An Architecture for Secure Interoperability between Coalition Tactical MANETs

Mazda Salmanian, J. David Brown, Susan Watson, Ronggong Song, Helen Tang, Darcy Simmelink
Defence R&D Canada - Ottawa, Ontario, Canada [first.last]@drdc-rddc.gc.ca

***Abstract*—International military forces are increasingly engaged in coalition-based operations with an expectation that future coalition forces will be tightly interoperable even down to the tactical level. At the same time, there is an emerging trend towards increasing connectivity at the tactical edge, with mobile ad hoc networking (MANET) seen as a key enabling technology for this improved connectivity. This paper explores the convergence of these two trends—a desire for secure coalition interoperability and its potential co-existence with a MANET-based tactical communication platform. We present an architecture consisting of three elements that enable allied MANETs to share information securely: a key management strategy, gateway discovery and security association and network address translation. These concepts are well researched individually; in this paper we combine them in the context of a coalition tactical operation. We present several tactical scenarios in which our architecture enables a MANET to discover nearby allied MANETs, to identify and authenticate gateways to relay its information and to connect specialized nodes of allied MANETs and establish communities of interest. Our solutions could serve as models for the future development of secure interoperability policies, service level agreements and standards, e.g., for future NATO standardization agreements (STANAGs) or Combined Communications-Electronics Board Allied Communication Publications (CCEB ACPs).**

***Keywords*—**Mobile ad hoc networks (MANET), Key Management, Network Address Translation, Tactical Edge, Network Address Translation

I. INTRODUCTION

Increasingly, military forces are seen to be deployed in allied coalition operations where there is a greater need for interoperability—not just between strategic networks but all the way to the tactical edge, including communications and networking between deployed tactical teams. Secure exchange of command and control (C2) messages as well as up-to-date situational awareness (SA) data, including troop location and movement, are critical to the success of a mission and the safety of teams deployed at the tactical edge.

Mobile ad hoc networks (MANETs) are believed to be a key technology that will facilitate dynamic and beyond line-of-sight networking in contested environments where no fixed infrastructure exists. In a MANET, every node can act as both a host and a router, forwarding data to allow for multi-hop connectivity and range extension. In this paper, we examine how national tactical MANETs could securely exchange information between one another as part of an international coalition. This is not a simple task, since MANETs have no central authority, fixed topology or guaranteed connectivity; furthermore, the imperative to protect national network boundaries and the security of national information hinders the free exchange of information between national MANETs.

We formulate the problem of secure interoperability between coalition tactical networks in the context of two neighboring MANETs from separate allied nations. We assume that a single national MANET subnet consists of a relatively small number of nodes, e.g., between 10 to 30 nodes. By limiting the size of the MANET subnets, one avoids well-known issues of scalability that plague mobile ad hoc networks; this is consistent with military deployment scenarios, where small (national) MANET subnets could provide local connectivity to a unit, e.g., section/platoon.

In our formulation, a MANET from nation A (MANET-A) and a MANET from nation B (MANET-B) require secure internetworking to exchange data (this may consist of SA data or any other data agreed-upon by policy). We present a key management scheme that enables neighbor discovery, authentication and the formation of gateways in each MANET. Gateways are those MANET nodes that are assigned the function of relaying inter-MANET messages. Our proposal describes a method for gateway assignment and how a gateway can ensure the security of information in transit between MANETs A and B. Throughout the paper, we assume that all MANET nodes have the potential to function as gateways and are equipped with an interoperable radio[1], such as the NATO Narrowband Waveform (NBWF) [1].

After two gateways (from MANET-A and MANET-B) have connected and authenticated, they still must contend with different address spaces to deliver traffic. We discuss how the gateways perform network address translation (NAT) to enable two allied MANETs of different Internet protocol (IP) address space and different routing protocols (assumed sovereign in each nation) to share information securely.

Once connectivity and addressing is established, we describe how a node (or nodes) in MANET-A can establish a security association through the gateways to another group of nodes in MANET-B, thus forming a community of interest (CoI). In our formulation, a CoI is an encrypted enclave amongst nodes in a coalition MANET with specialized responsibilities and security requirements, e.g., an intelligence (INT) team including nodes of both national MANETs could form a CoI, where certain information is shared only with members of the INT team.

[1] Without loss of generality or purpose, one could apply our proposal to a scenario where only a subset of MANET nodes are capable of being gateways; i.e., certain nodes would be equipped with gateway functionality and with two radios: one for national connectivity and one with common media access control (MAC) and physical (PHY) layers and shared spectrum for gateway "coalition" connectivity.

With our proposed architecture, we reduce the problem of secure interoperability to smaller, more manageable concepts and offer practical solutions to them. The concepts — key management, gateway formation and network address translation — have been researched for secure strategic networks [2-4]; they are also well researched individually for MANETs [5, 6], [7, 8], [9, 10]. The problems are also formed into concepts in the NATO Tactical Communications (TACOMS) [11] models. Here, we propose solutions and study them as an aggregate under one context for secure interoperability in a tactical environment, while preserving the national autonomy and sovereignty of a tactical military group.

The proposal in this paper is based in part on work by the same authors appearing in an internal government report [12]. In particular, large portions of the discussion regarding key management and communities of interest (Sections II, III and V) are modified excerpts from the internal report [12]. The work in [12] discusses a key management strategy for national tactical MANETs, whereas this paper extends the ideas to a coalition space and aggregates our proposal with solutions to gateway assignment, security associations and network address translation.

The rest of the paper is organized as follows. Section II provides definitions, notation and an overview of the types of cryptographic keys we propose to employ in our key management strategy. In Section III, we present our key management strategy, focusing on key creation, distribution and revocation. Gateway assignment and inter-gateway security association are presented in Section IV. We present our network address translation scheme in Section V with scenarios which include delivery of broadcast SA messages and of unicast or multicast CoI traffic. Finally, Section VI provides a brief conclusion.

II. Definitions, assumptions and notation

In this section, we establish definitions, notation and assumptions. These definitions are also used in [12], a proposal for a national network. We adapt them here to an international context.

We assume throughout the discussion that national MANET subnets (roughly platoon-sized) consist of a collection of dismounted nodes and vehicle-mounted nodes (including land and air vehicles such as unmanned aerial vehicles — UAV). Our proposed strategy relies on coordinated (automated) actions by a so-called "commander node" to perform functions such as gateway assignment and key generation. It is sensible that the commander node start out as the platoon commander, since this position is generally more fortified and less vulnerable than other nodes. Should the platoon commander node be compromised or destroyed, the second-in-command (2IC) is a logical choice to replace the commander node. Should both the platoon commander and 2IC be incapacitated, a dynamic selection process would need to take place (for algorithms to perform such selection see [13]).

Our key management strategy makes use of a trusted certificate authority (CA) and four types of encryption keys defined below; their usage is described in greater detail in Section III.

- **Certificate Authority**: A public key infrastructure (PKI) certificate authority, e.g., NATO PKI Authority, signs public key certificates for all users in an operational deployment. The CA must be trusted by the owners of the certificates and all others relying upon the certificates. The certificate authority is high-assurance and serves as the ultimate root of trust in the deployed operation.
- **Public/Private Key pairs** (asymmetric keys): These are generated and issued by the CA to all nodes in an operational deployment; unique public/private key pairs support device authentication, message non-repudiation and establishment of group and session keys (presented below). These asymmetric keys (including a public key certificate signed by the CA) will be pre-loaded into each provisioned device prior to the mission and will remain constant for the duration of the mission. Nodes will also be pre-loaded with an updated certificate revocation list (CRL). As storage capability permits, public keys of other relevant nodes can be pre-loaded during provisioning, e.g., the public keys for all members of a platoon from the same nation could be pre-loaded prior to a mission. It is assumed that stationary nodes at a forward operating base (FOB), or so called "HQ nodes", will have access to the public key certificates of all relevant national mission members. If necessary, a node can always transmit its own public key certificate as a first step in establishing communication in cases where this is not provisioned ahead of time.
- **Group Keys**: Most multicast and broadcast network communication in our proposed scheme take place using symmetric group keys. We consider two major group keys: subnet group keys and CoI group keys. The subnet group keys will be established dynamically in each national subnet at the beginning of a mission and refreshed/updated periodically during the mission (where, recall that a national MANET subnet is expected to be between 10 and 30 nodes between the sizes of a section or platoon, respectively). Note that the group key refresh rate will be much faster than the mission key cycling rate (discussed below). The CoI group keys will be established during the creation of a CoI (as explained in Section V) and will be refreshed/updated periodically depending on CoI security policy.
- **Mission Key:** The mission key is a symmetric key shared to all nodes on a common mission to support initial communication prior to establishing group keys. The mission key also supports other functions such as the identification of coalition forces. Upon deployment, a node will be pre-loaded with a set of mission keys that will be cycled at pre-defined times (where it is expected that the cycle-time will be very slow — on the order of days). The keys are renewed at the FOB before re-deployment. Because of the slow cycle-time, the mission key will only be used to encrypt low-value data, e.g., a generic identification of the platoon and/or nation.
- **Session Keys:** These will be used for unicast

TABLE I
NOTATION

Notation	Description
m	a message
$\{m\}_k$	a message m encrypted with symmetric key k
$h(m)$	a hash function h operating on a message m
H	a packet header
Pub_k_n	user n's public key
Pri_k_n	user n's private key
Mk	the current mission key
Gk_j	*the j^{th} group key (of a section or platoon)*
Gk_{CoI}	*The CoI group key*
Sk	*a unique session key*
$Cdr\text{-}A$	*commander of MANET-A, (nation-A)*
Cdr_AID	*public identification of commander A*
GW_BID	*identification of gateway B*
$IP_{src}(node)$	*the source IP address of a node*
$IP_{dest}(node)$	*the destination IP address of a node*

communication between two nodes; they are generated at the beginning of a communication session and expire at the end of the session.

We adopt the notation detailed in Table I to describe the encryption of data in our proposal. An example of notation usage is as follows: a packet containing a header, *H*, encrypted with mission key, *Mk*, followed by data and a nonce encrypted with group key "number 5" and signed with user 1's private key would be written as:

$\{\{H\}_{Mk}, \{Data, Nonce, \{h(Data, Nonce)\}_{Pri\_k\_1}\}_{Gk\_5}\}$.

Note that the details of message formats provided in this paper are primarily for pedagogical purposes to allow for ease of describing the algorithms for data sharing.

With these definitions established, in the following sections we describe the key management strategy and the use of the four types of keys in detail.

III. KEY MANAGEMENT STRATEGY

In this section we present our key management strategy, focusing on key creation, distribution and revocation, leveraging and adapting the concepts in [12]. We assume a typical MANET deployment will have a section or platoon of nodes (i.e., a MANET subnet) leaving a FOB as a group and powering up and authenticating to their devices. Standard user authentication mechanisms, e.g., username/password and/or multi-factor authentication, could be applied in this instance, depending upon the desired level of user-to-device authentication assurance. As discussed in Section II, all devices will be pre-loaded with unique public/private key pairs, public key certificates and a shared symmetric mission key. The default behavior of any node upon power-up is to utilize the mission key for routing, signaling and communications until a subnet group key is established, as discussed below.

This section of the report primarily describes the operation of the key management strategy within a national MANET subnet. Once these primitives are established, Sections IV, V and VI discuss how they are used in an international setting.

A. Group Key Creation and Distribution

The commander node will be capable of generating subnet group keys independently. Upon creating a subnet group key, the commander node will unicast a copy of this key to each member of the subnet. For example, to send a group key, *Gk*, to node *n*, the commander could send a message of the form:

$\{\{H\}_{MK}, \{Gk\}_{Pub\_k\_n}, \{CdrID, nonce, \{h(CdrID, Gk, nonce)\}_{Pri\_k\_Cdr}\}_{Gk}\}$.

Essentially, the commander sends a unicast copy of the group key to each subnet member node, encrypted with the public key for that subnet member. Upon receipt of the subnet group key, a subnet member node will respond to the commander node with an appropriate acknowledgement. After receiving "group key received acknowledgments" from all members of the subnet, a commander node will issue a command to all nodes in the subnet to begin using the subnet group key for all communications, including routing and signaling. At this point, subnet nodes will communicate data with each other and the commander using the subnet group key; the mission key is used to encrypt only the header. Packets sent using the subnet group key will be structured as $\{\{H\}_{Mk}, \{Data\}_{Gk}\}$.

B. Group Key Update

After subnet group keys have been established, it is desirable to refresh or update the keys periodically. The mechanism to refresh the group keys is similar to the mechanism of initial key establishment and distribution. In the standard case where the subnet group key is to be refreshed, the commander node simply unicasts copies of the subnet group key to each subnet member node as described in III-A. In the following discussion, we describe the process of subnet group key update in non-standard cases, where nodes are out of communication range when the subnet group key is refreshed.

1) Nomadic re-join

The first non-standard case we consider is of a nomadic node that is temporarily out of range during a subnet group key update that must re-join the network when it comes back in range. Upon coming back in range of the subnet, the nomadic node will observe header information (encrypted with the mission key) that allows the node to determine that this is its subnet. The node, however, does not have the current subnet group key and cannot decrypt the payload data. The node thus sends a unicast "re-join request" to the commander node, where the commander node will verify that the nomadic node is valid and not compromised (i.e., not on the CRL). The commander node will then unicast a new subnet group key to the nomadic node encrypted with the node's public key.

In the case where the nomadic node comes in range of a MANET from a different subnet (or an allied MANET from a different nation), the nomadic node will be treated as a gateway, as will be explained in Sections IV and V.

2) Subnet merge

If a MANET subnet becomes geographically split (i.e., where one part of the subnet is out of range of the other part), then when these distinct groups cycle their group keys, the two halves of the subnet will no longer share a common subnet group key. Should these two halves re-join, they will need to automatically manage a "subnet merge" to agree on a common key. Note that MANETs from different nations — or from the same nation but from different subnets — will not use the "subnet merge" strategy to share data, but will use gateways as will be discussed in Section IV.

We consider a subnet that is divided into two halves; we will refer to them as Snet-A and Snet-B. Additionally, each subnet will have an elected commander node, which we call Cdr-A and Cdr-B. When two nodes (*n1* from Snet-A and *n2* from SnetB) come within transmission range of each other, they will each mutually detect the other by observing the mission key-encrypted headers of network traffic. These headers will allow the nodes to conclude that they belong to the same subnet but share different subnet group keys. Each node will send a message to its respective commander node notifying it of the nearby subnet, at which point the commander nodes will initiate the process for a subnet merge.

For simplicity, we describe the process from the point of view of Cdr-A initiating the merge. Cdr-A will instruct *n1* to establish a secure link with *n2* (using a session key). Cdr-A and Cdr-B will then utilize the secure link to communicate and negotiate a new subnet group key[2], where *n1* and *n2* serve as temporary gateways to facilitate this communication. The commanders will each distribute the new subnet group key to Snet-A and Snet-B as unicast traffic as described in Section III-A. Finally, *n1* and *n2* will be instructed to close the secure link and resume standard communications using the new subnet group key.

C. Key Revocation

A strategy with locally distributed subnet group keys enables commander nodes (or connected nodes operating from a fixed location such as a FOB) to remotely (and cryptographically) remove compromised nodes from the network through key revocation and re-keying. A compromised node is cryptographically removed by refreshing the subnet group key and sending it to each node in the subnet (uniquely encrypted for each node), while withholding the new subnet group key from the compromised node. At the same time, the commander node adds the public key certificate of the compromised node to a mission CRL to thwart attempts by the compromised node to re-join the network. The CRL update is shared to all allied commanders (connected via gateways, discussed in the next Section). In this fashion, if the revoked node attempts to re-join the network (as a nomadic node) the attempt will be rejected by the commander since the node is now listed in the CRL.

IV. Gateway Assignment and Security Association

In our proposal, communication and relay of information between two allied MANETs require a secure link between two member nodes, which we call gateways. Gateway nodes share radio (PHY and MAC) connectivity with one another, while maintaining a connection to their national MANETs; this may be achieved by one or more radios. We assume that every node has the capacity to act as a gateway node, and that one or more nodes are assigned to be gateways by the commander node.

Gateways at the tactical edge could allow for secure connectivity and information sharing between coalition MANETs, enabling improved command and control and situational awareness. Multiple gateways in MANETs provide a diversity of connections with a neighboring MANET, and allow optimizations such as load balancing between gateways. The protected core networking (PCN) technology relies on gateways in strategic networks [2-4] to facilitate quality of service (QoS) and policy negotiations. The PCN approach will be relevant at the tactical edge once the dynamic internetworking challenges of MANETs are resolved, challenges such as dynamically establishing security associations between gateways and network address translation between MANETs. In this and the next section, we propose solutions to these challenges.

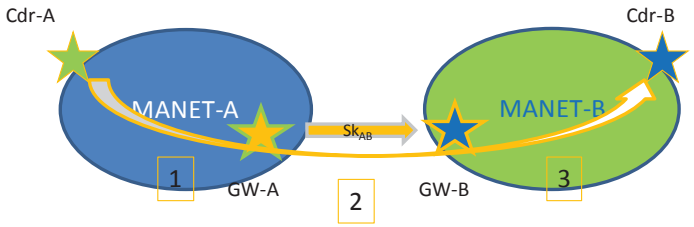

Fig. 1. A security association between gateway *A* (*GW-A*) and *GW-B* allows the two nodes to securely relay broadcast and policy-defined unicast traffic, e.g., traffic encrypted with CoI group key. Once in range, the nodes notify their respective commanders (Cdr) of the discovered allied MANET, as per mission encrypted traffic headers. The nodes are then assigned to become gateways by their respective commander nodes. The security association is established by exchanging public keys and CRLs, encrypted by the mission key, and addressed by MAC, network IDs and gateway IDs. Then a session key is exchanged following the *Group Key Creation and Distribution* (Section III-A) process, where the session key is encrypted with the receiving gateway's public key. All subsequent (negotiated) traffic between the MANETs will pass through the session key-encrypted secure link between the gateways, including ARP messages to exchange IP addresses.

We present our description analogous to that of the Subnet merge Section (III-B.2) above, where two nodes *n1*, *n2*, from nations *A* and *B*, respectively, come within transmission range of each other. The nodes will each mutually detect and identify one another by observing the mission key encrypted headers of their SA broadcasts (or other traffic) which will also include the network ID (NID). Each node will automatically notify its respective commander of a neighboring network. Again, from the point of view of commander *A* initiating gateway assignment, commander node *A* will instruct *n1* to assume the role of gateway for nation *A* (*GW-A*) and to establish a secure link with *n2* (using a session key), which will assume the role of *GW-B*, following commander *B*'s instruction. If *n2* is a nomadic node which has become disconnected from its commander node, it may assume the role of gateway autonomously.

A security association between the two gateways, depicted in Fig. 1, will be established once public keys are exchanged. The two gateways utilize the mission key to exchange public keys and CRLs. Instead of, or in addition to, using the mission key, the public key exchange could also be accomplished by a joint mechanism such as Diffie-Hellman [14]. The public key and CRL exchange is accomplished point to point via the MAC address, NID and the ID of the destination gateway, GW_BID, because its IP address has not yet been shared.

[2] This could be accomplished by either commander *A* or *B* generating a group key and sharing it with the other, or it could be accomplished by a joint mechanism such as Diffie-Hellman [14].

Once the public keys are exchanged, *GW-A* then creates and sends a session key (Sk_{AB}) to *GW-B* using the format presented in Section III-A, which encrypts the session key with the public key of the receiver in a unicast message:
$\{\{H\}_{MK}, \{Sk\}_{Pub\_k\_GW.B}, \{GW_BID, nonce, \{h(GW_BID, Sk, nonce)\}_{Pri\_k\_GW.A}\}_{Sk}\}$.
The gateways could then share address resolution protocol (ARP) messages, encrypted with the session key, and exchange IP addresses and subsequent relayed traffic of the form: $\{\{H\}_{Mk}, \{Data\}_{Sk}\}$. A gateway has the option of providing a public IP address for this purpose, protecting the private IP address it uses in its MANET subnet.

V. Network Address Translation (NAT)

In this section we present the MANET address translation portion of our proposal, which is essential in this interoperable architecture for sharing SA broadcast and CoI-encrypted traffic.

A. SA broadcast messages

The SA messages, broadcasted in MANET-A, are received at *GW-A*; if MANET-A is not fully connected, then *GW-A* will receive and relay a subset of SA messages. The SA data will include the node ID, network ID, public key, location, and other meta-data. The frequency and volume of relayed SA messages may be set based on policy agreements. The following steps summarize the data and address translation flows of a broadcast packet through two gateways; the step numbers correspond to those of Fig. 1 and Fig. 2:

1) The received SA data is encrypted with *Gk_A*, as shown in Fig. 2, left hand side with blue background.
2) *GW-A* replaces the encryption of the SA so that it can be sent through the secure link between the gateways. *GW-A* forwards the SA messages to *GW-B*, unicast using *GW-B*'s IP address.
3) The gateway in MANET-B replaces the encryption with *Gk_B* and re-broadcasts the SA message to the MANET.

B. CoI-encrypted traffic

Every coalition node can have the ability to dynamically establish encrypted CoIs with one or more nodes in the network. Establishing an encrypted CoI will allow nodes within the CoI to confidentially exchange data with one another, where only member nodes will have the key to decrypt the data. If we consider a CoI to be an encrypted enclave amongst the nodes of coalition MANETs, then a CoI can be thought of as a special case of establishing and using a group key amongst node members that could cross military command hierarchies and network boundaries.

The primary application for encrypted CoIs is to provide a mechanism for confidential data transmission among a group of nodes in the network, where the data is to be shared only with the nodes in the group and not with every node in the network. For instance, Cdr-A may wish to designate certain nodes in MANET-A and Cdr-B as "Intelligence" community. These nodes would share confidential information using an encrypted CoI group key — the messages would be relayed through the (non-CoI) nodes in the MANET, but only those

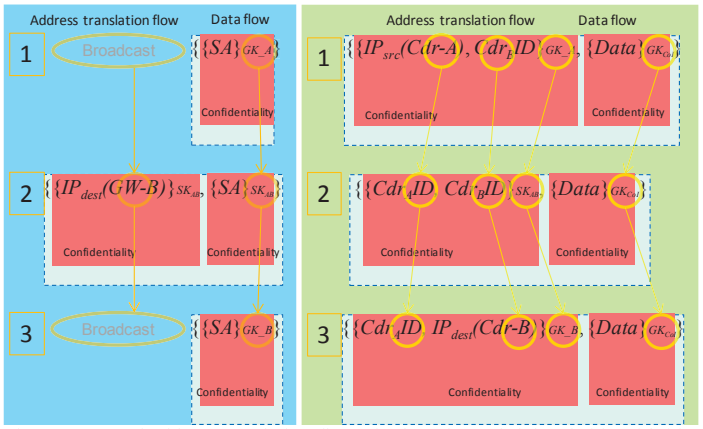

Fig. 2. Data and address translation flows for broadcast (left hand side with blue background) and CoI-encrypted traffic (right hand side with green background) are shown in steps 1-3 which correspond to the network locations shown in Fig. 1. **For SA broadcast**, *GW-A* receives an SA message with *Gk_A* encryption (step 1). It then decrypts it and re-encrypts it with the Sk_{AB} and forwards it to *GW-B* (step 2). In MANET-B, the gateway decrypts the SA message and re-encrypts it with *Gk_B* and broadcasts it to the MANET (step 3). **For a CoI-encrypted traffic** between two commanders, neither gateways change the Gk_{CoI} encryption of the CoI data. *GW-A* receives the CoI message with source and destination [IP_{src}(Cdr-A), Cdr_BID] addresses encrypted with *Gk_A* (step 1). It then decrypts and re-encrypts the addresses [Cdr_AID, Cdr_BID] with the Sk_{AB} and forwards it to *GW-B*, having replaced IP_{src}(Cdr-A) → Cdr_AID (step 2). In MANET-B, the gateway decrypts the CoI message addresses and re-encrypts them with *Gk_B* and forwards the message to the proper destination, having replaced Cdr_BID → IP_{dest}(Cdr-B) (step 3). In all, the private IP addresses are protected in gateway transition by being replaced with public IDs. The non-CoI members are capable of routing CoI packets because the addresses are encrypted with proper group keys.

nodes with the CoI group key could decrypt them.

The creation of an encrypted CoI requires two things: first, a new group key must be created and second, the key must be securely shared with all members of the CoI. Any node capable of establishing a CoI must have the ability to create group keys; thus, the assurance associated with the CoI may be related to the assurance of the node that creates it, especially applied to MANET nodes whose trust is monitored according to a trust model [15].

A node that creates a new CoI will create a new group key and will send a copy of it to each of the members of the CoI. To share the CoI group key with members of the CoI, the originating node sends individual unicast messages, each encrypted specifically for individual CoI members, similar to the process in Section III-A. For example, the following message could be used by node *j* to send a CoI group key to node *n*:
$\{\{H\}_{MK}, \{Gk_{CoI}, j\_ID, nonce, \{h(Gk_{CoI}, j\_ID, nonce)\}_{Pri\_k\_j}\}_{Pub\_k\_n}\}$.
This message is signed by node *j* and contains the CoI key encrypted with the public key of node *n*, which is known from SA broadcast messages. In our example, a CoI group key (Gk_{CoI}) is created and sent from Cdr-A to Cdr-B. Other members of the CoI must receive a similar unicast message.

To be routed properly, these messages that are destined to a member in another MANET will be sent to the local gateway by default. For example, in MANET-A, messages destined to Cdr-B will be addressed to *GW-A* in the local routing table of Cdr-A, a sample of which is shown in Fig. 3. Linked with the routing table containing each destination's node ID or IP address, we keep track of its public key and its possible session key or CoI group key. We must maintain an

Destination	Proxy Destination	Next	Local Interface	Distance	Public Key	Session Key	COI Group Key
ID \ IP Address	*IP Address*	*IP Address*	*MAC Address*	*# hops*	*12..*	*AB..*	*BC..*
IP(GW-A)	*N/A*	*IP(neighbor)*	*To neighbor*	*K*	*23..*	*CB..*	*DE..*
Cdr_BID	*IP(GW-A)*	*IP(neighbor)*	*To neighbor*	*K*	*34..*	*6F..*	*EA..*

Fig. 3. Commander-A's routing table is enhanced by the fields (in blue font) to keep track of its destination nodes' IDs and keys. In this sample representation of Cdr-A's routing table, *IP(GW-A)* acts as the 'Proxy Destination' address for Cdr_BID. Therefore, the values of the following fields in these two tuples (rows) will be the same, shown in yellow highlight: 'Next' hop's IP address en route to the 'Destination' is accessible by the 'Local Interface' MAC address. 'Distance' represents the number of hops to the 'Destination'.

association between these pieces of information. The sample shown in Fig. 3 is from Cdr-A's routing table in which Cdr-B's IP address is not known and, instead, its node ID (Cdr_BID) is linked to the IP address of *GW-A*. Essentially, *IP(GW-A)* acts as the 'Proxy Destination' address for Cdr_BID. In the sample table of Fig. 3, Cdr-B has its unique 'public key', 'session key' and 'CoI group key', but it shares the same content as *GW-A* in the following fields: 'Next' represents the IP address of the next hop neighbor in MANET-A en route to the 'Destination'; 'Local Interface' represents the local MAC address of Cdr-A that connects to the en route 'Next' hop neighbor; and finally 'Distance' represents the number of hops to the 'Destination'.

Once the CoI group key is disseminated, the communication exchange may begin amongst the members of the CoI. As shown in Fig. 2, right hand side with green background, the CoI data will remain encrypted through the gateways with Gk_{CoI}. We summarize the address translation flow of a CoI-encrypted packet through the two gateways in the following three steps which also correspond to the network locations in Fig. 1:

1) Because the (public) IP address of the destination node may not be available, we address the packet with the identification of the destination node, in this case Cdr_BID. The (private) IP address of the source (IP_{src}*(Cdr-A)*) is known inside MANET-A and it is used in the address field. The source and destination addresses will be encrypted with the *Gk_A* of the originating MANET-A.
2) *GW-A* replaces the source IP address with its associated (public) identification so that its (private) IP address in MANET-A may be protected, e.g., IP_{src}*(Cdr-A)* → Cdr_AID. The public identification of the destination (Cdr_BID) remains unchanged in the address field. Thus, both source and destination nodes now have public IDs in the address fields. *GW-A* also replaces the encryption of the addresses so that they can be sent through the secure link (via Sk_{AB}) between the gateways.
3) The gateway in MANET-B keeps the (public) ID of the source (Cdr_AID) but replaces that of the destination with its associated (private) IP address, e.g., Cdr_BID → IP_{dest}*(Cdr-B)*. *GW-B* then encrypts the addresses with its *Gk_B*.

Nodes using a CoI to send data would continue to use the standard message headers and would also need to ensure that signaling and routing information is encrypted with the subnet group key. This ensures that any allied node in possession of the mission key and subnet group key will be able to relay CoI information without access to the CoI-encrypted data.

CoIs are intended for use at the application level — that is, only certain application data would be encrypted with the CoI key, with other application data encrypted using the standard group key. Finally, we note that the CoI provides encryption only for data in transit — CoI encryption for data at rest locally on a device is out of scope of this proposal. Double encrypting CoI-encrypted data with the section *Gk* (within a MANET) is an option that could provide the result that revoking the subnet group key would make CoI-encrypted data unusable.

VI. Conclusion

We have proposed an architecture for secure interoperability in coalition MANETs. The architecture consists of a key dynamic management strategy, a gateway security association and a network address translation scheme. Our key management strategy leverages the hierarchy of military command to support, in a scalable fashion, the features of key creation, exchange and revocation which are used for tactical applications including authentication, communication and situational awareness updates. In addition, our proposed architecture includes features to support the following scenarios at the tactical edge: re-joining a nomadic node to an (allied) MANET, merging two MANETs of the same nation, relaying situational awareness data across allied MANETs and establishing and relaying encrypted community of interest data across allied MANETs.

References

[1] *North Atlantic Treaty Organization (NATO) Standardization Agency (NSA) Narrowband Waveform Network Standardization Agreement (STANAG), ACOMP-5633, Draft Edition 1.5, November, 2014.*

[2] *Lies, M., Dahlberg, D., Steinmetz, P., Hallingstad, G. and Calvez, P., THE PROTECTED CORE NETWORKING (PCN) INTEROPERABILITY SPECIFICATION (ISPEC), NATO Communications and Information Agency, Technical Report 2013/SPW008905/13, 2013.*

[3] *Hallingstad, G. and Oudkerk, S., Protected core networking: an architectural approach to secure and flexible communications. IEEE Communications Magazine, 2008.* ***46****(11): p. 35-41.*

[4] *Schutz, R., McLaughlin, S., Daeleman, T., Luoma, M., Peuhkuri, M., Carlen, P., and Haines, J. Protected Core Networking (PCN): PCN QoS and SLA definition. in Military Communications and Information Systems Conference (MCC). 2013.*

[5] *Dalal, R., Singh, Y. and Khari, M., A Review on Key Management Schemes in MANET. International Journal of Distributed and Parallel Systems (IJDPS) 2012.* ***3****(4).*

[6] *El-Sayed, A., Clustering Based Group Key Management for MANET, in Advances in Security of Information and Communication Networks, A. Awad, A. Hassanien, and K. Baba, Editors. 2013, Springer Berlin Heidelberg. p. 11-26.*

[7] *Lee, S.H., Alapati, N., Gerla, M. and Lee, K.W. Multiple Metric Gateway Election in Heterogeneous MANETs. in Army Science Conference. 2010.*

[8] *Gupta, A.K., Kumar, R. and Gupta, N.K. A trust based secure gateway selection and authentication scheme in MANET. in IEEE International Conference on Contemporary Computing and Informatics (IC3I). 2014.*

[9] *Yuan-Ying, H., Yu-Chee, T., Chien-Chao, T., Chi-fu, H., Jung-Hsuan, F. and Hsiao-Lu, W. Design and implementation of two-tier mobile ad hoc networks with seamless roaming and load-balancing routing capability. in Quality of Service in Heterogeneous Wired/Wireless Networks, 2004. QSHINE 2004. First International Conference on. 2004.*

[10] *Rahman, F.M. and Gregory, M.A. IP Address Associated 4-N Intelligent MANET routing algorithm utilising LTE cellular technology. in Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian. 2012.*

[11] *Echols, C. and Lysek, K. Tactical interoperable communication standards (TACOMS) - A key enabler to achieving NATO Network Enabled Capabilities. in NATO IST Symposium, Military Communications. RTO-MP-IST-054, 2006.*

[12] *Brown, J.D., Salmanian, M., Simmelink, D., Tang, H. and Song, R., Tactical edge cyber command and control (TEC3) concept: A vision for network situational awareness and network command and control at the tactical edge, Defence R&D Canada (DRDC) Scientific Report (SR), DRDC-RDDC-2014-R155, 2014.*

[13] *Brust, M.R., Andronache, A., Rothkugel, S. and Benenson, Z. Topology-based Clusterhead Candidate Selection in Wireless Ad-hoc and Sensor Networks. in Communication Systems Software and Middleware (COMSWARE). 2007.*

[14] *Diffie, W. and Hellman, M., New Directions in Cryptography. IEEE Transactions on Information Theory 1976. **22**(6): p. 644-654.*

[15] *Salmanian, M., Pan, L., Hu, J. and Li, M. On the Efficiency of Establishing and Maintaining Security Associations in Tactical MANETs in Group Formation. in IEEE MILCOM 2011.*