# Federating tactical edge networks: ways to improve connectivity, security and network efficiency in tactical heterogeneous networks

A. M. Hegland, M. Hauge, A. Holtzer

***Abstract*—This article elaborates on security and routing architectures for mobile tactical heterogeneous networks. It explores challenges and opportunities and highlights the characteristics of these types of networks and their differences from static and deployed networks. These architectures have value for designing national military networks, and especially for realizing IP based coalition networks at the mobile tactical edge. The article is based on work done within the NATO research group IST-124, and may serve as input for standardization of future federated tactical networks.**

***Index Terms*—Heterogeneous Networks, Security, IP, Routing, Mobile Ad Hoc Networks**

## I. INTRODUCTION

Successful military operations require efficient information sharing between the involved parties. Necessary preconditions are interoperability standards, guidelines and policies that enable interconnections between coalition partners' networks –from strategic level to the tactical edge.

Networks at the lower tactical levels are typically radio networks that use transmission technologies with dissimilar characteristics regarding bandwidth, frequency band, modulation scheme, delay, and range. This means low to high bandwidth, varying connectivity and delay, high bit-error rate, and nodes operating in radio silence behind the enemies' lines. Important types of traffic are voice group-communication and position data.

A node in a heterogeneous tactical network can be illustrated as shown in Figure 1. Users and applications connect to the LAN. The node connects to others via multiple radio networks. There will typically be a mix of long range narrowband radios and radios of shorter range but with higher bandwidth. Some radios have cryptographic protection (Z) embedded. Others depend on external crypto devices. The nodes in these tactical heterogeneous networks can be quite unlike as they span from dismounted soldier nodes that carry a single radio, via vehicle-mounted nodes with multiple users and radios, to stationary headquarters. Furthermore, the radios may be layer-three devices acting as routers or layer-two radios working as modems.

Figure 2 shows the radio model. A traditional IP protocol stack is assumed on the wired side. The wireless side can be a proprietary radio stack or an IP stack. Figure 1 shows multiple layer-three and layer-two radios with and without embedded crypto.

It is a challenge to make multinational heterogeneous tactical networks interoperable. Standards for interconnection of networks on the lower tactical level are currently not sufficiently present. This article is a step towards filling the gap. It highlights challenges and opportunities. The contribution is an exploration of different routing architectures and security concepts for heterogeneous tactical networks focusing on connectivity and security of data in transit.

The next section describes related work. Then the different routing architectures and their pros and cons are outlined. The following section elaborates on security challenges in tactical heterogeneous networks and their possible solutions. Impacts of different security concepts on the routing architectures are discussed before the final section that contains concluding remarks and suggestions for further work.

## II. RELATED WORK

Data dissemination schemes and networking approaches such as Software Defined Networking (SDN) [1] and Information Centric Networking (ICN) concepts outside the traditional IP architecture [2] are emerging. SDN decouples the forwarding plane from the control plane.

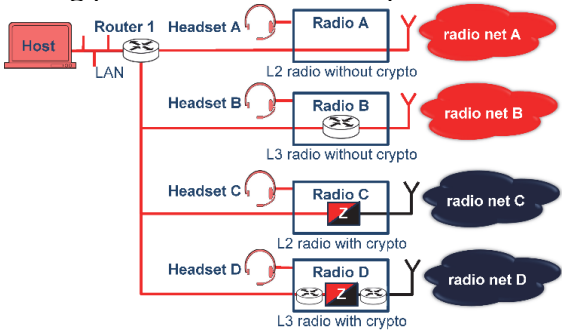


**Figure 1 Tactical heterogeneous network node**

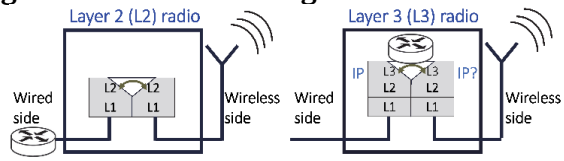


**Figure 2 Radio model**

*Anne Marie Hegland is with Kongsberg Defence & Aerospace*
*Mariann Hauge is with the Norwegian Defence Research Establishment*
*Arjen Holtzer is with TNO*


DOI til publisert versjon/DOI to published version: 10.1109/MCOM.001.1900508

Data are typically forwarded at layer two. The data may or may not be IP-based. ICN forwards data based on requests for specific content or names of the objects. Connectivity can be intermittent. It is fundamentally different from the host-centric IP paradigm. Reference [3] describes different deployments of ICN including combinations of ICN and IP such as ICN in the edge networks and IP in the core. Reference [4] discusses ICN in military networks.

Whereas these concepts may be included in the future, ongoing standardization for interoperability in military coalition operations such as the Federated Mission Networking (FMN) initiative, still rely on traditional IP networking [5]. This is the background for our work focusing on IP networking. A number of challenges need to be solved to achieve efficient and secure IP communication at the tactical level.

FMN adopts the Protected Core Networking (PCN) [6] concept. Collaborating nations share their transport network resources forming a Protected Core. Users are located in Colored Clouds (CCs) separated from the Protected Core by encryptors. These encryptors protect the user payload from CC to CC. The PCN concept was designed for fixed networks. Extending it to the tactical edge is still a topic for further studies.

The PCN concept can be implemented with SDN. The IST-142 group studies this [7]. How SDN can best be used for tactical edge networking, is still an active research topic [8]. As the SDN architecture for this domain matures, it can be one way to implement the concepts described in our work.

Reference [9] discusses content-based security policies at different layers of the TCP/IP model. Data are released based on attributes and labels. A related topic is Data Centric Security (DCS) [10] where each data object is encrypted separately. DCS is a necessity for cloud computing security. Mature solutions lack, and it is not evident how DCS can be implemented in a way that can be accredited and approved for protection of classified information. At least unless combined with other solutions such as those described herein.

## III. ROUTING ARCHITECTURES

**Figure 3** shows different routing architectures adopted for a meshed network topology [11]:

- *Flat*
- *Interconnect-Flat*
- *Interconnect-Overlay*

Each depends on a different information exchange interface (EI).

**Flat architecture** has one single routing domain. Every network segment runs the same routing protocol. It can consist of different transmission technologies, but it uses no proprietary routing protocols tailored for the specific transmission technologies. The architecture is typically deployed with layer-two radios that are connected to a tactical router that runs the common routing protocol. It requires a standardized EI between the routing function and the modem –referred to as EI-M.

The architecture could also be deployed with layer-three radios that run the common routing protocol on both the wireless and wired interfaces. The EI-M interface is then internal to the radio.

The flat routing architecture has its main benefits with high bandwidth and smaller heterogeneous networks where the amount of routing information will not fill the radio channels. It is also beneficial when most of the traffic is non-local and traverses multiple radio networks. Typically a proactive routing protocol is used and all nodes share the same view of the network.

One routing protocol used all over will likely cause reduced throughput compared to proprietary routing protocols tailored for the transmission technology.

Detection of link breaks and rerouting are done within one routing protocol, this is beneficial from an availability perspective. The uniformity makes configuration errors less likely, but more severe since all information is shared with all nodes in the network.

Nodes operating in radio silence behind the enemy's lines should continue receiving with their transmitter turned off. The radio systems are usually designed to handle this, but standard routing protocols that for instance expect periodic heart beats or acknowledgments are not compatible with this. This restricts the choice of routing protocol, or the candidate routing protocol may need an extension.

**Interconnect-Flat architecture** consists of interconnected network segments belonging to separate routing domains. The various network segments use standardized or proprietary routing protocols, running on a tactical router or as part of a layer three radio device.

Some segments may use identical routing protocols on separate frequency bands or under different administrative management. The routing domains are interconnected using a routing domain to routing domain Information Exchange Interface, referred to as *EI-R*. Each location that is part of multiple routing domains – that is, entities that run routing protocols from multiple routing domains – are called *interconnection platforms*. Each interconnection platform has an EI-R between each two routing domains. Via the EI-R, the routing domains inform each other about destinations that can be reached via the routing domain.

The solution is a well-known intranet architecture. Vendor specific protocols exist to implement the IE-R interface. It works well if only a few networks with few connections points are connected. The architecture has a high risk of routing loops. It therefore needs careful configuration – for instance share routes one way only [12]. This often leads to a setup where only a limited set of mobility scenarios is supported (transit of national networks unsupported).The scalability is better than with the Flat architecture at the cost of reduced end-to-end connectivity since typically not all information is shared and route sharing happens less frequently. Local connectivity and availability can be good as the Interconnect-flat architecture allows routing protocols that are optimized for the different transmission technologies. The end-to-end availability is more uncertain. Radio silence may or may not already be handled by proprietary routing protocols in the different network segments. With layer three

radios, support for radio silence often comes as an integral part of the proprietary routing protocol used over the radio net. Radio Silence support may be more challenging with layer two radios and routing handled by an external router with less awareness of the radio channel.

**Interconnect-Overlay architecture** resembles the interconnect-flat in the sense that it includes many network segments that are separate routing protocol domains. In addition, an extra layer of routing is introduced in an overlay that spans the whole heterogeneous network and connects the separate routing protocol domains. Only a subset of the routers in the heterogeneous network participates in the overlay network. These routers are located on the interconnection platforms. The scheme is similar to the architecture used by Inter Domain protocls such as Border Gateway Protocol (BGP) to connect different domains. A routing protocol Information Exchange Interface – referred to as *EI-RO* – is needed between the routing protocol in the overlay network and the routing protocol domains in the different network segments. The EI-RO is located on the routers in the interconnection platforms. Differently from the interconnect-flat architecture, there are no EI-Rs between the different routing protocol domains. It is also possible to apply a hybrid approach, for example an interconnect-overlay architecture that connects a collection of heterogeneous networks using the flat architecture and some single transmission technology routing domains. This is probably the most likely solution that can be tailored for a range of different scenarios.

Local traffic is handled by the local routing domains. End-to-end routing across routing domains is done by the overlay protocol.

Routing protocols to support Interconnect-Overlay architecture are still experimental, and the approach needs further exploration (see for instance [13]). Radio silence support must be included both locally in the different routing domains and in the overlay routing protocol.

The two-tier approach provides a flexible design. It is easier to deploy than the flat architecture, because it does not demand that all platforms run the same routing protocol. However, it requires that the parties agree on a common protocol for the overlay. The availability may be lower than for the flat design where all nodes maintain a view of the complete topology, but better than for the interconnect-flat where no single protocol has a global reach across the network.

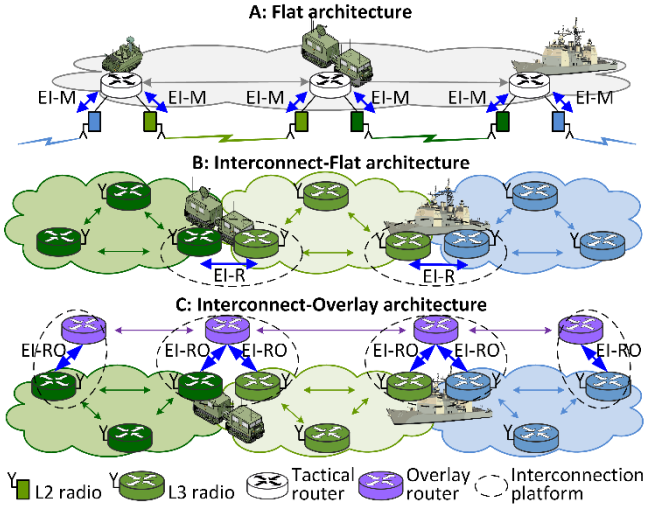


**Figure 3 Different routing architectures**

## IV. SECURITY IN TACTICAL NETWORKS

Appropriate protection of tactical heterogeneous networks – and networks in general –depend on the threats, what assets to protect, and the available protection schemes.

### *A. Assets to be protected*

**User payload** – Data that end-users and/or end-systems either generate or consume. This includes data from various types of data applications as well as voice. Confidentiality and integrity are essential; the user payload needs protection against unauthorised access and modification.

**User metadata** – information about who the user or system is, where he/she or it is, communicating peers, and communication patterns. It should be possible to conceal user metadata from unauthorised parties.

**Network management data** – the information that is exchanged in order to monitor and configure the network. The integrity and authenticity is essential in order to prevent disturbance and disruption of the network service. Confidentiality protection may also be required.

**Network control traffic and network metadata** – Network control traffic refers to the information that needs to be exchanged in order to keep the network service running –also referred to as network signalling, such as routing protocol messages. Network metadata is information about the network itself such as information on the network elements, addresses, mobility and communication patterns. Integrity and authenticity are important in order to prevent disturbance and disruption of the network service. Confidentiality protection may also be required in order to conceal network control traffic and metadata from unauthorised parties.

**Availability** – includes protection of the availability of the other assets as well as the availability of network components required to keep the network service running. Availability requires resilience to cyber attacks. It also requires protocols that account for the special characteristics of tactical hetereogenous networks regarding overhead, required responses and delays.

### *B. Trust, threat and attack vectors*

A large heterogeneous network will include a variety of entities. The article assumes a model with the following trust levels:

**Trusted internal entities** – this group includes own personnel with the proper security clearance and necessary authorization. It also includes certified and approved network elements, software, and hardware under proper physical protection and/or control of authorised personnel. This group can include coalition partners.

**Cooperative entities** – this includes network elements and actors that for instance are trusted to forward data correctly, but are not necessarily authorized to read the user payload conveyed. This can include commercial network providers, non-governmental organizations (NGOs), and coalition partners from the same or another alliance or

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/MCOM.001.1900508

different communities of interest. The cooperative entities are expected to behave according to the agreed protocol.

**Non-trusted entities** – this category includes other actors that are neither trusted nor authorized. The actors in this group may be malicious or non-malicious. It is hard to identify who belongs to which of these subgroups, and therefore we do not distinguish between malicious and non-malicious non-trusted entities. Any non-trusted entities could act maliciously.

The possible attack vectors include, but are not limited to, the end devices, the user applications, the network elements, the gateways, the software, the protocols and the wireless communication channels.

### *C. Cryptographic toolbox*

The specified protection of the assets can only be achieved through cryptographic mechanisms. These can be located at different layers in the OSI stack and on different places in the network: in the end hosts, intermediate routers and in the radios. We here define a cryptographic toolbox with three *levels* of protection: Application, Network, and Link Level Protection. These can also be mixed. All solutions have their pros and cons.

**Application Level Protection** refers to true end-to-end protection, and includes cryptographic protection located at the end hosts' network layer or above. Using Figure 1 as example, it encompasses DCS and any type of application layer encryption as well as transport and network layer schemes such as TLS/ SSH and IPsec implemented on the Host. Routing protocols and other protocols with cryptographic protection embedded in the protocol also fall into this category.

The overhead depends on the implementation and solution used. It can be from a few bytes with symmetric cryptographic schemes to several kilobytes where certificates and digital signatures are involved. Application Level Protection provides a fine-grained protection scheme. It enables communities of interest separation down to single hosts and applications. Another advantage is that one common transport network can be used for multiple security domains.

Application Level Protection protects user payload, but provides limited protection of user metadata and does not protect network management data, network control traffic and network metadata at all. A drawback of Application Level Protection as such, is that it leaves the end-systems open to attack. Additional measures are required in order to prevent attackers from gaining access to the end hosts.

The main disadvantages of Application Level Protection are the increased complexity of key management and requirement for trusted end hosts. The key management is significantly more complex compared to the case where a single crypto device protects multiple hosts. With application level protection every host needs to be securely provided with valid keys, and different keys are required for each of their security associations with other hosts. (Attribute Based Encryption (ABE) [14] that makes it possible to encrypt an object with one key and decrypt it by all recipients that possess the right attributes, may change this in the future.) Whereas Figure 1 only shows one host in each node, the number of hosts can in practice be large. Furthermore, the end hosts need to be certified and accredited. Cryptographic solutions used to protect classified data must undergo evaluation, certification and achieve security accreditation. Evaluation of a vast number of different hosts is time-consuming and expensive. Even if the number of hosts were limited to a few approved ones, the review and re-certification and re-accreditation is required every time the system configuration is modified – by patches, updates or new applications. In addition, off-the-shelf computers are frequently used behind a crypto device as they are cost-efficient and flexible, but they are in general not designed to meet the requirements to enforce the cryptographic protection of classified information. That is, the end hosts may not be a certifiable trusted platform, and not all end host equipment are able to support crypto.

**Network Level Protection** encompasses the traditional IPsec approach for perimeter protection based on network layer encryptors that separate the network into a red (plaintext) side and a black (ciphertext) side. The encryptor would typically be located between hosts in a LAN and the transport network as shown in Figure 1.

A benefit is that one crypto unit can protect a number of hosts and applications on the LAN side, and the encrypted data can be transmitted over an arbitrary unsecured network. One common transit network can be used for multiple security domains. Both user payload, red side routing information, and to some extent user metadata, are protected. Another benefit is that key management is easier compared to Application Level Protection as the same crypto function is used to protect multiple hosts.

IPsec tunnel mode adds an extra IP header plus an IPsec header. IPsec transport mode only adds an IPsec header, but is usually used together with a GRE tunnel or similar. Consequently, both modes of operation cause a significant amount of overhead. Black side network management data, network control traffic and network metadata are left unprotected. Another issue is that it does not provide true end-to-end protection of user payload. It only protects the data between the peer network layer encryptors. If these are located close to the originating host, this is usually not a problem. Network Level Protection represents a medium-grained protection scheme as it assumes all entities on its red side belong to the same security domain.

**Link Level Protection** includes the traditional hop-by-hop radio link protection approach. It protects not only user payload, but also network management data and network control traffic. In addition, it usually adds little overhead, which makes it more bandwidth efficient than Network Level- and Application Level Protection schemes. The disadvantages are that the hop-by-hop protection means that the traffic is decrypted and re-encrypted on every hop. This implicitly assumes all traffic belong to the same security domain. If there are cooperative entities that are trusted to forward data, but not access the content, additional protection is needed.

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/MCOM.001.1900508

**Hybrid solutions** use several mechanisms in series. Application Level Protection can for instance be combined with Link Level Protection. The benefit is that the user payload is cryptographically protected end-to-end from host to host, and the metadata and network control traffic are in addition protected hop-by-hop over the radio network. The disadvantages are basically the same as described for Application Level Protection. However, the requirement for certified end hosts may no longer be as hard as in the case when only Application Level Protection is used.

Hybrid solutions that combine Link Level Protection with Network Level Protection are probably even more common than those that include Application Level Protection. Multiple layers of protection can also be required as part of a "defence in depth" strategy [15] to ensure an attacker must pass multiple barriers to compromise the system.

Specific challenges related to hybrid solutions are added key management complexity and extra overhead with two levels of encryption.

### *D. Key Management*

Independently of what level the cryptogaphic protection is enforced at, the parties need the right key(s) to communicate. Confidence in the communicating peer is based on key posession. Depending on key(s) possessed, the peer is identified as a trusted internal or cooperative entity. Those that do no show possession of a correct key are considered non-trusted entities. Proper key management is a prerequisite. Constrained bandwidth, high bit error rates, varying connectivity and radio silence limit the applicability of key management solutions that demand on-line access to a central trusted entity and protocols with multiple rounds. The certificate sizes of public key schemes are another limiting factor. Besides, most of the communication at the tactical edge is group communication. There is no generally adopted and well-functioning method for group key establishment in tactical networks. Pre-shared keys – distributed during mission preparation – are therefore assumed. Pre-shared keys are expected to play an important role also in the future. Re-keying during mission represents a threat to availability and should be avoided.

## V. IMPACT OF SECURITY ON THE ROUTING

### *A. Concerns*

A main concern is if the security concept chosen for a routing architecture requires signaling to bypass cryptographic barriers. This either compromises the security or the chosen routing architecture cannot be implemented. A controlled bypass channel would solve the problem, but adds complexity, cost, and may not be acceptable for all classification levels.

Another concern is whether the security concept introduces multiple tunnels, more routing domains and parallel signaling across low capacity links. Resilience to cyber attacks is an additional concern.

### *B. General impacts of protection at different levels*

Application Level Protection is beneficial from a networking point of view as all cryptographic separation takes place on or above the network layer of the end host. The network service need not consider cryptographic boundaries. It does not affect the routing architecture, and makes no assumption about the underlying communication infrastructure.

Network Level Protection may introduce more routing domains –one on the black side and one on the red side of the cryptographic function. Network control traffic cannot pass freely between the red side and the black sides of a crypto device without compromising the security. Consequently, Network Level Protection can only be combined with a flat routing architecture if all routing happens either on the red or the black side.

Link Level Protection has no impact on the routing architecture as the encryption takes place hop-by-hop below the network layer.

Hybrid protection with Application Level and Link Level Protection is also fine from a networking perspective, as the encryption takes place above and below the network layer. Network Level Protection combined with Link Level Protection give the same challenges for the flat routing architecture as Network Level Protection alone.

All encryption layers will add extra overhead, but the overhead introduced by link layer encryption is generally low – usually significantly lower than the overhead provided by IPsec type of protection.

### *C. Securing heterogeneous tactical networks – challenges and opportunities*

A military deployment will likely –for a long time to come –include both layer-two and layer-three radios with or without crypto as Figure 1 shows. This cause challenges both from a security point of view as well as from a networking point of view.

#### *1) Mixing radios with and without crypto*

The layer-two Radio A and layer-three Radio B in Figure 1 do not have cryptographic protection embedded. Radio C includes crypto on layer two and Radio D on layer three. Radio C provides Link Level Protection. Radio D provides Link Level or Network Level protection depending on implementation and whether the data are decrypted and re-encrypted at each hop in the radio network.

Whereas data from the Host in the LAN as well as voice communication from the headsets are protected over radio net C and D, the configuration in Figure 1 is not sound from a security perspective. Data can be exposed in plaintext over radio net A and B. Additional protection is required. The headsets make it more complicated. The architecturally logical place to put services (including voice) is to the left of Router1 in the LAN. The move towards such a model is challenging, since current practical deployments often have user connections such as headsets for voice communication directly attached to the radio as shown in Figure 1. Secure and reliable voice communication is by many users regarded as the most critical service, and especially on the soldier level it has until now been hard to meet the user requirements without directly connecting the headset to the radio. Although vehicle and soldier

systems are being modernized, these connections will expectedly continue to complicate the security and network design – at least for the short and medium term. Secure voice communication with headsets directly connected to the radios can be achieved with crypto inside the radio.

*2) Tactial node with Network Level Protection*

Figure 4 shows one way to securing the configuration of Figure 1; the headsets have been removed from Radio A and B, and a network encryptor is inserted between Router 1 and Router 2 protecting all data that is transmitted over radio nets A and B. The solution is sound from a security point of view, but can impact the routing architecture in several ways. If routing is performed on the red side, the modem-to-router interface (IE-M) crosses a security boundary. In case there is both black and red routing, the routing information cannot flow in plaintext over the EI-R between Router 1 and Router 2 without causing a security breach. Router 1 and Router 2 will belong to different routing domains. In case all routing is on the black side, interaction with applications is complicated and link-level encryption is required to protect routing information. The placement of the Network Level Protection is therefore important. This applies both when the Network Level Protection is used alone and when combined with Link Level Protection in a Hybrid protection scheme. Also note that the overhead caused by the Network Level Protection schemes may prevent their use with low capacity radio channels.

*3) Application and Link Level Protection.*

Link Level Protection solutions have less impact on the routing architecture than Network Level Protection, in the sense that EI-R and EI-RO are less likely to cross a security boundary. The hop-by-hop Link Level Protection can be used as a Hybrid solution in conjunction with end-to-end Application Level Protection for proper protection of all assets.

All the described routing architectures can easily co-exist with this Hybrid solution, but it comes at the price of a more complex security solution. Link Level Protection is a commonly used protection type in tactical networks. The addition of Application Level Protection is less common. As long as there are only Trusted and Non-trusted entities in the trust model, this may be sufficient. The introduction of Cooperative entities makes additional protection necessary.

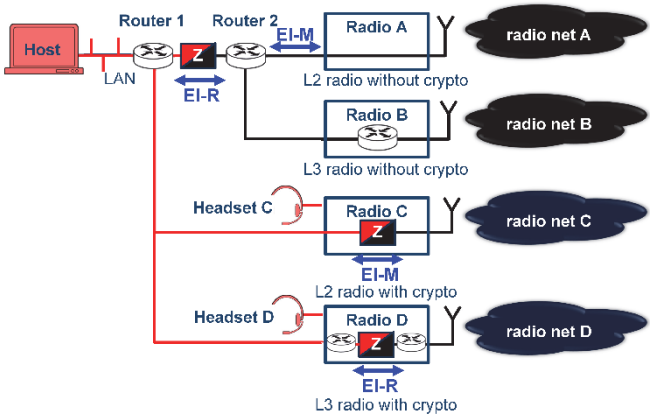


**Figure 4 Secure tactical communication node**

*4) Resilience to Cyber attacks*

Multiple factors determine the cyber attack resilience. A single protocol used all over leaves the flat routing architecture more vulnerable to cyber attacks in the sense that the impact of a successful attack on a single integrated system without additional internal compartmentalization may be larger. But monitoring and detection of cyber threats as well as reacting to cyber threats may be easier with a common flat routing domain.

With the interconnect solutions it is difficult to target the whole network, but maybe easy to find one vulnerable network segment that can be attacked. The assumption is that separate routing domains reduce the vulnerability compared to one large routing domain. A successful cyber attack on one domain does not necessarily affect the entire network. On the flip-side, it makes coherent monitoring and detection harder.

## VI. Concluding Remarks and Further Work

A central observation is that there is no one-size-fits-all routing architecture for tactical edge networks. When choosing routing architecture, consider:

- *Network size:* small networks enable sharing of network topology details, and a flat routing architecture can be a good option.
- *Nature of the traffic:* optimize for local traffic if most of the traffic is local to one transmission technology. Otherwise optimize for traffic that traverses different technologies.
- *Data capacity:* if the network consists of narrowband transmission technologies without capacity to distribute detailed topology and state information, choose the architecture accordingly.
- *Diversity in transmission technology:* For a tactical edge network with multiple radio and router types, an *interconnect* architecture is the most suitable. If participants agree on acquiring similar systems, the flat architecture can be an option.

In terms of security, Link Level Protection appears to be the most efficient regarding bandwidth and protection of all assets. However, it must be combined with Application Level or Network Level Protection for end-to-end protection when more communities of interests exist. Another argument for layered security is defence in depth. The Hybrid protection approach using Application Level with Link Level Protection appears to be most flexible, but has serious challenges in terms of its current feasibility. The other options are therefore important alternatives.

Standardization is a necessary precondition for interoperability, and security and routing should not be considered independently. A toolbox of standard schemes is required to achieve interoperability at the tactical edge.

The article extends the classical trust model of insiders and outsiders by including cooperative entities. When the network size and number of insiders grow, malicious insiders should be included in the model. Protection against malicious insiders requires additional measures such as system hardening and intrusion prevention. DCS

Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/MCOM.001.1900508

would also protect against both outsiders and insiders. How DCS can be implemented in a way that can be accredited and approved for protection of classified information is a topic for further work.

The article considers integration of tactical radio networks using classical IP routing. Alternative approaches with middleware for data dissemination, ICN, and network design improvements with the use of SDN are topics for further studies. Other topics for further studies are inclusion of Radio Silence awareness in tactical edge routing protocols and overlay interdomain protocols.

## References


[1] IETF RFC 7426 "Software-Defined Networking (SDN): Layers and Architecture Terminology," January 2015.

[2] IETF RFC 7476 "Information-Centric Networking:Baseline Scenarios," March 2015.

[3] A. Rahman *et al.*, "Deployment Considerations for Information-Centric Networking (ICN)," IETF Internet-Draft, September 3, 2019.

[4] L. Campioni *et al.*, "Considerations on the Adoption of Named Data Networking (NDN) in Tactical Environments," *ICMCIS*, Budva, Montenegro 2019.

[5] Federated Mission Networking Spiral 3 Specification, November 2018, https://storage.nisp.nw3.dk/20181118_Final_FMN_Spiral_3_Standards_Profile_Bundle.pdf, accessed November 9, 2019.

[6] G. Hallingstad and S. Oudkerk, "Protected core networking: an architectural approach to secure and flexible communications," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 35-41, 2008.

[7] S. McLaughlin *et al.* "National mobility in coalition tactical networks," *ICMCIS*, Oulu, Finland, 2017, pp. 1-7.

[8] J. Spencer and T. Willink, "SDN in coalition tactical networks," *MILCOM*, 2016, pp. 1053-1058.

[9] K. Wrona *et al.*, "Content-based security and protected core networking with software-defined networks," *IEEE Communications Magazine*, vol. 54, no. 10, October, 2016

[10] A. S. Arora, L. Raja, B. Bahl, "Data Centric Security Approach: A Way to Achieve Security & Privacy in Cloud Computing," *ICIoTCT*, March 2018.

[11] M. Hauge *et al.*, "IST-124 Final Report: Annex E - Architecture considerations for heterogeneous tactical networks," *STO-TR-IST-124-Part-I*, 2019.

[12] A. Holtzer *et al.*, "Tactical Router Interoperability: Concepts and Experiments," *MILCOM* 2018.

[13] L. Landmark *et al.*, "Resilient internetwork routing over heterogeneous mobile military networks," *MILCOM*, 2015.

[14] J. Tomida, Y. Kawahra, and R. Nishimaki, "Fast, Compact, and Expressive Attribute-Based Encryption," Cryptology ePrint Archive, Report 2019/966

[15] Y. B. Choi *et al.*, "Survey of Layered Defense, Defense in Depth and Testing of Network Security," *International Journal of Computer and Information Technology*, vol. 3, no. 5, 2014.


## Biographies


Anne Marie Hegland (anne.m.hegland@kongsberg.com) is a Department Manager at Kongsberg Defence & Aerospace, Norway. She received her M.Sc. in electronics from the Norwegian University of Science and Technology in 1997, and a Ph.D. in informatics from the University of Oslo in 2007. A main research interest is efficient and secure integration of heterogeneous tactical networks.

Mariann Hauge (mariann.hauge@ffi.no) received her M.S. in Electrical Engineering from the University of California, Santa Barbara in 1994 and her Ph.D. from the University of Oslo in 2007. She is currently a principal research scientist at the Norwegian Defence Research Establishment (FFI). Her current research interest includes point-to-point and group communication protocols as well as resource management and quality of service in heterogeneous mobile wireless ad hoc networks.

Arjen Holtzer (arjen.holtzer@tno.nl) is a Senior Consultant in the Networks Research Group of TNO, The Hague, The Netherlands. Arjen received his M.Sc. in Electrical Engineering from TU Delft, The Netherlands, in 2008. Currently, his main focus is on ICT-solutions for mobile tactical operations, with a particular interest in interoperability.



Dette er en postprint-versjon/This is a postprint version.
DOI til publisert versjon/DOI to published version: 10.1109/MCOM.001.1900508