Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

A cross layer architecture for improved performance and security in tactical networks

David Kidston, Li Li, Helen Tang and Peter Mason

Defence R&D Canada – Ottawa

Canada

Technical Memorandum
DRDC Ottawa TM 2011-131
October 2011

A cross layer architecture for improved performance and security in tactical networks

David Kidston
Li Li
CRC

Helen Tang
Peter Mason
DRDC Ottawa

Defence R&D Canada – Ottawa

Technical Memorandum
DRDC Ottawa TM 2011-131
October 2011

Principal Author

Original signed by David Kidston

David Kidston

Research Scientist

Approved by

Original signed by Joe Schlesak

Joe Schlesak

Head/CRC/DCP

Approved for release by

Original signed by Chris McMillan

Chris McMillan

Chairman Document Review Panel

Abstract

Cross-layer mechanisms are often proposed for coping with performance issues in mobile ad hoc networks (MANETs). The concept behind this technique is for each protocol layer to be enhanced to exploit information produced by other layers so as to optimize network-wide operations. However, the need for a new interaction paradigm inside the protocol stack has to be balanced against the need for layer separation that allows for easy development, maintenance and integration with existing systems. Tactical networks are a type of MANET characterized by limited mobility and low bandwidth for which efficiency and performance are not just desirable, but critical for successful operations. Such networks are also characterized by strict security requirements, which can subject them to excessive bandwidth and processing burdens. In this paper, we argue that network security and performance could be improved in tactical networks through cross layer design. A cross-layer architecture is described that maintains a clean horizontal interface between layers, but also allows layers to coordinate cross-layer information through a vertical publish-subscribe interface. We explore this architecture through its application specifically to the performance and security of tactical networks.

Résumé

On propose souvent les mécanismes intercouches (*cross-layer*) pour faire face aux problèmes de performance des réseaux mobiles ad hoc (MANET). Le concept qui sous-tend cette technique est le suivant : améliorer chaque couche du protocole afin qu'elle exploite l'information produite par d'autres couches de manière à optimiser les opérations du réseau entier. Cependant, le besoin d'un nouveau paradigme d'interaction au sein de la pile du protocole de communication doit se mesurer au besoin de séparation des couches qui facilite le développement et la maintenance des systèmes existants, ainsi que l'intégration à ces systèmes. Les réseaux tactiques (type de réseau MANET) se caractérisant par une mobilité réduite et une faible bande passante, leur efficacité et leur performance ne sont pas seulement souhaitables mais essentielles au fonctionnement opérationnel. Un réseau de ce type se distingue également par des exigences strictes en matière de sécurité, ce qui peut leur imposer une bande passante et une charge de traitement excessives. Dans cet article, nous soutenons qu'un design intercouche pourrait améliorer la sécurité et la performance des réseaux tactiques. Une architecture intercouche maintient une interface horizontale nette entre les couches et permet également à celles-ci de coordonner les informations d'autres couches grâce à une interface verticale dite « de publication et de souscription ». Nous explorons en particulier l'application de cette architecture du point de vue de la performance et de la sécurité des réseaux tactiques.

This page intentionally left blank.

Executive summary

A Cross Layer Architecture for Improved Performance and Security in Tactical Networks

David Kidston; Helen Tang; Li Li; Peter Mason; DRDC Ottawa TM 2011-131; Defence R&D Canada – Ottawa; October 2011.

Introduction or background: Tactical wireless networks are often bandwidth constrained and require strong security to protect both the data within the network and the integrity of the network itself. These security requirements can be difficult to implement when they demand bandwidth resources that the network is incapable of offering. At the heart of the problem is the layered approach used in the design of network protocols. The approach of having each layer operating independently of the others in the stack is one which has worked extremely well for wired networks, but is proving cumbersome in certain types of wireless networks, particularly those intended for tactical environments.

The problems of efficient network management and integration of security in tactical wireless networks can be mitigated to some degree by the introduction of cross-layer solutions. Cross-layer design allows for targeted information from each layer to be shared with other layers so that performance can be optimised at each layer in a coordinated manner and with a more global view of the networking environment.

Results: We present a cross-layer architecture that uses a vertical interface through which each layer in the network model can access a common metric store on a publish-subscribe basis. This architecture allows for context-aware decisions to be made at each layer. This architecture is well-suited for a policy-based approach for integrating security and network management. We show how this design enables security applications such as intrusion detection and authentication to be managed more effectively and present a case study for implementing the Lightweight Integrated Authentication (LIA) algorithm.

Significance: Cross-layer network management allows for the network to optimise for QoS, survivability, or security posture and to adapt in real-time to changes in its environment. The integration of a policy engine into the design is a significant benefit since policy plays such an important role in military communications and operations. An automated integration of policy into all layers of the network can help develop the efficiencies needed to deploy secure tactical wireless networks. Finally, an important aspect of this architecture is that it preserves interoperability with existing standards.

Future plans: This architecture could be modelled in a simulator such as Qualnet in order to gain an understanding of which metrics are required or could have the greatest impact on improving network security and efficiency. In addition, mobility models need to be considered so that the effect of limited lifetimes of certain metrics can be understood.

Sommaire

A Cross Layer Architecture for Improved Performance and Security in Tactical Networks

David Kidston; Helen Tang; Li Li; Peter Mason; DRDC Ottawa TM 2011-131; R & D pour la défense Canada – Ottawa; octobre 2011.

Introduction ou contexte: Les réseaux tactiques sans fil présentent souvent une bande passante réduite et requièrent une sécurité renforcée pour protéger à la fois les données du réseau et l'intégrité du réseau lui-même. Ces exigences en matière de sécurité sont parfois difficiles à mettre en œuvre si elles sollicitent des ressources en bande passante que le réseau est incapable d'offrir. L'architecture en couches utilisée dans la conception des protocoles de réseau est au cœur du problème. Ce type d'architecture, qui préconise le fonctionnement indépendant de chaque couche dans la pile, a démontré de bons résultats dans le cas des réseaux câblés, mais montre un manque d'adaptation à certains types de réseaux sans fil, particulièrement ceux qui sont destinés aux environnements tactiques.

La mise en place de solutions intercouche peut régler jusqu'à un certain point les problèmes d'efficacité au plan de la gestion de réseau et de l'intégration de la sécurité aux réseaux tactiques sans fil. Le design intercouche permet le partage de données ciblées entre couches de manière à ce que chacune d'entre elles présente une performance optimale et coordonnée. Il offre également une meilleure perspective d'ensemble de l'environnement du réseau.

Résultats: Nous présentons une architecture intercouche utilisant une interface verticale qui permet à chaque couche du modèle de réseau d'accéder à un entrepôt commun de mesures en fonction des opérations de publication et de souscription. Cette architecture favorise la prise de décisions éclairées au niveau de chaque couche et convient à une approche de l'intégration de la sécurité et de la gestion de réseau fondée sur la politique. Nous montrons comment le design intercouche améliore la gestion des applications de sécurité, comme par exemple la détection des intrusions et l'authentification, et présentons une étude de cas sur la mise en œuvre de l'algorithme d'authentification intégrée légère (AIL).

Importance: La gestion intercouche permet d'optimiser un réseau au plan de la qualité de service, de la pérennité ou de la sécurité et de l'adapter en temps réel aux changements que subit son environnement. L'intégration d'un moteur de politique au design intercouche constitue un atout important, puisque la politique joue un rôle important dans les communications et les opérations militaires. Son intégration automatique dans toutes les couches du réseau permet de développer l'efficacité nécessaire pour déployer des réseaux tactiques sécurisés sans fil. Enfin, un aspect important de ce design est la préservation de l'interopérabilité avec les normes existantes.

Perspectives: L'architecture intercouche pourrait être modélisée dans un simulateur, tel Qualnet, dans le but de cerner les mesures nécessaires et celles le plus susceptibles d'améliorer la sécurité et l'efficacité du réseau. Par ailleurs, les modèles de mobilité doivent être pris en compte pour comprendre les conséquences de la durée de vie limitée de certaines mesures.

Table of contents

List of figures

1 Introduction

Tactical communications networks are limited by low bandwidth, high error rates and mobility. Existing protocols suffer degraded operations in the tactical environment to the point that very little useful operational information can be communicated, especially considering the additional bandwidth required for management and security. One of the reasons for this is the protocol overhead engendered by a layered protocol design that was developed for resource-rich wire-line equipment.

One topical solution is to find cross-layer efficiencies by sharing information between protocol layers. Each layer can then optimise its performance based on a more complete picture of the state of communications locally and potentially within the rest of the network. There has been quite a bit of research in the use of this cross-layer design in generic mobile ad-hoc networks (MANETs). Indeed, John Stine proposes in [1] that cross layering is a requirement for efficient MANET design and operation since the current layered design prevents desirable interactions between layers that can be exploited for improved performance.

However, a mobile tactical network embodies distinct characteristics when compared with MANETs. The type of MANET most cited in the literature are WiFi MANETs based on the IEEE 802.11 standard. While WiFi radios offer a link bandwidth between 2.5MHz to 10MHz or data bandwidth of 1.1Mb/s to 4.4Mb/s, tactical radios that operate on the military VHF/UHF bands only provide bandwidth from a few to a couple of hundred kHz [2]. These tactical radios support robust long range signals of 5km, 10 km or even 30 km through complex terrains [3] and provide jamming resistance using simple anti-jamming techniques (e.g., channel frequency hopping).

- In a tactical network, the responsiveness, reliability and robustness are paramount, instead of scalability, which is often the key objective in other types of networks. Though a tactical network might scale up to 100 or 200 nodes in the future, it currently consists of 20 – 60 nodes on average, or even fewer for operations on the move. This is much smaller than networks such as the fixed IP network, whose design principles lead to today's networking protocol stacks.
- Tactical networks must support bandwidth-intensive 1-to-many and many-to-many real-time group communications such as all-informed voice, group push-to-talk, situational information sharing, etc despite their limited available spectrum.
- Mobility is limited due to slow speed of tactical nodes and the long transmission range of VHF/UHF tactical radios. The long range also results in a large node degree in the network leading to strong network connectivity but also to a congested node vicinity.

Performance and security are two critical issues in tactical networks. Compared with WiFi MANETs, perhaps the most serious networking issue is limited bandwidth. Several methods of improving performance have been proposed or implemented at different layers. To mitigate medium congestion for network access and to support real-time tactical communications, a TDMA (Time-Division Multiplex Access) scheme is often employed to schedule MAC (Media Access Control) layer transmissions. This can provide the required priority and pre-emption required in tactical networks. Similarly at the network layer, the overhead caused by protocols headers may reach more than 100% of the transmitted data. We have previously proposed the use

of header compression and packet aggregation to alleviate this problem [4]. It may be possible to use cross layered coordination of these and other schemes to increase network efficiencies.

Security is another critical issue in tactical networks as well as MANETs. Byzantine attacks and spoofing are examples of potential security threats that are investigated in the literature. Byzantine attacks are a particular threat in wireless networks. In this case distributed and often unseen peers in the network cooperate to interfere with network functions such as routing. Behavioural and statistical analyses at the network level are generally used to identify and mitigate Byzantine threats. Spoofing is an application layer threat where the adversary attempts to inject apparently valid messages into the network for some desired effect such as congestion and data corruption. Authentication of nodes and users at the application level is a common solution. Again, cross-layer solutions would allow results from one level to be shared with another in order to improve their effectiveness. In this case, results of a trust systems and authentication systems could be coordinated to locate rogue nodes.

Cross-layer optimisation for mitigating performance and security issues in WiFi MANETs is relatively well known, but this technique has rarely been applied to tactical networks. In [5] a cross-layer architecture is proposed with a vertical management plane to support multimedia services in tactical networks. This research, like much in the field, focuses specifically on QoS requirements and does not discuss other management activities in the network. Another example is [6] where Policy-based management (effectively, constraint satisfaction) is applied concurrently to the spectrum allocation, routing, network planning, and mission planning layers for tactical networks. Our work is focused on a cross-layer solution which is suited for security and management functions at all protocol layers.

In this report we present a cross-layer architecture to support improved performance and security in tactical networks. Cross-layering is accomplished through a vertical interface implemented as a publish-subscribe metric store. Each layer may publish locally measured, derived or created metrics that may be of interest to other layers which may, in turn, alter their operations based on the metrics to which they have subscribed. However, horizontal boundaries between adjacent layers are left unchanged. This allows legacy layers to interoperate with enhanced layers. A separate management plane has been included in this architecture. Within this plane vertical services have access to the metric store to monitor the status of the network and also influence the protocol layers by publishing operational metrics. These cross-layer services may be automated through interactions with a policy system.

The remainder of the paper is organised as follows. In Section 2 we describe the cross-layer architecture developed for this environment. The value of this framework to tactical networks is explored through its application to performance and security. In Section 3, the cross-layer architecture is described in terms of its potential impact on network performance in the operation of individual protocol layers. In Section 4 several cross-layer security services including frequency hopping, intrusion detection and distributed authentication are discussed. Finally, the framework is investigated more in depth in Section 5 in terms of a case study based on our previous work on lightweight authentication for tactical networks. The paper ends with Section 6 with some conclusions and future work.

2 Cross-Layer Architecture

The most relevant previous work on cross-layer design is associated mainly with achieving better QoS in MANETs through improved routing, resource allocation, or per-node queuing [7]. Cross-layering similarly be applied to improve the efficiency of network security. In this section we propose a cross-layer architecture that can support several advantages in the creation and operation of communication protocols for tactical networks. These potential advantages include service optimisation, context awareness, service adaptation, service coordination, efficiency, development opaqueness, and service automation.

Since the operations of the different network layers are available, network functions can be re-written to **optimise** for things such as survivability, communications range, and throughput. Similarly, by providing a method for sharing metrics between the layers the various applications and protocol layers can be informed immediately about changes in the tactical network environment and communication posture to provide the node with **context awareness**. Context awareness allows the protocols to **adapt** in real-time to environmental changes, and if necessary notify remote nodes. The centralisation of data for local communication metrics allows each layer to **coordinate** its operation with other layers in a consistent manner. Instead of each layer calculating its own version of a metric, the network management service can provide node appropriate normalised metrics for use by all other services. This coordination provides an **efficient** method for reducing processing and storage overhead. The separation of metric-store information passing (horizontal information) with operational information passing (vertical information) means that layers can be developed and maintained without invalidating other layers. This **opaqueness** avoids the negative consequences of spaghetti code by controlling the interaction between layers both horizontally and vertically [8]. The option of policy control for the cross-layer services allows the context awareness and adaptation to be combined into an **automated** method for management though the execution of per-layer policy directives rather than operator entered per-node configuration directives.

When developing this cross-layer architecture, there were several approaches which could be taken to increase the cooperation between different layers. The simplest is the use of enhanced interfaces between layers to directly notify adjacent layers of events. An example of this is the explicit congestion notification mechanism which can be used by the network layer to tell the transport layer that congestion has been detected on the communication route [9]. The most extreme change would be to rewrite the entire communication stack as a monolithic cross-layer pipe where protocol information can be shared without regard to its origin. This latter method would however result in code that is difficult to produce and maintain. There is also the question of interoperability with exiting protocols.

In our work we followed the approach of the MobileMAN project [10] and use an architecture which is fully compatible with existing standards (each layer's core functionality is unchanged) and thus allows for the development and maintenance of protocol layers to be independent of the other layers. This maintains interoperability with current network implementations while retaining the benefits of modular design. Cross-layer information sharing is provided by a separate "horizontal" information pipe.

To attain horizontal cross-layer information sharing while supporting strict backwards compatibility we propose the use of a publish-subscribe system as vertical interface between layers [11]. This messaging system is available to all protocol layers so that critical metrics of operation can be shared as desired. For this reason we have called the messaging system the Metric Store. Each enhanced layer is able to publish their internally calculated and derived operational metrics in the metric store. These metrics can be subscribed to by any other enhanced layer or by a separate cross layer service if any exist. Cross-layer network services such as management and security are concerned not with the operation of any particular layer, but are instead "helper" services that provide additional information for use by enhanced network layers. If a layer is not enhanced, it will not be able to participate in cross-layer optimisations. However, the complete network stack will continue to operate correctly. The complete architecture is shown in Figure 2.

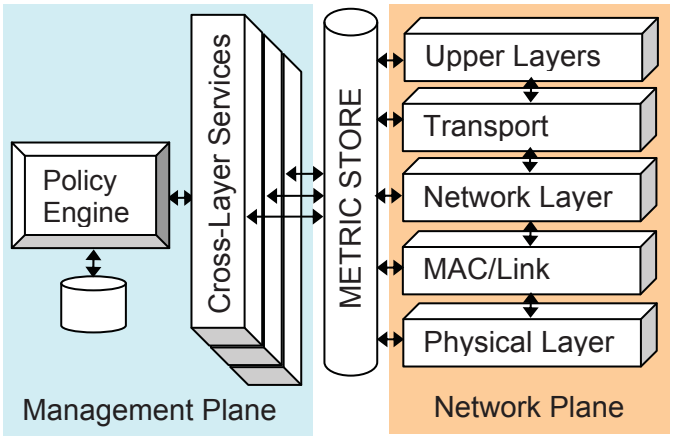

Figure 1: Cross Layer Architecture.

This architecture was designed to coordinate protocol operations (including security) across the various network layers. In particular, per-layer information can be combined to build a security situational awareness picture that can aid the operator or an automated management system to determine an appropriate course of action to a network attack. This type of design can also mitigate the effect of individual security mechanisms operating at different protocol layers from working at cross-purposes to one another.

The individual components of the architecture are described in more detail below.

2.1 Metric Store

The heart of the system is the metric store, a persistent publish-subscribe based message queue with the following properties:

- robust to failure (transactional in nature)
- old messages(metrics) may be immediately purged upon update by the publisher
- no data filtering (all subscribers can see all stored messages)

- guaranteed delivery (all subscribers will receive the message as soon as it is posted if they are available, and if not will receive it when they "return")
- messages are acknowledged by subscribers
- secure (in the sense publishers and subscribers are authenticated and subscribers must meet the publishers authorisation requirements, messages may be encrypted)

This message queue if available to all protocol layers as well as cross-layer services as a clearinghouse for information that may be of interest to others. Each layer/service must be able to function without such information being available, but for cross-layer optimisation the use of such information is encouraged.

2.2 Enhanced Protocol Layers

In order to provide performance gains, protocol layers can be enhanced to make use of information shared through the metric store. This information may be published by other layers or cross-layer services. Interoperability with un-enhanced layers is ensured since the standardised horizontal interface between layers remains unchanged. Enhanced layers will continue to operate even if cross-layer information they would like to use is not available. Care must be taken to ensure that protocol layers on each node remain consistent in the case where the node will need to communicate with remote legacy nodes. The use of a gateway is possible, and should be considered especially in the case of MANETs such as tactical network which are likely to connect with backbone infrastructure for some applications.

2.3 Cross-Layer Services

Unlike previous recommendations for cross layer design, we propose the development of separate cross-layer services for the purpose of protocol stack wide enhancements such as network management and security. These services interact with the metric store in the same way as enhanced protocol layers. They have access to the complete set of metrics from all layers and at the same time are unburdened by layer-specific requirements. Each protocol layers can thus focus on their core functionality while subscribing to value-added metrics instead of calculating them locally. For example, instead of calculating a layer-specific view of the network status, the enhanced layer could use the metrics published by a cross-layer service devoted to network monitoring. The use of metrics from a service that has a more complete view of the local node and the local network can reduce per-layer processing overhead and avoid potential conflicts with other layers when diverging views of the environment are calculated independently..

2.4 Policy Engine

In order to aid in the operation of the cross-layer service, a mechanism for directed automation and adaptation has been added to our architecture. Policy-based systems are well known for their support of network management functions, and can also be of use for directing other services such as security. In tactical networks coordination among nodes may be limited by bandwidth constraints. For this reason the use of policy directives (which are generally less resource bandwidth intensive than configuration scripts) are desirable for tactical networks.

This page intentionally left blank.

3 Application: Per-Layer Enhanced Performance

In this section we provide several examples of cross-layer enhancements through the network layers and review the applicability of our cross-layer architecture to the tactical networking environment.

3.1 Physical Layer:

It could be assumed that the physical layer would be best enhanced by modifying its operation to fit the information flow demands placed on it by higher layers. For example metrics published by the MAC layer could be used by the physical layer to choose spectrally efficient transmission properties (power, waveform, etc.) in real time. Such techniques are fairly well known [7].

A more complex example of this can be found in [12] where the requirements for extremely fast forwarding of information in MANETs can be achieved if we assume the use of multiple (shared access) radios per node. Coordination between the physical, MAC and network layer allows flows received on one radio to be sent out on another radio immediately to minimise round trip transmission time. The problem of how to ensure the next hop is ready to receive (no contention), requires the coordination of the MAC layer (reading physical and network layer metrics) so that an end-to-end transmission silence can be achieved for this particular traffic flow. Note that this requires the cooperation of all possible interfering nodes, an example of non-local cross-layer management. In our architecture this would be achievable by using the cross-layer management service to note when such a flow was becoming active in the region of the local node. Such a service would be of potentially great value in tactical networks where some nodes, especially vehicular mounted ones, have multiple radio platforms already. In such cases, one could also envision one communication path being activated when another is under attack, or applying a different level of cryptography to different links when the security posture deems it appropriate.

3.2 Data Link (MAC) Layer

There have been many proposals on how cross-layer information can be used to enhance the MAC layer. One of the more straightforward methods involves using metrics from all layers (especially physical) to tune the amount of error correction included in MAC frames. This allows error correction to be optimised so that a minimal overhead per frame can be achieved to reach the desired reliability. Another such method is the use of metrics published by the application layer about how much traffic to expect to help in resource access negotiation. Application requirements could also be shared with neighbour nodes for an even more optimised distributed solution.

A more complex scheme described in [7] suggests the use of scheduled but unused transmission slots to re-transmit data towards a receiver along a “disjoint” path. Such cooperative transport should only be done if confident that the data being transmitted has sufficient priority and can make use of the increased probability of success of part of its data (application layer metrics). Network layer cooperation is needed to provide metrics characterising alternate paths to the destination. Note that this scheme may impact other protocols that rely on knowledge of the

physical layer's use of spectrum to know about network congestion. Coordination through a cross-layer network management service is one method to keep track of the true value of this type of metric (including for distribution to remote nodes).

Critical to tactical networks, the MAC layer discussion is an appropriate place to talk about efficiency in the use of spectrum from a throughput point of view. As mentioned previously, in such networks a TDMA MAC is used engendering fixed size MAC frame sizes. As discussed in the case study below, each network packet is currently sent in its own, meaning potentially low application data throughput. This "unused" space can be filled with any remaining traffic to be transmitted, like "SMS messages" – assign no space but gets through eventually. This method can be used to efficiently transmit network-wide management information to remote nodes. The case study provides a more comprehensive treatment in terms of data.

3.3 Network Layer

A standard proposal for the network layer is to use of physical and link layer metrics to provide smarter routing and thus better per-flow better QoS [7]. This can involve avoiding routes through nodes that are overloaded, mobile, or otherwise experiencing poor forwarding success. A more complex proposal for the network layer consists of routing schemes for improved security. By evaluating the current physical layer metrics (for reliability) and the security requirements from application packets (security classification) network routing can be based on which nodes are the most trusted. This trust can be arrived at based on the neighbouring nodes past performance on forwarding traffic, crypto-logical, or other factors. This information could also be used at the network layer to add IPsec authentication headers (AHs) to protect particularly sensitive payloads for forwarding over un-trusted nodes. Since the security metrics are centrally stored this avoids duplication of application or other level security schemes. Efficiencies are provided by ensuring that security can be added using the most appropriate scheme by coordinating with the network management service.

3.4 Transport Layer

The transport layer is mainly concerned with providing a reliable and connection oriented service to the application layer. In tactical networks this would benefits from coordination with lower layers to ensure that such services remain efficient. An example of cross-layer design at the transport layer can be found in [13]. In this work the reliable transmission multiple jpeg images in a sensor network is achieved through a number of mechanisms. First, the verification of lower layer success rates is used to synchronise transmission priority at the network level so that images from multiple sensors are received at the same rate. At the application layer the nature of the jpeg application standard is used for progressive transmission so that a low resolution picture can be displayed when the picture is partly transmitted and further detail is unveiled as more data arrives. The transport layer is also another layer that can make use of cross-layer, either to deny access to the medium for flow based applications in times of high security risk, or reducing the number of flows allowed in times of low network QoS.

3.5 Upper Layers

Though little has been published on cross-layer effects at the upper layers, there are still some examples of how it can be useful. One example has to do with the use of MAC information (queue lengths) to avoid cache pre-fetching in times of congestion [14]. In this scheme, the MAC layer's published backlog of transmissions can be used by enhanced applications/session layer to know that the network is currently busy and no pro-active information retrieval across the network should be done.

Another potential application is the use of geographical location to provide applications with context-based information. By routing location sensitive information only to people in a certain geographical area, the other nodes are not burdened with unnecessary traffic (efficiency). Also, from a security point of view, there it represents a way to avoid information leakage (security). In this architecture, the metric store would contain location information generated by the physical (GPS) or network (topological) which could be used by the network layer to avoid routing beyond of the desired geographical area.

A final example of application level cross-layer enhancement is its use for multi-factor authentication. With multiple layers providing authentication methods (from different hardware to different communication streams to operations conformance), information published to the metrics store can be collated by the cross-layer security service into a single authentication value. The value can be used by any layer for efficiency (no layer needs make this calculation on its own) and for enhanced reliability (additional robustness since multiple methods are being used).

This page intentionally left blank.

4 Application: Cross-Layer Security

There are advantages to using this cross-layer architecture for security in tactical networks. By using metrics from the security services at the upper layer, such as from authentication systems and intrusion detection systems (IDS), sensing for cognitive networks at Layer 1 (physical) and Layer 2 (data link) can be made more secure. Authentication and intrusion detection can be integrated into a single cross-layer security service and the results (metric or metrics) can be used by different layers to improve their efficiency (they don't have to calculate the security metric themselves) and robustness (security is derived from multiple methods). While this framework may increase the complexity and internal processing within a node (in order to integrate multiple functions), it can reduce the communication requirements between nodes (since confirmation with neighbouring nodes is no longer as critical). This is especially beneficial to tactical networks where communication is the more expensive operation. Some potential security services that could be integrated into this framework are described below.

4.1 Intrusion detection

Intrusion detection systems (IDS) can be employed to determine when the network is being subjected to a network or application layer attack. Such systems are one of the more effective ways to counter Byzantine threats. An IDS can benefit from the establishment of a "trust model", for example, to distinguish among friends, acquaintances and adversaries. An intrusion detection or similar behavioural analysis engine can be charged with monitoring neighbours. In tactical networks, the IDS will likely need to be local and distributed rather than centralised as it is in wired networks. This leads to a "watchdog" approach where nodes monitor and analyse the behaviour of their local neighbours [15].

Lessons can be drawn from existing work in the area of Byzantine routing, including consensus algorithms to eliminate falsified information, which can make the system more robust. There are also various methods of establishing trusted routes based on hash chains and digital signatures, but these methods may prove to have too much overhead and consume too much bandwidth to be applicable to tactical networks [16]. In fact, many of the security overlays proposed in the area of ad hoc networking suffer from overhead issues or complicate the communication protocols such that interoperability among coalition partners could be threatened if different security solutions are employed. Research is being conducted that allows for the provision of security services such as intrusion detection and authentication in mobile ad hoc networks without relying on additional messaging [15], however it is often the case that detection of an attack at one layer requires mitigation techniques be applied at another. For example, if a Sybil attack, in which a node claims several identities, is detected at the application layer, the response may be to block all traffic coming from the attack's location by eliminating the route from the routing table [17].

4.2 Distributed authentication

For security services in a distributed network, threshold cryptography is generally used to let some or all network nodes share a network master key and collaboratively provide security services such as issuing and refreshing private keys. In a network with N nodes, a group of n

special nodes is capable of generating partial certificates using their shares of the certificate signing key. A valid certificate can be obtained by combining k such partial certificates, which is called (k, n)-threshold cryptography.

In MANETs, identity (ID)-based cryptography with threshold cryptography is a popular approach for the security design because key management is simpler than that of public key infrastructure (PKI). In threshold schemes, the network can tolerate the compromise of up to (k −1) shareholders. The security of the whole network is breached when a threshold number of shareholders (k) is compromised. Therefore, the optimal selection of nodes in threshold cryptography should be carefully investigated. However, most previous work for key management in this framework concentrates on the protocols and structures. Consequently, how to optimally conduct node selection in ID-based cryptography with threshold secret sharing is largely ignored. In [18], a distributed scheme based on the stochastic multi-arm bandit formulation is proposed. The proposed scheme can select the best nodes for reconstructing the full secret taking into account the security conditions to minimise the overall threat posed to the network. We can utilize the information obtained from the metric store for node selection. For example, we can assign a weight value for a node based on the information from metric store. If a node has high security, it may have higher weights. We then conduct the node selection process considering the weights to achieve higher security.

5 Case Study: Lightweight Integrated Authentication

In order to further validate our architecture, this section describes a security problem for tactical networks and details how a solution can be augmented using our cross-layer architecture. We base the case study on previous work on the lightweight integrated authentication (LIA) scheme in MANETs [19]. Authentication is an important element of network security because it is the first step toward prevention of, and guarding against, unauthorized access to network resources and sensitive information. We hope to efficiently utilize the authentication results for other security services such as secure routing through the cross-layer scheme. LIA is summarised below, followed by a discussion of how it could be adapted to and benefit from a cross-layer design such as the one detailed in this paper.

5.1 Overview of LIA

In the LIA scheme, each node maintains a trust table which is a fusion of security information of all the neighbouring network nodes. It is first established based on authentication and then kept updated based on any available IDSs and the key self-revocation mechanism of LIA. The value of the trust field can be thought of as raw data – its utilisation is application dependent [19]. One application is secure routing.

The details of managing the trust table are provided as follows:

Step 1: Bootstrapping: As described by McGrath et. al. [20], LIA uses an off-line PKG that generates Identity Based Encryption (IBE) private keys for all devices based on their unique identities. This is feasible in tactical networks because before deployment, users with their devices have to report to a command post where the Private Key Generator (PKG) could be located.

Step 2: Pre-authentication: Using its private key and the public key of its recipient node, every node can compute its pairwise symmetric key for authentication with the recipient. This key is the same for both nodes because of the bilinearity property of IBE [21].

Step 3: Credential establishment: The pairwise symmetric keys are communicated between the two nodes. The symmetric key is encrypted for confidentiality using the public key of the recipient, and signed for authentication using the private key of the sender.

Step 4: Authentication: Mutual authentication is performed when the two nodes compare their pair-wise symmetric keys. This key can also be used as session key for securing the data communications. A trust table is then built to store the trust values of its neighbours. The value of the trust field can be either Boolean (e.g., zero or one) or multi-level (e.g., zero, low, medium, high). Once node i is authenticated by node j, the trust value of node i can be set to one in node j's Trust Table. Once the public key of node i is revoked, the trust value of node i can be set to zero in node j's Trust Table. The Trusted routes could then be established through authenticated nodes with non-zero trust values. A zero value in the trust field indicates existing routing functionality making the trusted routes a subset of all available routes. Security policy can define if a message can be routed through all available routes or only trusted routes

Step 5: Monitoring: This is accomplished through continuous user-to-device authentication with IDS. User and device are assumed to be tightly coupled in a tactical operation. When user-to-device authentication fails, it implies that the device is not in the hands of a legitimate user. This event triggers revocation of the public key of the device. We recommend performing user-to-device authentication through wearable biometric sensors because they have the following properties: 1) direct user binding, 2) non-disruptive re-authentication, 3) inherent liveliness detection [22].

Step 6: Revocation: LIA introduces a self-revocation mechanism by leveraging the integration of user-to-device and device-to-network authentication. This concept is illustrated in Figure 3. Once the user-to-device authentication fails, which implies the compromise of the device, the device informs the neighbouring nodes using a GoodBye message. The node will then be excluded from the trusted routes of its neighbors. The GoodBye message is similar to a Hello message in a proactive routing protocol such as the Optimised Link State Routing protocol (OLSR) [23] but it performs a GoodBye-type operation, excluding the sender from its neighbours' trusted routes. The existing message handlers in OLSR can be re-used to process this message to implement the Distributed Revocation Authority and to propagate the GoodBye message to neighbouring nodes' Trust Tables.

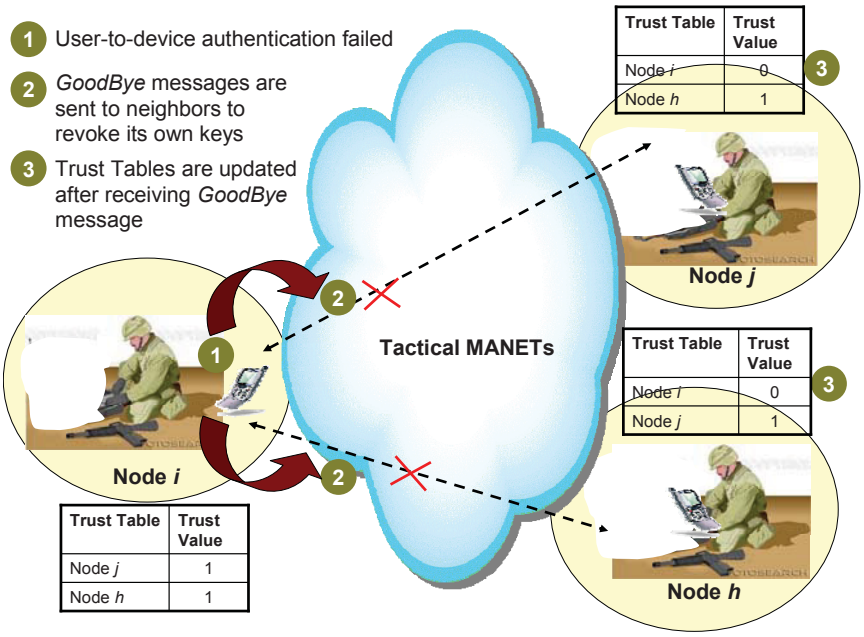

Figure 2: LIA's Self-revocation Mechanism.

In order to create a GoodBye message, LIA proposes adding a LinkType to the existing format of the Hello message indicating that the trust value of the sender should be changed to zero in the receivers' trusted routing table. The GoodBye messages must be encrypted and sent to all the neighbours as adversaries may fabricate such messages to cause public keys of uncompromised nodes to be revoked – a denial of service attack.

5.2 LIA within a Cross-layered Architecture

As we mentioned in Section 5.1, the trust table can be viewed as the fusion of the security information of all network nodes. As such, it is a natural extension to allow the trust table to be a part of the metric store. The trust value can be set with the authentication and IDS results obtained in the application layer, results which can also be part of the metric store. Any layer that is interested in the trust values can subscribe to the service and access the trust table. In the following, we list 4 examples showing how 4 layers can enhance their security by utilizing the trust values.

1. At the session layer, a security policy can be defined to allow applications establish sessions with those nodes that have a minimum trust value. During a session establishment, in addition to session parameters such as IP address and port number, the trust value of a node is also communicated. The source node automatically decides whether to continue establishing a session to that destination node or not. The applications can range from e-mail, FTP, HTTP, VoIP or even a video or data session. Deploying this approach at session layer not only eliminate user intervention but also reduces the security risks while adaptively adjust to time varying security requirements.

2. At the routing layer, routing table can be built incorporating the trust values. The routing table is built based on certain routing algorithms such as OLSR [23]. The security of routing algorithms is usually addressed through cryptographic algorithms. If we could incorporate the trust values when we build the routing tables, we can more efficiently enforce certain security policies such as letting a message be routed through any available route or only through nodes with certain trust value. This feature is especially useful in coalition operations where multiple countries cooperate but with different security requirements. For example, certain encrypted messages like command and control messages for designated receivers must be routed through nodes with a minimum trust value.

3. For MAC layer, longer medium access time may be allocated to the nodes that have higher trusted value;

4. For physical layer, we can utilize the information obtained from the trust table for distributed spectrum sensing. We can increase the trustworthiness of the spectrum sensing results by assigning higher weights to the sensing results obtained from nodes with higher trust values.

There are two main advantages of using LIA within this scheme for tactical MANETs. It results in less communication overhead between nodes and it enhances the security at different layers, allowing greater flexibility in defining the security policy according to application needs.

This page intentionally left blank.

6 Conclusions and Future Work

In this paper we have introduced an architecture for enabling cross-layer-based services to improve performance and security in tactical networks. This architecture consists of a vertical integration layer called a metric store in which each protocol layer from the physical layer to the application layer can publish their internal operational metrics or alternately subscribe to metrics from other layers. This publish-subscribe messaging model allows the protocol layers to remain logically separated in functionality so that each layer can be developed and maintained separately, but also provides the option of making use of information available from any other layer in the network plane.

A set of vertical services may also make use of the metric store. In the management plane a set of cross-layer services may act as subscribers to the operations of the enhanced protocol layers, while at the same time publishing metrics of their own. These metrics can be as simple as compound metrics that distil multiple metrics into a single more useful metric to save individual layers from duplicate processing. Alternately, they can be complex configuration directives based on internal logic informed by some adaptive or autonomous system such as a policy-based system. The application of this type of capability to the per-layer and cross-layer security of tactical networks has been outlined here.

6.1 Advantages for Tactical Networks

There are several potential advantages to using a cross-layered architecture including service optimisation, context awareness, service adaptation, service coordination, efficiency, development opaqueness, and service automation. Since the operations of the different network layers are available, network functions can be re-written to **optimise** for things such as survivability, communications range, and throughput. Similarly, by providing a method for sharing metrics between the layers the various applications and protocol layers can be informed immediately about changes in the tactical network environment and communication posture to provide the node with **context awareness**. Context awareness allows the protocols to **adapt** in real-time to environmental changes, and if necessary notify remote nodes. The centralisation of data for local communication metrics allows each layer to **coordinate** its operation with other layers in a consistent manner. Instead of each layer calculating its own version of a metric, the network management service can provide node appropriate normalised metrics for use by all other services. This coordination provides an **efficient** method for reducing processing and storage overhead. The separation of metric-store information passing (horizontal information) with operational information passing (vertical information) means that layers can be developed and maintained without invalidating other layers. This **opaqueness** avoids the negative consequences of spaghetti code by controlling the interaction between layers both horizontally and vertically [8]. The option of policy control for the cross-layer services allows the context awareness and adaptation to be combined into an **automated** method for management though the execution of per-layer policy directives rather than operator entered per-node configuration directives.

A case study based on previous work on lightweight integrated authentication was used to show how this cross-layer architecture could be used to enhance per-layer security in this type of network. It also suggested how security-sensitive routing traffic could use a similar service, even in such a bandwidth constrained environment.

6.2 Future Directions

In order to quantify the improvements suggested in this report, our next step is a modeling and simulation exercise to measure the impact of this approach. We plan to model a tactical network using the Qualnet simulation environment. By simulating the mobility and traffic patterns of several tactical network scenarios, the relative improvement compared to non cross-layered performance and security services will be evaluated.

In addition to the efficiencies this architecture makes available to each layer, the metric store also provides opportunities for cross-layer services. These services are not application services supporting the user but rather network services supporting the operation of the network. As such they provide information through the metric store that can be used by any layer to improve their operation. This information is itself derived from input from the metric store (for adaptation) as well as input from other sources such as the policy engine (for automation).

When developing a new cross-layer service, the question becomes what information should be shared and how can it be used to provide enhanced "service" in the network. Current research using this method has focused on achieving improved QoS (service differentiation) in MANETs [7] but what about efficient resource utilisation, management and security? The use of information pathways other than the inter-layer boundary increases the complexity of developing enhanced protocol layers and cross-layer services. This must be managed so that it doesn't interfere with the intended goals of the cross-layer system. In mobile networks, even if the metric collection, distribution and processing are efficient there is still the problem of mobility. This implies that the "lifetime" accuracy and availability of shared metrics must also be considered.

The security of the metric store itself also remains to be addressed. For example, the metric store may be kept in Trusted Platform Module (TPM) chip [24] or Non-volatile random access memory (NVRAM) for security, with encryption techniques to increase its security.

References

[1] J.A. Stine, Cross-Layer Design of MANETs: The Only Option, in IEEE Military Communications Conference, 2006.

[2] L. Li and T. Kunz, Efficient mobile networking for tactical radios, in IEEE Military Communications Conference, 2009.

[3] J. Pugh, R. Bultitude, and P. Vigneron, "Propagation Measurements and Modelling for Multiband Communications on Tactical VHF Channels", proceedings of IEEE Military Communications Conference, Oct. 2007.

[4] D. Kidston and L. Li, "IP Header Compression and Packet Aggregation in Mobile Tactical Networks", proceedings of IEEE Military Communications Conference, Oct. 2009

[5] S. Ci and J. Sonnenberg, A Cognitive Cross-Layer Architecture for Next-Generation Tactical Networks, in IEEE Military Communications Conference, 2007, pp. 1-6.

[6] G. Denker, et al., An Architecture for Policy-Based Cognitive Tactical Networking in IEEE Military Communications Conference, 2006.

[7] Q. Zhang and Y-Q. Zhang, Cross Layer Design for QoS Support in Multihop Wireless Networks, in Proceedings of the IEEE, Vol. 96, No. 1, pp 64-76, Jan. 2008.

[8] V. Kawadia and P.R. Kumar, A Cautionary Perspective on Cross-Layer Design, in IEEE Wireless Communications, Vol. 12, No. 1, pp. 3-11, Feb. 2005.

[9] K. Ramakrishnan, S. Floyd, D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", IETF RFC 3168, Sep. 2001.

[10] M Conti, G. Maselli, G., Turi, and S. Giordano, Cross-Layering in Mobile Ad-Hoc Network Design, in IEEE Computer, Vol. 37, No. 2, pp. 48-51, Feb. 2004.

[11] D. Kidston, L. Li, "Management through Cross-Layer Design in Mobile Tactical Networks", Proceedings of the 12th IEEE/IFIP Network Operations and Management Symposium, Apr. 2010.

[12] R. Ramanathan, Challenges: A Radically New Architecture for Next Generation Mobile Ad Hoc Networks, in Proceedings of the 11th Annual International Conference on Mobile Computing and Networking, 2005, pp. 132-139.

[13] A. Boukerche, Y. Du, J. Feng, and R. Pazzi, A Reliable Synchronous Transport Protocol for Wireless Image Sensor Networks, in IEEE Symposium on Computers and Communications. 2008, pp. 1083-1089.

[14] J. Tian and M.K. Denko, Exploiting Clustering and Cross-Layer Design Approaches for Data Caching in MANETs, in Third IEEE International Conference on Wireless and Mobile Computing, 2007, pp.52-29.

[15] D. Lynch et al., Providing Effective Security in Mobile Ad Hoc Networks Without Affecting Bandwidth or Interoperability, in Army Science Conference 08, 2008.

[16] Y.C. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, in IEEE Security and Privacy, 2004.

[17] F. R. Yu, H.Tang, F. Wang, V. C.M. Leung, Distributed Node Selection for Threshold Key Management with Intrusion Detection in Mobile Ad Hoc Networks, in the 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-09), Vancouver, Canada, August 29-31, 2009.

[18] John R. Douceur, The Sybil Attack, Revised Papers from the First International Workshop on Peer-to-Peer Systems, p.251-260, March 07-08, 2002

[19] H. Tang and M. Salmanian, Lightweight Integrated Authentication for Tactical MANETs, in International Symposium on Trusted Computing (TrustCom-08), Nov. 18-21, 2008, Zhangjiajie, China.

[20] C. McGrath, A.S. Ghazanfar and M. McLoone, Novel Authenticated Key Management Framework for Ad Hoc Network Security, in Proceedings of. ISSC 2006, Dublin, June, 2006.

[21] D. Boneh, and M. Franklin, Identity-based encryption from the Weil Pairing, in Advances in Cryptology – CRYPTO ‘2001, LNCS 2139, pp 213-229, 2001.

[22] H. Tang, M. Salmanian and Q. Xiao, Biometric-based User Authentication for Tactical Mobile ad-hoc networks, (DRDC Ottawa TN 2007-100), Defence R&D Canada - Ottawa May 2007. Internal publication

[23] T.Clausen and P.Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003. http://www.ietf.org/rfc/rfc3626.txt

[24] Trusted Computing Group. TPM Specification Version 1.2 Revision 103. Trusted Computing Group, 2009.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Communications Research Centre
3701 Carling Avenue
Box 11490, Station H
Ottawa, Ontario K2H 8S2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC June 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

A Cross Layer Architecture for Improved Performance and Security in Tactical Networks

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Kidston, D; Tang, H; Li, L; Mason, P

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
October 2011	30	20

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC Ottawa TM 2011-131	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Cross-layer mechanisms are often proposed for coping with performance issues in mobile ad hoc networks. The concept behind this technique is for each protocol layer to exploit information produced by other layers so as to optimize network-wide operations. However, the need for a new interaction paradigm inside the protocol stack has to be balanced against the need for layer separation that allows for easy development, maintenance and integration with existing systems. Mobile tactical networks are typically characterized by limited mobility and low bandwidth for which efficiency and performance are not just desirable, but critical for successful operations. Such networks are also characterized by strict security requirements, which can subject them to excessive bandwidth and processing burdens. In this paper, we argue that network security and management can be achieved in tactical networks using cross layer design. A cross-layer architecture is described that maintains a clean horizontal interface between layers, but also allows layers to coordinate cross-layer information through a vertical publish-subscribe interface. We explore this architecture through its application to a number of case studies including per-layer performance and cross-layer security services.

On propose souvent les mécanismes intercouches (cross-layer) pour faire face aux problèmes de performance des réseaux mobiles ad hoc (MANET). Le concept qui sous-tend cette technique est le suivant : améliorer chaque couche du protocole afin qu'elle exploite l'information produite par d'autres couches de manière à optimiser les opérations du réseau entier. Cependant, le besoin d'un nouveau paradigme d'interaction au sein de la pile du protocole de communication doit se mesurer au besoin de séparation des couches qui facilite le développement et la maintenance des systèmes existants, ainsi que l'intégration à ces systèmes. Les réseaux tactiques (type de réseau MANET) se caractérisant par une mobilité réduite et une faible bande passante, leur efficacité et leur performance ne sont pas seulement souhaitables mais essentielles au fonctionnement opérationnel. Un réseau de ce type se distingue également par des exigences strictes en matière de sécurité, ce qui peut leur imposer une bande passante et une charge de traitement excessives. Dans cet article, nous soutenons qu'un design intercouche pourrait améliorer la sécurité et la performance des réseaux tactiques. Une architecture intercouche maintient une interface horizontale nette entre les couches et permet également à celles-ci de coordonner les informations d'autres couches grâce à une interface verticale dite « de publication et de souscription ». Nous explorons en particulier l'application de cette architecture du point de vue de la performance et de la sécurité des réseaux tactiques.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Network Management; Network Security; Cross-Layer Design; Tactical Networks

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

DEFENCE DÉFENSE

www.drdc-rddc.gc.ca