ITMAN: An Inter Tactical Mobile Ad Hoc Network Routing Protocol

Florian Grandhomme, Gilles Guette
IRISA / Université de Rennes 1, France
Firstname.Lastname@irisa.fr

Adlen Ksentini
Communication Systems Dept. / 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, constitute ad hoc networks and specifically, Mobile Ad hoc NETworks (MANET). The battlefield where these equipment are deployed includes a majority of coalition communication. Each group on the battleground may communicate with other members of the coalition and establish inter-MANETs links. Operational communications tend to provide tactical ad hoc networks some capacities. There is a better broadband radio in UHF band (ex: NATO - 225-400 MHz) and some heterogeneous services such as voice or video (ex: capture from a drone) are provided. Several Network-layer protocols have been proposed in order to handle inter-domain routing for tactical MANETs. In this paper, we present a coalition context and describe the functional hypothesis we used. Then, we propose a protocol that would fit such a network and conduct experimentation that tend to show that our proposition is quite efficient.

I. Introduction

New generation radio equipment, used by soldiers and vehicles on the battlefield, constitute ad hoc networks, namely, Mobile Ad hoc NETworks (MANET).

The increasing needs in data rate in the lowest tactical levels implies an important number of nodes and a high density of tactical radio equipment. These equipment have a high mobility potential.

Usually, the battlefield is composed of several nations, grouped under a coalition against the same enemies. Tactical ad hoc military networks, forming MANETs, have to connect and operate with tactical radio networks but also with other military networks (*e.g.*: satellite communications with metropolis). Military operation evolution considerably increased coalition needs and interoperability for the tactical networks. Information can be exchanged between heterogeneous networks fluidly in order to have a better information and gain a tactical advantage.

In order to have an efficient coalition, nations have to communicate. Therefore, MANETs would be organized differently due to the independence of each nation constituting the coalition. Depending on the trust in other nations, some MANETs would like to control the level of data they exchange. Thus, some sensitive data would be sent to defined groups rather than others with less confidence. Accordingly, we have a coalition organized with different groups which want to communicate data, while maintaining control over the sensitive data and their destination; which could be done through routing policies. In this paper, we deal with the exchange of routing information (not application data information), and the construction of route between nodes.

Such a situation has been encountered in the past to build the Internet where network operators had to collaborate. These groups (networks of operators) have to exchange data but want to keep their network organization confidential and keep control of the shared data with other operators. Nowadays, those groups are called Autonomous Systems (AS) [7]. BGP (Border Gateway Protocol) interconnects the AS to make the Internet possible, regarding the requirements on routing policy. BGP allows each AS to select trusted ASes with which they want to communicate and the routing information to share. Nowadays, BGP is mainly used on the Internet and is known to fit inter-domain requirements for the wired networks. However, due to the characteristics of BGP wired networks such as manual configuration, no mobility or long route recovery time, BGP is not adaptable to ad hoc networks for inter-MANET communications. In this paper, after a thorough analysis of MANET constraints and interactions between network and security layers (which is mandatory), we propose a new protocol called ITMAN that would provide efficient inter-MANET routing in tactical MANETs.

This paper is organized as follows. First in Section II, we present our operational environment and the functional hypothesis we used to design our protocol. Then, we describe in Section III the algorithms that handle situations of an operational battleground. The efficiency of our protocol is evaluated in Section V. Finally, we focus on the new elements brought by our protocol and compare them with existing inter-MANET protocols.

II. Operational considerations

As described before, tactical ad hoc networks should be able to collaborate with other MANETs in a coalition, whereby each MANET is under an independent authority. Before detailing the proposed solution, we begin by introducing some definitions and assumptions.

A. Group Definition

We define a *group* as a set of nodes able to communicate together. This leads to two types of constraints:

i) communications should depend on the used network technologies.
ii) communications should depend on organisational constraints such as ciphered communication.

1) Network Capabilities: As the members of a group has to communicate with each others, this implies that network topologies are compatible; meaning that layer 3 protocols (Network Layer) are compatible, for example all the nodes use IPv4 (resp. IPv6). Furthermore, layer 2 protocols (Data-Link Layer) should also be compatible. Therefore, all the nodes should use the same technology (UHF/VHF, CSMA/Wifi, TDMA, etc.). This constraint of homogeneity is also present for the used routing protocol. Although we talk here about homogeneity, this does not mean that only one technology is used by a node. Indeed, a node can have multiple communication devices and support multiple technologies. Nevertheless, a group is homogeneous and needs to keep the ad hoc philosophy that avoids single point of failure. That is, if a node supports multiple technologies, this means that all the nodes of the group should support these technologies. These constraints describe a group in term of communication capabilities, which is not sufficient. We also consider the fact that if a group is under an authority, the latter should keep control over its communication. Indeed, as we are in ad hoc mode, if an external node (node not in the group) with the same layer 2, layer 3 and routing capabilities enters in the communication range, it is able to communicate with the group (as in ad hoc networks, nodes can communicate regardless of their IP prefixes [6]). This advocates for ciphered communication in order to keep control over the exchanged data.

2) Organisationnal Capabilities: We assume that tactical nodes have to cipher their communications. This *defacto* creates a group, as any node without the cryptographic material (*i.e.* the credentials) cannot understand the communication. Given that security material management is out of scope of this paper, we just made some assumptions that seem realistic in our context. During the mission planning of a coalition, each node is assigned, (at least) a certified public/private key pair with the associated certificate and the (trusted) certificates of authorities used in the coalition. Inside a group, each node can send ciphered and/or signed messages.

With these assumptions, technologies used in the group are homogeneous. Thus, nodes can communicate even if different technologies are used as each node can act as a gateway. Cryptography isolates communication inside the group.

To satisfy all the requirements of an inter-MANET routing protocol (*i.e.* requirements described in [3]), we will consider two aspects. First, the routing aspects that cover the freshness and update of the routing tables during the networks lifetime. Second, the security and routing policy aspects to be handled. Indeed, groups are under the same coalition, but they probably do not want to share all the routing information. Some communications are more sensitive than others, and hence they should not be routed through some MANETs constituting the coalition. It is necessary to respect those policies. For example, a policy routing of a MANET A can say that this MANET can send packets to the MANET B, unless packets must go through MANET C to reach MANET B.

III. The ITMAN protocol

In this section, we present the main algorithms composing the ITMAN protocol. The idea of this protocol is to take advantage of the security policy (*i.e.* cryptographic material and encryption) to define a group. Groups are able to communicate with each other by creating links, which may be compared to tunnels. These tunnels are built according to the local policy and are encrypted with a shared key. Shared key generation is discussed later.

A. Definitions and notations

As mentionned in section II, a node owns pre-defined elements. The latter are needed to communicate inside its own group or with other groups, or to merge with another group. Table I describes the elements owned by a node N at the beginning of the mission.

OGN	The node's Original Group Number
$K_{Priv}(N)/K_{Pub}(N)$	Public/Private key pair
$Cert(N)_{CA}$	A certificate signed by the authority *CA* for the node N_i covering its public key and its OGN
$Cert(CA_i)$	Trusted Certificate of the CA used in the coalition
$K(OGN)$	Key to communicate inside the OGN group
$PolicyList$	Policies to apply with other groups

Table I: Elements owned by a node N

To build communications between nodes or between groups, we define three communication channels:

- Intra-group channel: Channel encrypted by a Key $K(OGN)$ inside a given group
- Inter-group channel: Channel encrypted by a shared Key between two different groups
- General channel: Channel used for Beaconing, beacons are clear text

B. Mission planning

Before starting a mission, some steps are needed in order to enable communications inside a group. First, elements described in Table I have to be loaded in each node. The $K(OGN)$ key will be used to cipher communication (in our case at least routing information) inside the group OGN. For a seek of simplicity only one key is used. Solutions like multiple keys, key rollover and so on could also be used to add more flexibility in the key management. Being encrypted, the routing information provided by the nodes of the group cannot be understood by an external node.

During the mission planning, the $PolicyList$ is also decided. We define three policies between groups:

- Deny: no communication with the other group
- Link: a communication is possible with a unique link between the two groups (*i.e.* only one node of each group acts as a gateway)
- Merge: every node of the group 1 will communicate (directly or not) with all the nodes of the group 2, whatever the number of links is

For a given group, the $PolicyList$ contains all the associations (policy, OGN) for all the OGN involved in the mission.

C. Beaconing routine

During the mission, nodes communicate inside their group with $K(OGN)$. However, an external node in the communication range could not understand the packets. Thus, we use a beaconing system with non-encrypted packets to discover neighbors.

Algorithm 1 Beaconing routine

```
Periodically broadcast (Cert(A)_CA,Timestamp)_Sig_K_Priv(A)
while true do
    if Receive (Cert(B)_CA,Timestamp)_Sig_K_Priv(B) then
        if Verify(Sig_K_Priv(B)) & Verify(Timestamp) & Verify(Cert(A)_CA) then
            Extract OGN from Cert(B)_CA
            if It is a new OGN then
                Check(PolicyList)
            end if
        end if
    end if
end while
```

Each node periodically broadcasts a beacon to announce its presence. This packet contains elements to authenticate the node and a time-stamp to mitigate replay attacks. When receiving this kind of packet, a node verifies the signature, the time-stamp and the certificate. If the OGN of the sender is not a current active group for the receiver, the latter checks the $PolicyList$ and acts accordingly.

In case of a Deny policy, no more exchanges are made. Indeed, even if two groups are close to each other, they are kept separated since they are using different $K(OGN)$ keys. In the following subsections, we explain how we create communication to respect a Link or Merge policy.

D. Link Policy Routine

When A receives a beacon from node B of another group with an associated Link Policy, A and B have to create a ciphered channel. As the $PolicyList$ is created during the mission planning, we assume that the $PolicyLists$ are consistent (if A trusts B, B trusts A). Algorithm 2 illustrates the creation of a link between A and B (from the point of view of A). We assume that both nodes are in communication range and have received a beacon from each other.

After receiving a beacon, if the policy is to create a link, both nodes negotiate a shared key. This key could be loaded during the mission planning or be the result of an authenticated Diffie-Hellman exchange for example. Then, both nodes use this secure channel to tell with which groups they are able to route packets. Then, each node can decide to follow up the process and exchange routing information or to close the communication. The following example (Fig 1) illustrates why the communication could be closed.

Algorithm 2 Link Policy Routine

```
if Check(PolicyList) = Link then
    Negotiate the Shared Key K_AB
    Send reachable OGN to group B through the K_AB encrypted channel
    Receive reachable OGN from B through K_AB encrypted channel
    if Reachable OGN are consistent with the PolicyList then
        When needed encrypt routing data with K_AB
    end if
end if
```

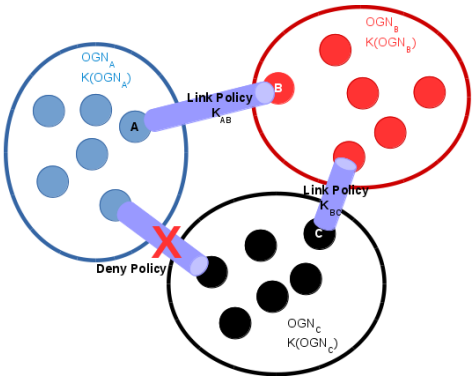
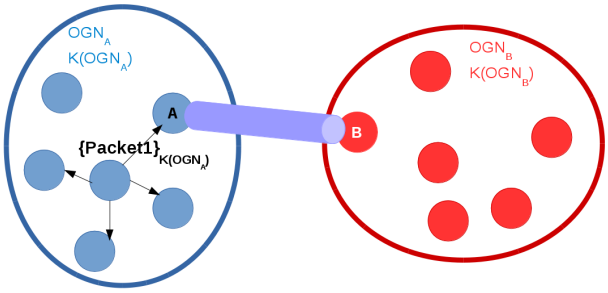


Figure 1: "Transitivity" of trust

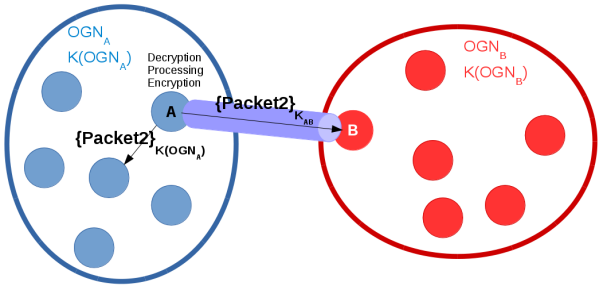
Let A from OGN_A, B from OGN_B and C from OGN_C be three nodes from three different groups. We assume the following policies exist: (i) Link between OGN_A and OGN_B, (ii) Link between OGN_B and OGN_C and (iii) Deny between OGN_A and OGN_C. If the protocol processes correctly, nothing prevents group OGN_B from revealing routing information about group OGN_A to group OGN_C and vice-versa; that is why A and B have to exchange reachable OGN from their group. If the node B announced to A that the group OGN_C is reachable, then A may decide to prefer the Deny policy even for the group OGN_B in order to protect its routing information.

After the tunnel creation, ad hoc routing protocol runs as usual on each "gateway". Then, routing data exchange proceeds as follow (Figure 2):

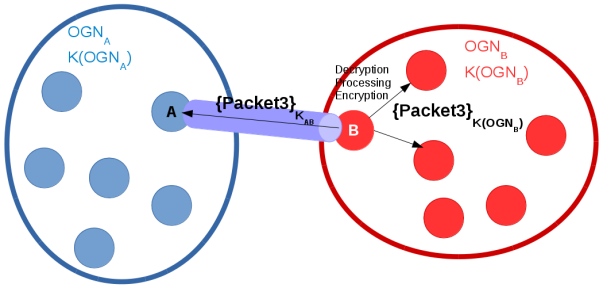
- A node in group OGN_A sends routing data ciphered with $K(OGN_A)$.
- The packet arrives to the "gateway" of the group OGN_A. The packet is decrypted and if forwarding is needed, the packet is sent two times once encrypted with K_{AB} and once encrypted with $K(OGN_A)$.



(a) Routing Data Packet generated in OGN_A



(b) Routing Data Packet processed and forwarded



(c) Routing Data Packet processed in OGN_B

Figure 2: Routing Data exchange with a Link Policy

- The packet arrives to the "gateway" of the group OGN_B. The packet is encrypted with K_{AB} , decrypted, processed and then re-encrypted with $K(OGN_B)$.
- Inside the group OGN_B, the packet is encrypted and decrypted with $K(OGN_B)$.

E. Merge policy Routine

When a node A receives a beacon from a node B of another group with an associated Merge Policy, the two nodes have to create common cryptographic material (a shared key). Unlike in the Link policy, this time the shared key is broadcasted to all the nodes of the group OGN_A and to all the nodes of the group OGN_B. Algorithm 3 illustrates the different steps between node A and node B for a merge between two groups.

The idea is that once the shared key is created and broadcasted, all the nodes of OGN_A and OGN_B groups can directly exchanged routing data by encrypted it with K_{AB}.

IV. Policy considerations

A. Key Management and Validity

As we have seen above, notion of group is closely linked to cryptographic material. In the protocol description, we assume

Algorithm 3 Merge policy routine

1: **if** Check($PolicyList$) = Merge **then**
2: Negotiate the Shared Key K_{AB}
3: Send reachable OGN to group B through the K_{AB} encrypted channel
4: Receive reachable OGN from B through K_{AB} encrypted channel
5: **if** Reachable OGN are consistent with the $PolicyList$ **then**
6: Broadcast K_{AB} in the group channel (ciphered with $K(OGN)$
7: **end if**
8: **end if**

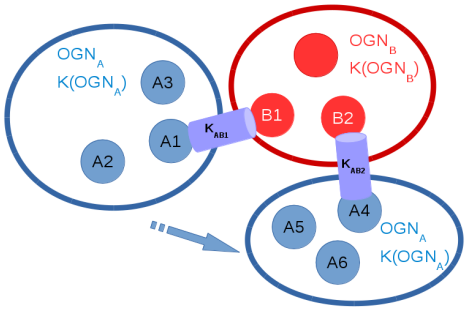


Figure 3: Link policy on a splitted group

that a node owns the key of its own group and will negotiate a shared key to communicate with other group according to its communication policy. As we are in a coalition environment with a mission planning, to minimize communication and computation overhead, we also can assume that during the mission planning, the different authorities have already negotiated shared keys according to their communication policies. Moreover, these shared keys are loaded into the nodes before the mission starts. Then, we reduce the number of key negotiation between members of different groups that want to exchange routing data.

Concerning the validity of the shared keys, as they will be used to encrypt routing data, it is important to delete a shared key when it is not needed anymore. For example, when two groups are not connected anymore (no beacon received), a timer is launched. Once the timer is out, the key is deleted and will be renegotiated if needed. Another possibility for the key deletion is a direct order from the hierarchy, for example, if a policy between two groups changes and the shared key does not fit anymore this new policy.

B. Policy and mobility issues

Another particular case that can occur due to mobility is illustrated Figure 3.

Two groups OGN_A and OGN_B are sharing routing data by using a Link policy. The group OGN_A splits into two parts. One part of the group OGN_A moves around OGN_B and finally reconnects with it. Considering the situation from OGN_B point of view, it shares a Link policy with OGN_A

that stipulates only one link between the two groups. Now, the second part of OGN_A should not be rejected, as it is physically two distinct groups. Therefore, we propose the following solution: once the node has been authenticated during the beaconing routine, the node $B2$ sends a ping to $A4$. The following cases can arise:

1) There is no entry in its routing table $\Rightarrow$ this corresponds to a split, therefore a second link has to be created.
2) There is no response to the ping $\Rightarrow$ this is a split but the old route is not yet deleted by the routing protocol, therefore a second link has to be created.
3) There is a response $\Rightarrow$ $A4$ is already reachable, this is not a split, no link has to be created.

V. Latency evaluation

To evaluate the ITMAN protocol, we measured the latency caused by encryption. The test consists in measuring the delay between the reception of the first OLSR Hello packet and the creation of a new route in the routing table.

The test environment is composed by two laptops on top of Intel Core i3-400 CPU with two 2.4 GHz cores, 4 Gigabytes of memory and running a Debian 8 distribution (kernel 3.16). During the experiment, we have to intercept OLSR packets to encrypt payload. Packet sniffing and interception is done with *iptables* and NFQUEUE option. Packet manipulation and encryption is done with Python scripts and *Scapy*[1]. We decide to modify packets on the fly rather than modify the OLSR code. This allows to test different implementations of OLSR. To evaluate the latency caused by encryption, we run three tests:

- First test: packets are just intercepted by NFQUEUE and forwarded as is,
- Second test: packets are intercepted by NFQUEUE, checksum and header/packet length are re-computed,
- Third test: packets are intercepted by NFQUEUE, OLSR payload is encrypted, checksum and header/packet length are re-computed.

As encryption modifies the packet length, we need to re-compute checksum and packet length, that is why we have done the second test to estimate latency generated by this computation (without encryption). The test runs as follows: the first laptop is configured with OLSR timer following the recommendation of the RFC 2636 (Hello 2s, TC 5s) , while a python script intercepts the OLSR packets. Depending on the test number, it forwards, re-computes or encrypts packets with AES-128. On the second laptop, OLSR packets are also intercepted with NFQUEUE (and decrypted if needed). We check time when the first Hello is received and when the route is added to the routing table.

These tests have been conducted a thousand of times each. Figure 4 shows the distribution of this delay for the two communication modes (encrypted and non-encrypted).

Table II synthesizes statistic values to easily compare the two experimentation. It shows that our proof-of-concept based on *iptables* rules and python scripts does not add a significant delay even if Python is known to be slow. The encryption of the OLSR payload add less than 300ms in the neighbor discovery process. We can also note that with a complete implementation of our protocol, time due to checksum computation and NFQUEUE interception can be reduced. This gain can be increased using language more suited than Python. Another delay we evaluate is that if the shared keys are not loaded during the mission planning, they have to be computed in our beaconing process. We measured the time needed to the creation of a shared key during the first encounter of two nodes. On a thousand of shared key creations, the mean delay is about 0.5 second which is perfectly acceptable.

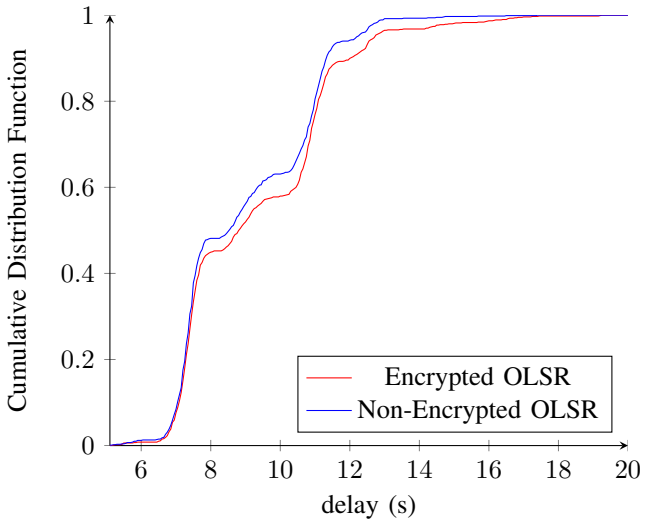


Figure 4: Route adding time comparison

	Simple Interception	N-E payload	E payload
Mean value (sec)	9.01	9.08	9.35
Standard dev. (sec)	2.07	2.53	2.35

Table II: Route adding time (non-encrypted (N-E) and encrypted (E) OLSR)

VI. Related Work

Several works have been proposed to solve the issue of inter-MANET communication in tactical networks.

In [9], the authors propose the Inter-MANET Routing protocol (InterMR). This protocol proposes features such as BGP which are an inter-domain routing table, external and internal messages and a beaconing routine to know the current neighborhood. The address plan of a MANET is based on a Bloom Filter [1], [2], which synthesizes all members of the group. Inter-domain communication is made with gateways election process, which is based on their traffic. InterMR is an evolution of a previous protocol designed by the authors, namely InterDomain Routing for MANET (IDRM [4]). Compare to this solution, our proposition does not need a Name Server to know which nodes belong to the AS. Indeed, a group is defined by a cryptographic group

[1]http://www.secdev.org/projects/scapy/

key that guarantees intra-group communications only. The messages cannot be processed from the point of view of an external member of this group. Our experiments showed that ITMAN does not involve significant overhead and can be an alternative to the Bloom Filter and gateway election systems.

Two evolution of BGP have been proposed in [8] and [10]. The first proposition is named BGP-MX for BGP Mobility eXtension, where the main contribution is the DPBS (Distributed Peer Broker Service), a central name server. Nodes are permanently connected to this server and get their network information (IP address, AS number...) from it. Thus, this system is not fully distributed and can be easily weakened if the DPBS is out of order. This solution brings a central element that needs a permanent connection. In our proposition, configuration and route discovering are fully distributed in the network and can be done by each node in the MANET. Furthermore, routing information are calculated by the OLSR protocol and not provided by an external server.

The second evolution is BGP-MR (BGP Manet Routing) described in [10]. BGP-MR runs in collaboration with OSPF-MDR, an evolution of OSPFv3 [5]. The OSPF DR (Designated Router) elected are used to easily transmit information all over the network. All nodes act as gateways. Two states exist: passive and active. In passive mode, a node behaves as a simple router. However, it does not prevent it to listen to beacons in order to detect new neighbors. If a neighbor from a different AS is close, the node turns on an active gateway and distributes its routing information with this neighbor. In case of AS split or merge, BGP-MR removes from its routing table all the entries provided by the missing neighbor, in order to keep fresh and valid routes. Membership in an AS is memorized thanks to a Bloom Filter. In our protocol, we do not use a Bloom Filter as explained above. Furthermore, we do not use specific nodes in the network such as Designated Router to route the packets. Finally, we proposed a solution to handle policy issues, as authors suggested as future work.

In [11], CIDR (Cluster-based Inter-Domain Routing) protocol uses a cluster approach. In the AS, a node is elected as a Cluster Head based on its significance from the point of view of traffic. Its role is to centralize the information and redistribute routing information. AS membership is known thanks to a Bloom Filter. CIDR supports some situations of splitting and merging. Indeed, resulting AS of a mobility scenario must be identical of a previous one, particularly in merge processes. With our proposition, merging conditions are relaxed. Mobility is free and communications can be created wherever the nodes are. Finally, there is no central point of failure. Nodes are able to calculate routes with the routing policy list they embed during the operation.

VII. Conclusion and Future work

In this article, we proposed a new inter-MANET routing protocol for tactical networks. We first defined our operational environment, particularly in terms of used layer 2 and 3 technologies, group definition and organisational capabilities. Then, we proposed algorithms based on cryptography to both ensure inter-MANET communication and security. To evaluate the performance of these new algorithms, we used an experimental platform to measure the delay added by encryption. The results of experiments showed that cryptography does not add significant latency. Thus, ITMAN brings some new solutions to inter-MANET communication in tactical networks. Communications are isolated inside a group and cannot be understood if intercepted. Furthermore, the beaconing routine provides a quick reaction to neighbor discovery and route creation. Finally, we discussed about policy conflicts, cryptographic material generation and validity in operational context. As future work, we plan to deploy the ITMAN in a full real context, with several groups and policies in order to evaluate application level performance. Second, we plan to study policy conflict in a huge coalition. Finally, we will to have routing policy that can include non-military entities such as non-governmental organizations (*i.e.* group of nodes that do not participate to the mission planning and that do not have 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] J. L. Burbank, P. F. Chimento, B. K. Haberman, and W. Kasch. Key challenges of military tactical networking and the elusive promise of MANET technology. *IEEE Communications Magazine*, 44(11):39–45, 2006.

[4] 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.

[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. Comparing Inter-Domain Routing Protocol Assessment Tools for MANET. In *International Conference on Communications (ICC)*. IEEE, 2016.

[7] J. Hawkinson and T. Bates. Guidelines for creation, selection, and registration of an Autonomous System (AS), 1996. RFC 1930.

[8] 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.

[9] 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.

[10] 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.

[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.