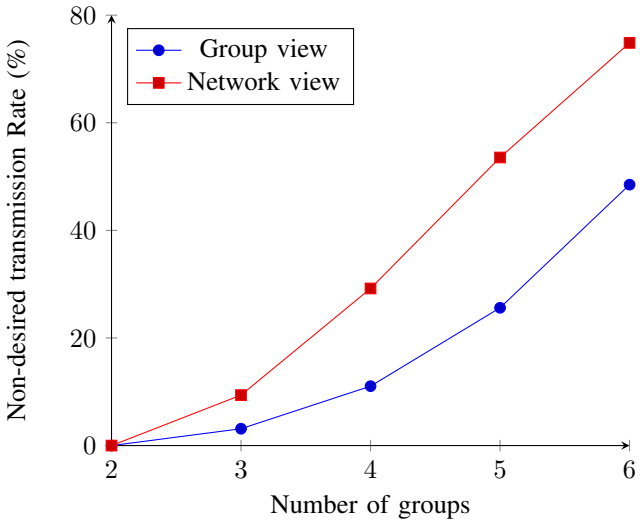


Figure 5: Theoretical non-desired transmission rates

III. Extensions of binary routing policies

In this section, we present two propositions to improve inter-group communications. We make the assumption that in the coalition context, even if there are communication restrictions between some groups, they collaborate and transmit routing data of other groups. With this availability assumption, we focus on the confidentiality of the transmitted data through the other groups. Furthermore, these propositions are alternatives to the *Allow* or *Deny* policies that will not be used anymore.

A. Filtered announcements

The first solution aims to prevent groups from announcing non-desired nodes in their groups. This is a functionality of BGP that we apply in the MANET environment. To explain the method, we use the following example, represented by Figure 6.

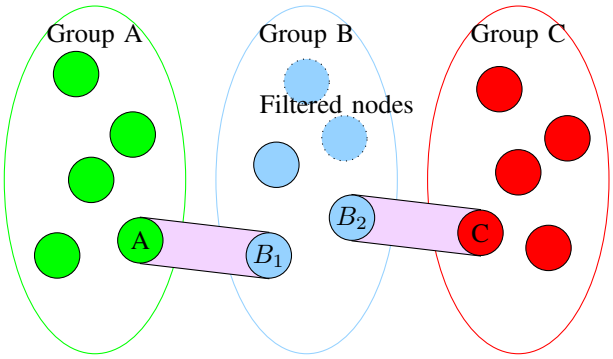


Figure 6: Inter-MANET communication with the filtering solution

Group A and group C are allowed to communicate; however, B and C have low-level trust. Our proposition to make the two distant A and C groups communicate, even if there is a blocking group on the route, is as follows. Groups A and C

have no restriction on their announcements and can broadcast all the routes. B1 and B2 receive these new accessible nodes and share them in group B. Once routes from group A reach B2 (and reciprocally routes from group C reach B1), the gateways B1 and B2 remove from the announcement all the nodes from group B they do not want to share. B1 and B2 act as gateways *i.e.* as nodes that have at least one neighbor in another group. They have no particular capacities or features but are useful to establish communications. This method let A and C exchange first routing data, then data, without knowledge of group B topology. When A sends a packet to C, the packet is forwarded to the gateway of A, which forwards to B1, designed as next hop. B1, by its intra-domain routing protocol, sends the packet to B2. Finally, B2 delivers the packet to group C.

B. Tunneling

The second solution we propose is to build ciphered communications through the network and not only inside groups or between two adjacent groups. The main advantage of this solution is to keep confidential communications, whatever the groups on the data route are. As illustrated in Figure 7, two levels of communication exist:

- Group level: application data are exchanged inside the groups. Ciphered with the group key (K_{group}),
- Inter-domain level: application data are exchanged between groups. Ciphered with a shared key, previously created in the coalition plan (K_{AC}, for group A and group C communication).

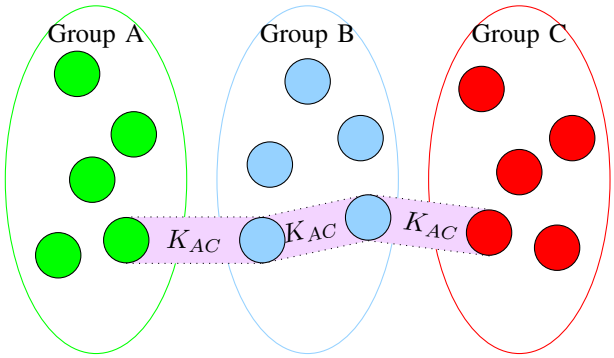


Figure 7: Inter-MANET communication with the tunneling solution

IV. Experimentation

In this section, we will present the conducted experimentation, the assumptions and the comparison points for the propositions of Section III.

A. Functional assumptions

In this part, we introduce some assumptions and definitions to describe how the coalition is deployed. On the communication level, we consider that all the groups of the coalition use the same technology, particularly about layer 2 protocols (Data Link layer) and layer 3 protocols (Network layer). In our experimentation, all nodes use WiFi and IPv4 technologies since TDMA military devices were not possible to use. In other deployments, it could also be UHF/VHF, TDMA... This assumption is made to guarantee the transmission of routing data through the network. The routing protocol used to build the network is OLSR [4]. This proactive protocol periodically sends HELLO messages to discover its neighbors. Once the neighbors have been discovered, Topology Control (TC) messages are in charge to report the link costs to calculate routes to all available nodes. The timers used for OLSR protocols are those advised in RFC 7181 (Hello 2s, TC 5s).

On the security level, we consider that all the exchanged data are ciphered. Each group uses its own group key. External nodes of the group can intercept communication but ciphered packets prevent them from understanding communications. Each node has two elements that enable it to prove its identity to the other members of the coalition; a public/private key pair with an associated certificate, and the trusted certificate of the authorities used in the coalition. Given these elements, each node is able to send ciphered and/or signed messages in the coalition.

On the organizational level, each node embeds a policy file. These policies are defined during the mission preparation. Therefore, nodes are operational to build the coalition network. According to each proposition of Section III, the policy file is organized as follows:

- Filtered announcements: this file contains all the nodes of the group that are not allowed to be announced for inter-domain communications.
- Tunneling: this file contains all external nodes that are allowed to communicate and the associate ciphering key. This policy is consistent all over the coalition; *i.e.* if A trusts B then, B trusts A.

B. Scenario

After the description of the deployment of the coalition network, this part describes the scenario that is used to evaluate the two propositions.

Our coalition scenario is composed of three groups, each composed of three nodes. Groups A and C are high-level trusted allied and can exchange routing information, but group B, wants to keep confidential its routing data. By using simple routing policies, such as *Allow* or *Deny*, the communication between A and C would not be possible.

Our two solutions are compared with a flat OLSR network, without inter-domain communications. By doing so, we build a reference, which allows us to evaluate our solutions efficiency about the mobility and the additional cost they generate.

Our propositions showed similar performances in terms of data rate, packet loss or round-time trip on the given scenario with static nodes. We included a mobile node to stress the network and show the real performances of the solutions. The scenario we used is illustrated in Figure 8. Nodes n1 and n9 want to exchange information on a UDP flow. During the first thirty seconds, n1 moves and is still in range with its group by the node n2. At 30 seconds, n1 goes in east direction during

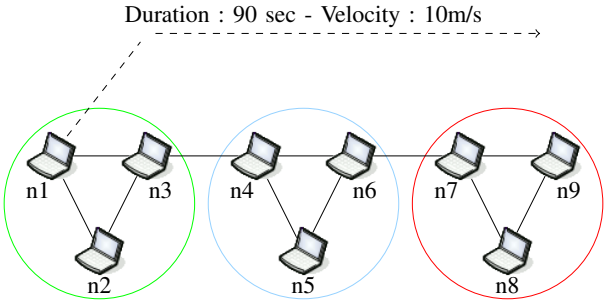


Figure 8: Scenario used for experimentation

60 seconds to reach n8 range. In this interval, n1 will undergo regular disconnections that will measure the effectiveness of the solutions during a mobility situation.

C. Implementation

This section describes the environment used to simulate the scenario and evaluate the efficiency of the proposed solutions. We used Common Open Research Emulator (CORE[2]) software to easily integrate our propositions in an ad hoc environment and use mobility scripts. Filtered announcements and tunneling are based on the same principle. Packets are intercepted by a combination of *iptables* and NFQUEUE commands. They are manipulated in a Python script with the *Scapy*[3] library. Each solution has its own script that do different tasks.

For the filtering solution, the *iptables* interception occurs on OLSR packets only. These packets are evaluated with the policy file that contains all the nodes that are not supposed to be announced on the inter-domain links. If one or several nodes are announced in the packet, it is removed and the packet is reformed. Indeed, due to several fields that indicate packet or message sizes, there is a need to recalculate each of these fields and ensure that the packet remains understandable and coherent for destination.

For the tunneling solution, the *iptables* interception occurs on all packets. Depending on the destination (OLSR broadcast, group member, inter-domain communication), the packet is ciphered with the suitable key. For the incoming ciphered packets, because we have no information on the nature of the packet, we have to try all the possible keys. However, it is more likely to receive a packet from the node group or an OLSR beacon rather than a packet from another group. Thus, we have defined a priority order on the use of the keys to have more probability to correctly decipher the packet.

V. Results

In this section, we present several measures that have been extracted using the previous scenario. We made a connectivity test including data speed, packet loss, jitter and round-time trip between two distant allied nodes. In order to measure the impact of such processing, we compare the measures for the given scenario, to a simple OLSR network without groups.

[2]http://www.nrl.navy.mil/itd/ncs/products/core
[3]http://www.secdev.org/projects/scapy/

Figures 9 and 10 respectively show the data rate and the jitter evolution during the simulation time. This experimentation is conducted ten times. All mean and standard deviation values are synthesized in Table I.

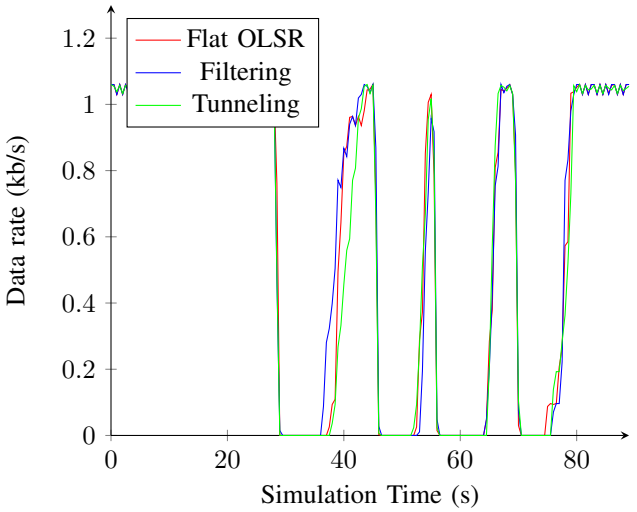


Figure 9: Data rate evolution during mobile scenario

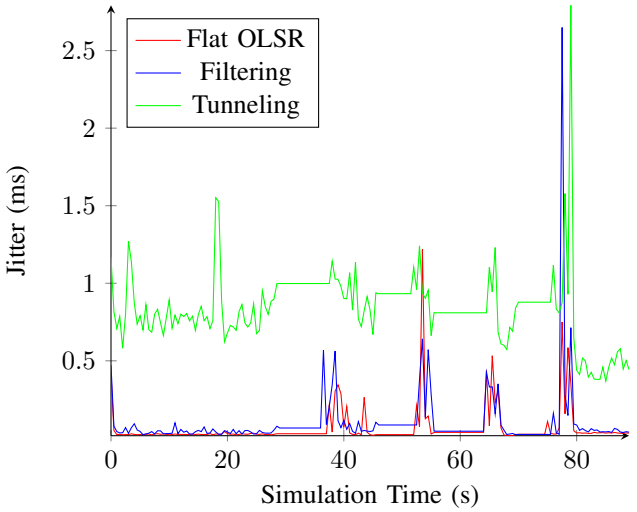


Figure 10: Jitter evolution during mobile scenario

Configuration	Flat OLSR	Filtering	Tunneling
Mean Data rate (Mb/s)	0,614	0,612	0,603
$\sigma_{Datarate}$ (Mb/s)	0,487	0,488	0,486
Mean jitter (ms)	0,071	0,101	0,831
σ_{jitter} (ms)	0,146	0,207	0,235
Mean Round-Trip time (ms)	166,660	168,127	171,923
$\sigma_{Round-TripTime}$ (ms)	3,08	4,80	6,98
Packet Loss	41,7%	41,9%	42,4%

Table I: Mean and standard deviation values for a set of ten experimentations on the mobile scenario

Iperf calculates performances in 1-second intervals. At the begin of the mobility (0-30 sec), the communication is

fully operational. n1 is moving in range of its group so the connection is not interrupted. During the second interval, n1 loses connectivity. That is the reason that received data rate is decreasing. This phenomenon repeats as cycles until n1 reaches its final position. However, we can highlight these variations whatever the network configuration is (flat, filtering or tunneling). For all the configurations, the packet loss is similar, which means, as the data rate, that the solutions does not impact performances. It is mainly due to mobility and the recovery delay of the routing protocol. The tunneling mode slightly increases the jitter and the round-trip time. This can be justified by the computation of the ciphering and deciphering processes.

VI. Related Work

Several works have been proposed to solve the issue of inter-MANET communication in tactical networks. In this section, we review some of them and how they work. In [8], the authors propose the Inter-MANET Routing protocol (InterMR). This protocol uses some functionalities of BGP such as inter-domain routing table, external and internal messages and a beaconing routine to regularly discover neighbors. A Bloom Filter [1], [2] is attached to each MANET and is in charge of the address plan synthesis. To communicate with the other domains, each groups elects one or several gateways based on their traffic. InterMR is an evolution of a previous protocol designed by the authors, namely InterDomain Routing for MANET (IDRM [3]).

Two BGP evolutions have been proposed in [7] and [9]. The first protocol is BGP Mobility eXtension (named BGP-MX). The main contribution is a central name server called DPBS (Distributed Peer Broker Service). Each node is permanently connected to this server to receive the network information (IP address, AS number...). Thus, this system can be easily downed if the DPBS is out of order.

The second evolution is BGP Manet Routing (BGP-MR) described in [9]. BGP-MR runs with OSPF-MDR, an evolution of OSPFv3 [5]. The OSPF DR (Designated Router) elected are used to easily transmit information all over the network and build the topology. All nodes are gateways but they can be in different states: passive or active. In passive mode, a node behaves as a simple router. However, it can still listen to beacons from other groups to detect new neighbors. If a node from another AS is close, the node becomes an active gateway and distributes its routing information with this neighbor. In case of AS split or merge, the gateway removes from its routing table all the information provided by the disconnected neighbor, in order to keep fresh and valid routes. ASes memberships are defined by the Bloom Filter. In our previous work and in this paper, we proposed solutions to integrate policies and improve them, as authors suggested as future work.

In [11], CIDR (Cluster-based Inter-Domain Routing) protocol uses the cluster architecture. In each AS, a Cluster Head is elected depending on the traffic it carries. Its goal is to collect all the information for the nodes of its cluster and redistribute routing information. The Bloom Filter is also used to have a representation of the nodes in each AS. CIDR handles specific cases of splitting and merging. Indeed, if an AS splits, the resulting ASes have to recreate the previous AS if they want to merge again. Other merge combinations are not possible.

VII. Conclusion & Future Work

In this article, we proposed a representation model of connectivity and policy in an inter-MANET network. Based on this model, we showed that binary policies (*Allowed* and *Denied* links) lead to block communications in a coalition network. Thus, we proposed two solutions to improve the use of routing policies in coalition networks. On the one hand, a filtering solution to prevent groups from broadcasting their internal topologies. On the other hand, a tunneling solution where each communication is ciphered from source to destination. These two propositions have been validated on a static network and show equivalent performances. We have therefore chosen to propose a scenario including mobility to test the robustness of the solutions. This experimentation showed that our two solutions are efficient and do not degrade network performances.

The next step is to include non-military entities such as non-governmental organizations or civil safety services that are groups of nodes that do not participate to the mission planning and do not have the same technology or credential

VIII. Acknowledgment

We thanks Direction Générale de l'Armement (DGA) for the financial support brought to this PhD work.

References

[1] B.H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, 1970.

[2] A. Broder and M. Mitzenmacher. Network applications of bloom filters: A survey. *Internet mathematics*, 1(4):485–509, 2004.

[3] C.-K. Chau, J. Crowcroft, K.-W. Lee, and S. H.Y. Wong. Inter-domain routing for mobile ad hoc networks. In *3rd International Workshop on Mobility in the Evolving Internet Architecture*, MobiArch '08, pages 61–66. ACM, 2008.

[4] T. Clausen and P. Jacquet. Optimized link state routing protocol (olsr), 2003. RFC 3626.

[5] R. Coltun, D. Ferguson, J. Moy, and A. Lindem. OSPF for IPv6, 2008. RFC 5340.

[6] F. Grandhomme, G. Guette, A. Ksentini, and T. Plesse. ITMAN: An inter tactical mobile ad hoc network routing protocol. In *MILCOM2016*, 2016.

[7] M. Kaddoura, B. Trent, R. Ramanujan, and G. Hadynski. BGP-MX: Border gateway protocol with mobility extensions. In *Military Communications Conference (MILCOM)*, pages 687–692. IEEE, 2011.

[8] S.-H. Lee, S. H. Wong, C.-K. Chau, K.-W. Lee, J. Crowcroft, and M. Gerla. InterMR: Inter-MANET routing in heterogeneous networks. In *International Conference on Mobile Ad-Hoc and Sensor Systems*, pages 372–381. IEEE, 2010.

[9] I. Okundaye, T. Kunz, and S. Gulder. Inter-domain routing for tactical mobile ad-hoc networks. In *80th Vehicular Technology Conference (VTC Fall)*, pages 1–6. IEEE, 2014.

[10] Y. Rekhter and T. Li. A border gateway protocol 4 (BGP-4), 1995. RFC 1771.

[11] B. Zhou, Z. Cao, and M. Gerla. Cluster-based inter-domain routing (CIDR) protocol for MANETs. In *Sixth International Conference on Wireless On-Demand Network Systems and Services*, pages 19–26. IEEE, 2009.