A Distributed Routing Architecture for Secure Communication over Highly Dynamic Radio Networks

Sebastian Hanigk, Michael Kretzschmar and Frank Eyermann
Faculty of Informatics
Universität der Bundeswehr, München
{sebastian.hanigk, michael.kretzschmar, frank.eyermann}@unibw.de

***Abstract*—Highly dynamic *ad hoc* radio networks are the key technology for future military and crisis management operations but also raise additional challenges for secure communication between networks with higher security levels attached to mobile nodes.**

We propose an efficient solution to the currently not satisfactorily handled task of providing a mapping between node identifiers in the radio network and reachable addresses in the attached secure networks while separating security domains and supporting the nodes' ability to leave and join different radio networks, for example IP-based *ad hoc* or non-IP radio links. The approach is based on the concept of a distributed network element which encapsulates the radio network and hides its dynamic behaviour behind a single virtual network entity, e.g. a router which implements routing protocols of the adjacent networks; by means of suitably secured internal communication this entity is on the same security level as the attached networks.

While existing approaches mostly focus on more static environments or do not take different security levels into account, our proposed solution deals efficiently with highly dynamic radio node behaviour to flexibly build secure communication channels over the underlying radio transport network. We apply the generic concept in a case study to a concrete realisation based on an IP-based MANET as transport network for attached IP domains.

I. Introduction

Wireless networks have established themselves as a major part of many infrastructures but in their current role they mostly provide only access for edge devices. Furthermore, node mobility is ever increasing as are their capabilities for *ad hoc* networking. What is missing is the integration of these mobile networks as integral parts of a communication infrastructure due to security aspects currently not handled in a scalable and mobility-supporting way.

The next generation of military tactical networks, but also communication networks in crisis operations (e.g., networks of first responders after natural catastrophes) will constitute of IP-based radio networks. Radio devices installed in vehicles and mobile radio devices carried by people will form mobile *ad hoc* networks (MANETs) which allow communication not only with directly reachable participants of a radio circuit, but with anyone in the whole network infrastructure.

Virtual private network (VPN) techniques will be used between the mobile nodes to protect the transported information against eavesdropping when transmitting over the air. This results in at least two security domains: The encrypted information on the wireless network (referred to as *black*) and unencrypted information on the attached networks (referred to as *red*).

Typical scenarios are highly dynamic with a continuously changing topology of the MANETs and frequently leaving and joining nodes caused by node movement. Accordingly, the VPN built upon the wireless network needs to change dynamically, too: Static configuration of tunnels is neither efficient nor effective. Tunnel establishment must be based upon a dynamic process depending on the final destination of a packet and the current topology of the MANET. From the point of view of one mobile node, this task equals the problem of determining the most appropriate tunnel end point, given the final destination address of a packet.

Several approaches to solve this question exist, however, all of them lack the required flexibility, thus limiting the functionality of the whole system, especially the joining and leaving of nodes is not solved satisfactorily.

Focusing less on specific aspects of communication security but instead having a more holistic solution in mind, we propose an integrated but distributed architecture, based on the separation of forwarding and control elements, to enable not only routing and connectivity as such over an insecure wireless transport network, but also to provide efficiently a secure communication link infrastructure, taking into account the requirement for security and mobility.

This paper is organised as follows: after describing the scenario in section II, we deduce requirements for an approach which handles the specified problem. Afterwards we evaluate our problem in the context of previous works in section III; to provide familiarisation with the concept of a distributed router we introduce the ForCES architecture in general in section IV. In section V we propose a design for a secure network element and elaborate the proposed concrete solution approach in section VI. An evaluation of its properties follows in section VII and we conclude this paper in section VIII and give an outlook into further work.

II. Scenario

In the following a scenario from a military context is presented. The scenario motivates the requirements we develop

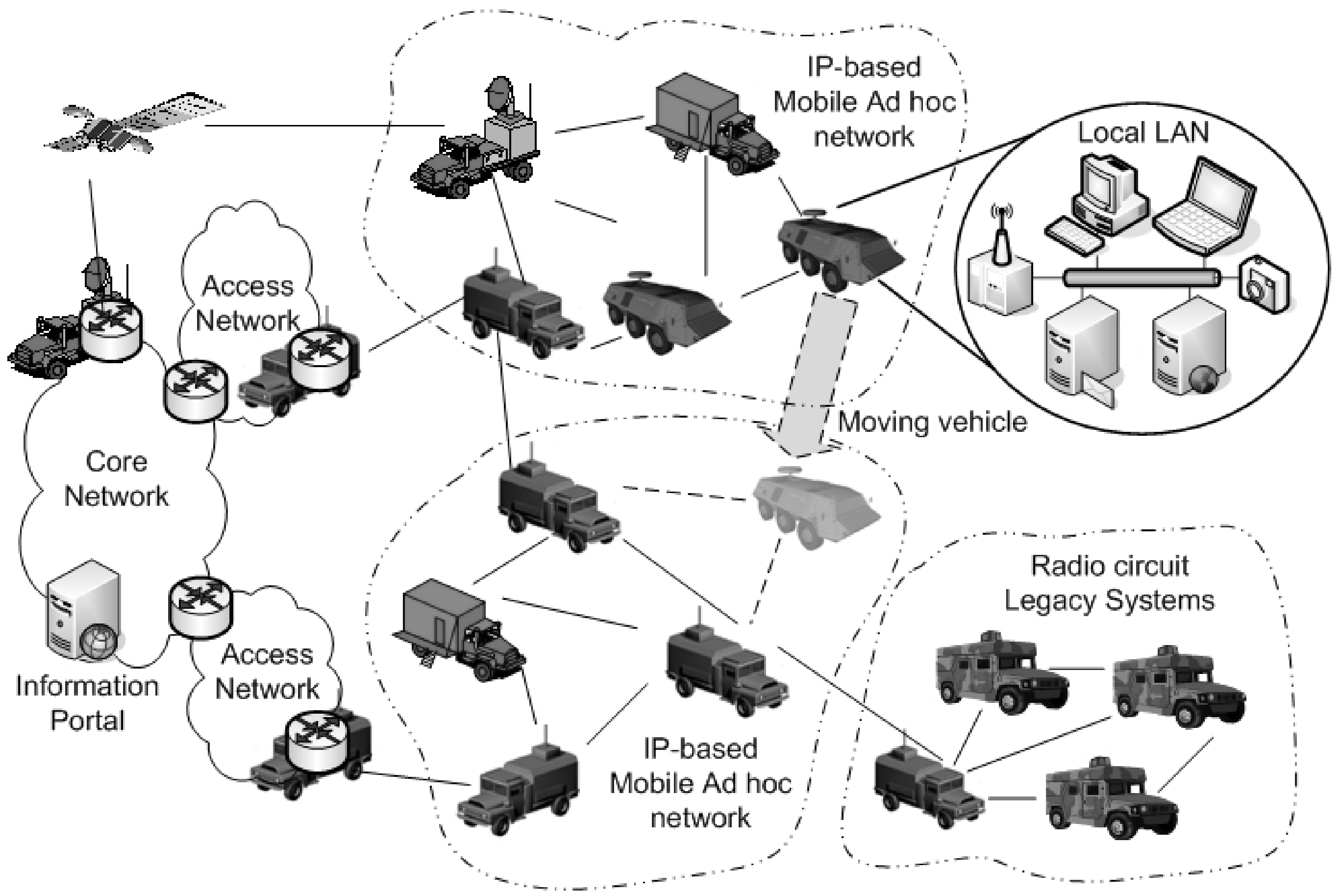

Figure 1. Exemplary scenario with three MANETs (dashed outline) consisting of mobile nodes and their connected secure networks, e.g. command posts, vehicular LANs, etc. Mobile nodes should be able to change their MANET-association while data between the secure domains will be routed transparently.

in the second part of this section. The mechanism we present in this paper, however, is not limited to this kind of scenario. It is flexible enough to be applied to a larger class of similar scenarios, where mobile forces need to communicate without a fixed infrastructure.

A. Description

Figure 1 depicts a typical tactical scenario: A number of vehicles is deployed in an area. In order to communicate with each other, all are equipped with radio units. A number of these units which operate on the same set of radio parameters (e.g. frequency, hopping patterns, etc.) comprise one domain (this can be a radio circuit in legacy radio links or a MANET, if an IP-capable link is used). In this figure two MANETs and a third domain which uses conventional, not IP-aware legacy radio technology, consisting of some vehicles each, are depicted.

Each of the shown MANET nodes is in fact a router; It can forward data of locally attached devices, e.g., laptops, servers, or sensors in or attached to the vehicle, as well as forward traffic of other nodes.

In contrast to the nodes of the MANET which are highly mobile and might change their absolute and relative position continuously, the nodes and links of the core and access networks are rather static. The nodes of the MANETs run a proactive or reactive MANET routing protocol like OLSR [1] or AODV [2] which is capable of coping with the frequently changing network topology. The access and core networks run a typical interior or exterior routing protocol like OSPF [3], [4], IS-IS [5], [6] or BGP [7].

When moving it is likely that at one point in time a node leaves the domain of its MANET, i.e. it cannot connect to any other node of its MANET for an extended period of time. However, it could be the case that the node comes in range of another MANET's node, in this case the first node should acquire access to the other network. Discovering and readdressing mechanisms in place ensure that the node automatically becomes member of the new network.

Data in need of protection, e.g. from the vehicular local network, are termed *red* data, systems working with *red* data (like the ones in the vehicle or the core network) are called *red* systems. IPsec tunnels are a certified solution to be used between nodes to ensure this protection, resulting in a *black* overlay network. The term *black*, in opposite of *red*, denotes data and systems which do not need to be protected against eavesdropping, either because the information is public anyway or because the data have already been encrypted. The *black* transport overlay network covers in this scenario exactly the MANET.

B. Requirements

From the scenario above a list of requirements can be derived. The first requirement is obvious when looking at the case of a user sitting at his laptop requesting information from an information server outside his network. The request arriving on the *red* side of the vehicle's radio has to be encrypted and needs to be routed over the air to the access and core networks. Therefore the radio must be able to determine the most appropriate node in the MANET to which a tunnel should be established. In order to avoid delays due to additional decrypting and encrypting, a termination of the tunnel at each hop within the MANET must not happen.

As the tunnel itself—in contrast to the tunnelled data—belongs to the *black* overlay network, the tunnel end points where decapsulation of encrypted traffic takes place must be denoted in terms of *black* overlay IP addresses. The mapping of nodes to *black* IP addresses must not be static: If the vehicle roams to another MANET, readdressing will happen and the (*black*) MANET IP address changes while the IP addresses of the *red* systems within a vehicle will stay the same. Therefore the nodes in the MANET must be able to map dynamically *red* network addresses, like the addresses of the access or core network or the addresses of the LAN in the vehicle, to the *black* IP address of a potential tunnel end point. This mapping must be consistent even if nodes leave or join a MANET and therefore get new IP addresses.

From the perspective of information assurance it is crucial that no information about the *red* network (even its existence) is allowed to leak into the unsecured domain. This usually requires end-to-end encryption, integrity assurance as well as authentication of control messages. These requirements are also true for external management components which might influence the system's behaviour and the communication with those management components.

In addition, the limited bandwidth in wireless networks (especially in military ones) requires efficient communication (i.e. minimal overhead). This should be taken into account when choosing a communication protocol and designing the processes within the system.

Furthermore, the system should require only the least possible amount of additional functionality from the connected *red* networks. However, if a node roams to another MANET, and thus its attached *red* LAN is now reachable over a different route, this change must be propagated in the *red* network.

In the scenario above a radio circuit of legacy systems is depicted. Such radio circuits do not offer native IP communication between the nodes and likewise do not build MANETs. The nodes in legacy radio circuits do not have IP addresses, however, it is assumed they can transport digital data and can be addressed by an identifier. The mapping needs to be able to work with such identifiers, too, thus being able to connect transparently *red* IP networks over *black* legacy networks. Examples of legacy radio systems in the military domain are, e.g. SATURN [8], HAVE QUICK [9] or SINCGARS [10].

III. Related work

Providing secure communication links over wireless channels has been investigated in a number of ways. Kannhavong *et al.* [11] did a survey on routing attacks in MANETs and provided some mitigation strategies while Ganzinger *et al.* [12] focused on securing an existing MANET routing protocol (OLSR [1]). The drawback of such a solution is that the dynamics of a mobile network are exposed to the connecting infrastructure which is undesirable from an information security point of view due to the information leakage.

Embodying IPsec tunnelling mechanisms brings with it the complexity of providing mappings between attached networks and tunnel end point addresses. Burbank *et al.* [13] analyse military wireless networks and describe pitfalls encountered in *ad hoc* network scenarios. Also, different transport networks—especially legacy radio links—are of interest; Wang *et al.* [14] have already described a MANET implementation over legacy radio links. Route discovery mechanisms for IPsec have been developed, e.g. by Tran [15] (a proactive approach with route dissemination over a special IPsec-secured multicast address) or Gruber *et al.* [16] (a static table provides information about attached networks and at most one default gateway), but these approaches can be categorised as a rather heavy-handed solution with especially quite limited support for node mobility.

Earlier work focusing on providing some secure routing aspects over wireless links has been done in a patent application by Gruber *et al.* [16] and in the development of the *High Assurance Internet Protocol Encryptor* (HAIPE, formerly known as HAIPIS, c.f. Mirhakkak *et al.* [17]), but the currently static approach to the mapping problem allows neither for the required node mobility nor for the possibility for general routing between networks attached to wireless nodes.

For an overview over the aspect of available capacity in wireless network, a treatise by Garetto *et al.* [18] has quantified this information and Levchenko *et al.* [19] recently provided a more efficient approach to routing protocols.

An elegant approach to the aforementioned problems is the concept of a distributed network element based on the separation of forwarding and control elements as described in RFC 3746 [20] (*Forwarding and Control Element Separation*, ForCES). This concept has not yet been applied to security in general and VPNs in particualar before. Hagsand *et al.* [21] and Zhuge *et al.* [22] describe the design and implementation of a distributed wired-network-based router, but they assume an available trusted transport link and attached networks with identical security levels between the entities comprising the distributed network element. The *virtual routers on the move* (VROOM) [23] approach tackles a similar problem, but concentrates on router functionality migration while we deal with physical router movement.

None of the aforementioned systems can efficiently solve the problem of determining the appropriate tunnel end points as required above. Under certain assumptions the approaches of

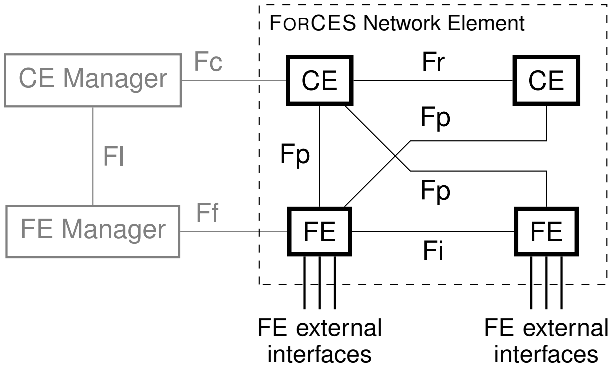

Figure 2. Schematics of the FORCES architecture consisting of control elements (CE), forwarding elements (FE) and communication reference points; ancillary managing components are not part of the architecture proper

Gruber *et al.* or HAIPE might work, but they lack the necessary flexibility. We propose an integrated but distributed architecture, based on the separation of forwarding and control elements, to enable not only routing and connectivity as such over an insecure wireless transport network, but also to provide the necessary flexibility.

IV. THE FORCES ARCHITECTURE

The foundations of this architecture have been developed by an IETF working group (*Forwarding and Control Element Separation (forces)*) as an answer to the problem of router scalability caused by the traditionally rather tight coupling of control and forwarding functions. The approach taken describes a virtual network element which consists of two types of building blocks: *forwarding elements* (FE) which encapsulate physical network interfaces and are tasked with data forwarding. They are configured and managed by *control elements* (CE). These CEs manage their assigned FEs and implement the necessary higher level protocol functionality (e.g. routing protocols) of the distributed element's outward facade.

Figure 2 shows schematically the elements and their communication reference points. Ancillary elements—the CE *and* FE *managers* which play an active role in assigning FEs to CEs and general internal management tasks—are described but not part of the architecture proper. While every addressable entity (AE)—CEs, FEs and the managing entities—must communicate via the given reference points (*Fp*, *Fi*, *Fr*, etc.) and therefore has some kind of network connectivity present, the external interfaces alone provide communication capability with the attached networks.

The abstract concepts are specified in RFC 3654 [24] (requirements) and RFC 3746 [20] (architecture). Dong *et al.* have submitted a draft document [25] elaborating the FORCES protocol between control and forwarding elements over the reference point *Fp*.

Additional reference points are *Fr* over which the inter-CE communication takes place and *Fi* which is the *fast path* for forwarding data between the interfaces. Protocols for these reference points are deliberately implementation specific to enable efficient solutions depending on what kind of distributed network element (switch, router, etc.) is to be constructed.

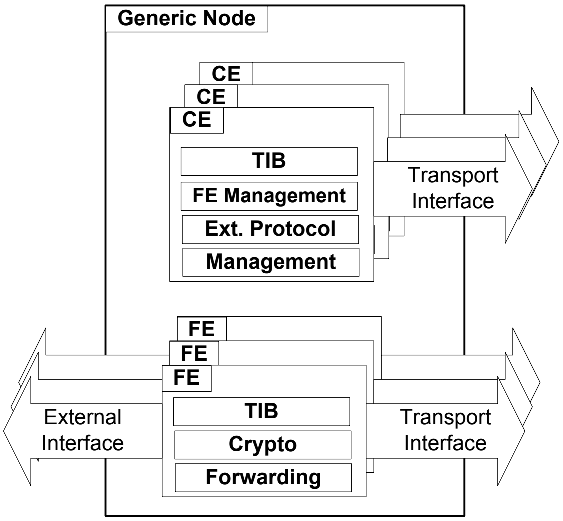

Figure 3. Generic node with n CEs and m FEs; while the protocol and management logic resides in the CE, the FE concerns itself only with basic topology information and the forwarding of data. The transport interface module provides connection to the data links used for the *Fp*, *Fi* or *Fr* communication.

In general the concept suggests a fast and high-bandwidth communication link for the *Fi* data transfer while the *Fp* and *Fr* links can feature substantially smaller bandwidth; this is possible because most data can be forwarded by direct destination look-up inside the FE (the *fast path*) while only a smaller fraction of the incoming data is either addressed to the virtual network element itself or unknown to the FE and has to be processed specifically by the CEs (the *slow path*).

Hiding specifics of the underlying transport links (the links within the distributed router) behind a consistent facade is anadvantage of the above shown design principle. We will use especially this benefit within the paper to handle the security and mobility requirements.

V. GENERIC DESIGN

The generic FORCES architecture as described in the previous section provides a rather high-level abstraction. We use the basic principle of FORCES—the separation of networking functions—to design a system which is able to provide a dynamic mapping between *red* IP addresses and transport network (*black*) identifiers.

Having our requirements for flexibility, mobility and security in mind, a separation approach offers the best potential for an efficient solution because the forwarding aspect is decoupled from the management and control aspect. This enables a separation of concerns: while the forwarding elements handle the encryption and forwarding of data, the control elements' task is to create a consistent facade of the distributed network element through management of external protocol information, dissemination of this information to other CEs and updating the forwarding element's information base.

In figure 4, as an example, a distributed network element providing layer three services, i.e. a distributed router, is depicted. It consists of four mobile nodes, each with an attached *red* network. As could be seen in the upper half of the figure, the distributed network element hides its internal organisation from external entities and represents a single entity to outside networks. Internally, however, it is composed of numerous separated entities that cooperate as a distributed application to provide the defined functionality. The internal structure is shown in the lower half of the figure: four mobile nodes connected via radio links (the *black* network).

A. Internal structure

Two types of major network element components exist: *control elements* (CE) in the control plane and *forwarding elements* (FE) in forwarding plane. Figure 3 depicts a generic node with CEs and FEs.

A CE controls FEs how to process packets, i.e. it updates the FE's forwarding information base with entries for known destination tunnel end points. It is up to the FE to establish crypto tunnels and forward the packet.

While it is assumed that most implementations will instantiate a number of identical CEs, it is perfectly reasonable to create CEs with differing functionality and join them with the distributed network element to enhance the capabilities of the whole distributed element.

Identical components on the CE and FE are the topology information base (TIB) and communication links to the transport networks. It is possible to operate separate transport networks inside a distributed network element, e.g. separate channels for the communication between CEs and FEs (*Fp*) and between FEs while forwarding data (*Fi*).

Based on the information acquired through CEs' control processing respectively through external protocol participation—be it some kind of routing protocol or another network layer's protocol—CEs will frequently manipulate the packet forwarding behaviours of their FEs by sending instructions to them.

The topology information base (TIB) holds topology information about the element's internal structure as well as information concerning the external protocol support, e.g. routing paths for network or host destination addresses in the case of a distributed router or MAC addresses and interface identifiers if a distributed switch is to be realised.

Information from the TIB is used to construct secured communication links in the *black* transport network for the communication between a CE and the assigned FEs. The second and most important function of the TIB is to provide mappings for resolving *red* destination addresses to *black* transport net identifiers for the most suitable forwarding element.

Secure end-to-end links between FEs will be used for data forwarding. Forwarding table entries for these end-to-end links—tuples of *red* addresses and *black* identifiers, e.g. IP or MAC addresses—will be constructed by the CEs with information from the TIB and transferred to the FEs by the CE's FE management module.

To support management of the distributed router, every CE has to be able to process incoming management data; to achieve this task it communicates with sibling CEs via the *Fr* reference point.

To enable communication capabilities, a device has to be configured with data concerning group communication identifiers of the distributed network element, identifiers on the *red* and *black* interfaces and initial keying material (pre-shared keys, certificates, etc.) as well as a list of external (*red* side) protocols which have to be supported.

These data can be provided by auxiliary management systems—network management systems (NMS) fulfil the CE/FE manager (CEM/FEM) role—once an initial bootstrapping configuration set has been provided during the roll-out process.

B. Generic behaviour

1) Pre-association phase: In the pre-association phase all addressable elements—CEs and FEs—discover their topology via group communication and set up basic element-to-element communication security; to enable this, a preliminary secure communication channel has to be configured already.

The pre-association phase is entered by an element (CE or FE) every time it has to (re-)acquire its distributed network element association, e.g. after powering the device or leaving and reentering a transport network domain, for example a MANET. Other elements in the distributed router react to the joining element's messages without disruption of their current operations.

2) Topology synchronisation: The most important function is the routing and topology information base synchronisation. This task can be handled for example by an announcement mechanism or via an explicit synchronisation step. If an announcement scheme is used, the basic event sequence consists of *new route* announcement messages from a CE to all other CEs which add those messages' information into their local TIB and update their managed FEs.

The explicit synchronization is necessary as the external protocols (like OSPF) do not run inside the distributed network element. For these external protocols the distributed network element, consisting of several internal nodes, is only one element, which has to ensure, however, that the topology information received or distributed is consistent over all interfaces (i.e. nodes).

In case an entity joins a distributed network element, a *route request* message can be used to receive up-to-date topology and routing information from all other CEs at once.

3) Dead element detection: In order to detect elements which are unreachable since a certain time (and possibly have left the distributed element without giving notice), one approach can be a heartbeat mechanism: In configurable intervals, every element multicasts a short packet announcing its presence to all other addressable entities. Further efficiency could be gained in single-hop networks by using a MAC layer beacon feature directly.

4) Disconnect from transport network: While disconnects can be handled via the dead element detection mechanism, it is prudent to offer nodes which wish to leave a distributed network element a procedure to disconnect in a clean fashion.

VI. Prototypical implementation of a distributed router for MANETs

As a proof of concept we implemented the architectural design developed in Section V for the case of an IPv6-based transport network. This means the wireless network is a MANET and the virtual distributed network element becomes a distributed router. The routing protocol we used in the attached *red* network was OSPF. For the implementation we have chosen exactly one CE and one FE for one mobile node. This simplifies the implementation as the assignment of FEs to CEs is inherently given. The communication between CE and FE (reference point *Fp*) can now be realised completely inside the device, thus no protocol for this communication needs to be implemented. Furthermore the CE does not need an own transport stack and crypto mechanisms. It can rely on the services of its FE.

A. Implementation of the modules

We use for the implementation of the mobile node a Linux based PC. This offers the advantage of very good support of different networking protocols as well as a huge basis of open source software and tools. Figure 5 shows the simplified implementation architecture.

The Linux kernel offers already all functionality necessary for an FE. It has support for several network interfaces (here one is used as interface for the *red* network, another one for the connection to the transport network). The kernel implements IPv6 and if configured accordingly, it can forward packets between these interfaces based on a routing table.

Part of the IPv6 stack is IPsec. Daemons running in user space implement the *internet key exchange* (IKE) protocol [26] or a multicast-capable IKE improvement (referred to as MIKE [15], [27]), two protocols necessary to establish IPsec security associations (SAs) dynamically between two or a group of nodes. Even if one could argument that establishing SAs should be part of the CE, in our prototypical implementation we leave this functionality with the FE.

We implemented the CE as an user space process. An open source implementation of the OSPF routing daemon was used as the basis for the external protocol support module. It was modified in such a way, that routing updates are not written to the routing table of the kernel but to the *topology information base* (TIB), in addition with the IP address of the *black* interface.

The information in the TIB is updated not only by the OSPF daemon implemented in the local node but also by the information of all other OSPF daemons of the distributed router. The information they write to their TIB is synchronised with all other TIBs, thus each OSPF daemon of all nodes of the distributed router announces the networks of all other nodes. Because of this, the distributed router appears to all attached networks as one entity. The internal transport network is thus transparent to the outside. The TIB synchroniser implements a standard replication mechanism to keep all TIBs consistent. Synchronisation is triggered by the TIB whenever an update happened.

The function of updating the kernel's routing table is instead performed by the FE manager. It updates the routing table and the *Security Policy Database* (SPD) of the kernel. Because each node writes its routes (i.e., the networks it could reach via its *red* interface) together with its black IP address in its TIB, the FE manager can create routes and SPD entries, which map *red* IP addresses to *black* IP addresses.

A task of the *Internal Topology Generator* is removing stale node entries from the TIB. A node is declared dead and all entries in the TIB are removed if for a certain period of time no heartbeat message was received. Removing the entries from the TIB removes them also from the routing table and the SPD of the kernel. Sending heartbeat messages is also a task of this module. The heartbeat is sent periodically using IPv6 multicast.

B. Operational workflows

As generically described in the previous section, the communication between the CEs is structured in phases. Because of the simplifications of the prototypical implementation only three phases need to be implemented.

1) Pre-association phase: When a CE lost communication to its MANET and later on wants to join a distributed router again, it starts its communication in pre-association phase. Therefore a **HELLO** message is sent to the multicast address which is the same for each MANET and reaches all nodes of the distributed router. CEs receiving a **HELLO** message append the sender to their list of nodes and send their TIB to the new node. Because of the simplifications in this prototypical implementation the pre-association phase consists only of this **HELLO** message.

Please note, all router internal communication between the CEs is performed via the *black* network stack of the FEs. Thus all communication of the CEs is encrypted. This means by sending the **HELLO** message, the FE's MIKE daemon starts negotiating the relevant multicast SA.

2) Route announcement: Whenever the TIB is changed it triggers the TIB synchroniser which announces this change in form of a **UPDATE** message to all other CEs. The TIB synchroniser uses the same multicast address as it is used for the **HELLO** messages. A binary message format is used for the **UPDATE** message in order to minimise the message size. Whenever the local TIB is changed because of an **UPDATE** message, the FE manager is triggered in order to update the local routing table and SPD if necessary.

3) Disconnect from transport network: While disconnects can be handled via the heartbeat mechanism, it is prudent to offer nodes which wish to leave a distributed network element a procedure to disconnect in a clean fashion. A node might want to disconnect if another MANET which comes into range offers a better connection quality.

In this case the CE sends a **LEAVE** message to the multicast group. This declares the node immediately dead and the same procedure starts as described above.

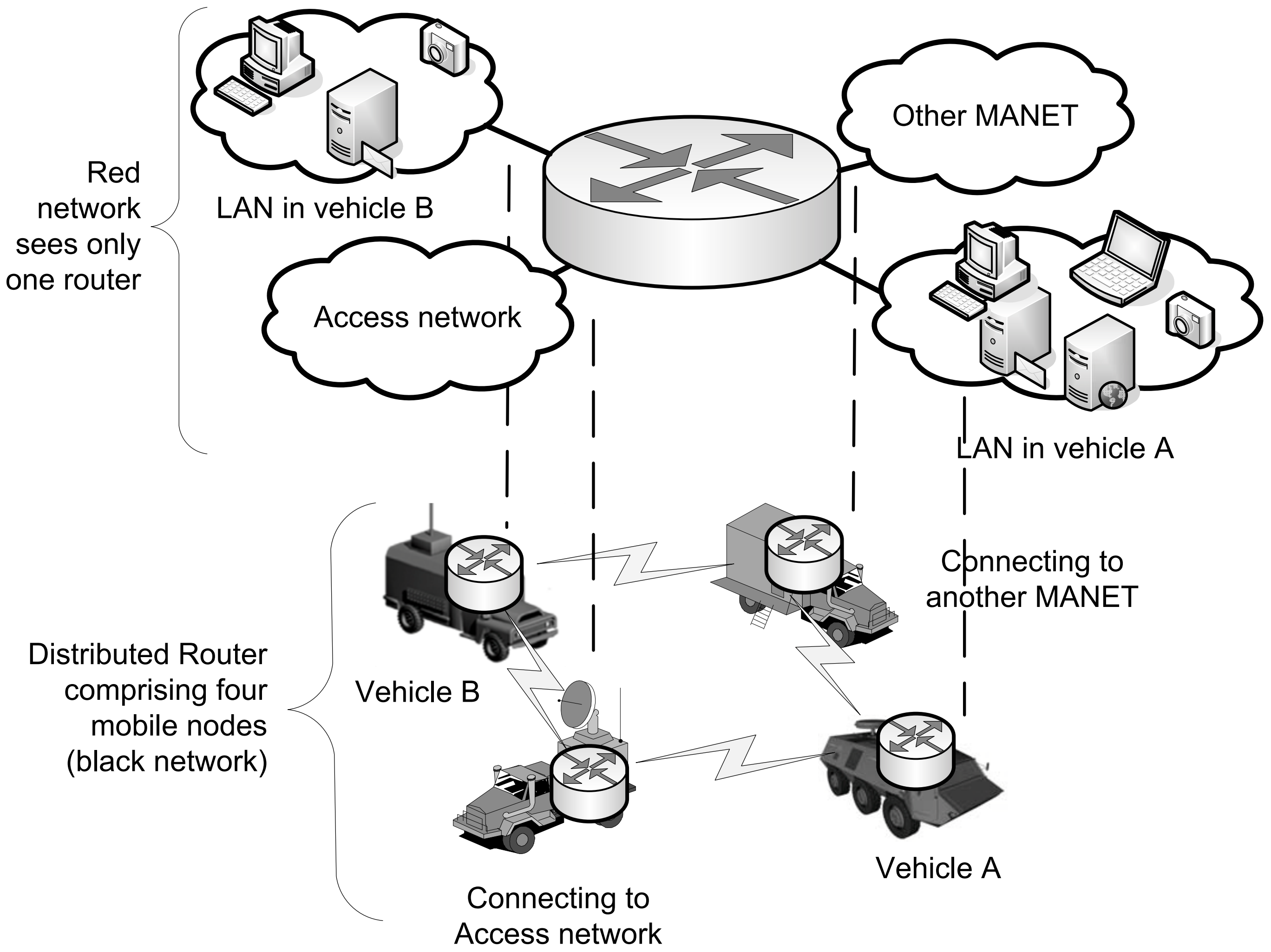
Red network sees only one router
LAN in vehicle B
Other MANET
Access network
LAN in vehicle A
Connecting to another MANET
Distributed Router comprising four mobile nodes (black network)
Vehicle B
Vehicle A
Connecting to Access network

Figure 4. Two-layer view of a distributed network element (here as an example a distributed router). The underlying transport network details, i.e. the radio links (lower half of the figure), are hidden by a logical router facade from the point of view of the *red* network (upper half of the figure).

VII. Evaluation

In this section we evaluate our solution in two ways: first we compare the system to the requirements and check which ones could be fulfilled and which not. Second we present first results from evaluating the system in a testbed.

A. Fulfilment of the requirements

In section II-B requirements for a system which can dynamically map *red* IP addresses to *black* identifiers have been developed. The first requirement described exactly this functionality which is fully supported by the distributed router approach shown within the paper. The CE combines the knowledge about the external network topology and the internal topology. It knows therefore which *red* networks are connected to each node of the MANET and can always calculate the most appropriate tunnel end point for a given destination IP address. External routing support and internal topology generator update the information about the internal and external network topology periodically, thus providing an up-to-date view of the network and mapping the *red* IP addresses dynamically to the *black* identifiers, which has been another requirement.

All communication between CEs, between CEs and FEs, and between FEs is protected using the same encryption mechanisms as in place for the payload data. In the general case an CE indeed implements those crypto mechanisms itself. If coupled with an FE as shown in section VI, the CE uses the crypto implementation of the FE. In this case the communication between CE and FE does not need to be protected, as it is device-internal.

Management components external to the distributed router have not been defined in this paper. This is a functionality we will tackle in future work. Thus no security mechanisms have been defined and the requirement for a management system is not fulfilled in the current stage of work. However, interfaces to these management components have been identified in section IV.

The distributed router uses internally a binary protocol

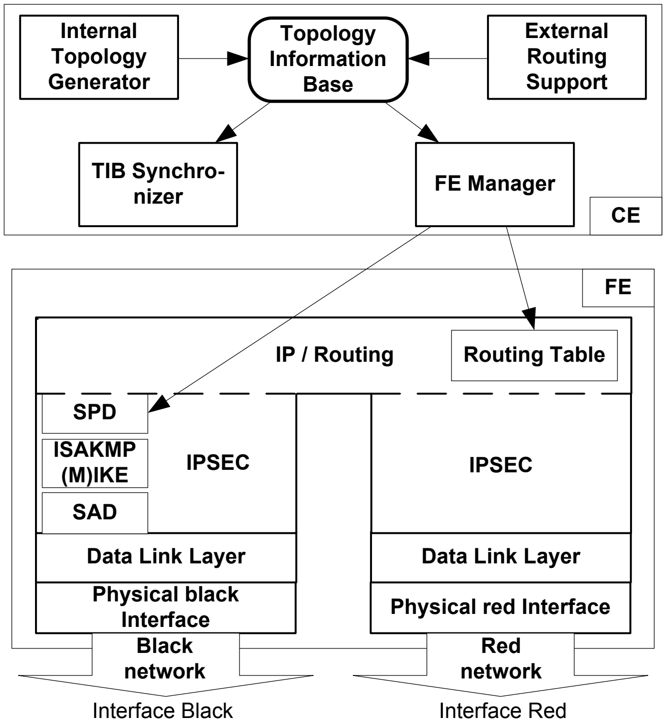

Figure 5. Block diagram of a basic node of a distributed router implementation with an IP MANET as interior transport network. A single node consists of one CE and one FE with two network interfaces.

in order to minimise the size of the messages. This allows encoding data much more compact than with plain text protocols (e.g. HTTP). Messages containing information which are of interest for all nodes are sent as multicast messages, thus requiring sending the information only once. Messages which are of interest for only one node are sent as unicast.

The distributed router puts almost no requirements on the *red* network. It is only required that the network runs a routing protocol which is most probably true for every bigger network. The routing protocol is essential in order for the CE discovering the attached *red* networks and to propagate route changes if nodes have roamed to another MANET. Even if our distributed router fully complies with the requirement it should be noted that the CE needs to be adapted to the used routing protocol.

The distributed router encapsulates completely the structure of the wireless network. Internally the distributed router only works with identifiers for nodes. These identifiers could be IP addresses, however, they could also be identifiers of a legacy system. The only assumption made is that given the identifier, the FE could transport data to the denoted node.

B. Testbed results

As a proof of concept for the approach of using a distributed router for mapping *red* IP addresses to *black* identifiers a first prototypical implementation has been evaluated in a testbed. The testbed consists of 16 clients running the Linux operating system. Each of the clients emulates a MANET node and the attached *red* network, i.e. the *red* networks and its devices exist only virtually. All nodes have a wired Ethernet connection to a central server. The central server runs the network simulator `ns-2` [28] in emulation mode, emulating wireless characteristics for the communication between the nodes. Nodes can only communicate via the central server's ns-2 channel emulation with each other, however, from the point of view of each node, the central server is transparent.

As already mentioned above the components of the *red* network exist only virtually. We use XEN [29] as a virtualisation technique. The network interface of the clients is used as the *black* interface of the node. A bridge was configured in the kernel which connects all (virtual) *red* interfaces.

Traffic in the network is generated by HTTP downloads. Web servers have been installed on four of the 16 clients. The remaining twelve clients periodically download HTML files of different sizes. Two MANETs and simple movement patterns of nodes have been configured in the central server. Even if the traffic profiles and movement patterns are not yet very realistic the principle operability of the distributed router could be proofed.

Latency times and traffic overhead introduced by the distributed router are marginal, however, before quantitative statement could be made, traffic profiles and movement patterns need to be refined. We must also notice that the choice of the MANET protocol has a huge impact on the convergence rate of the distributed router's information. Further work is necessary to analyse these reasons and possible reduce this impact.

VIII. Conclusion

This paper proposes a generic approach to solve the problem of determining the address in the *black* network to which a VPN tunnel has to be established, given the final destination address in the *red* network in highly dynamic, mobile radio networks. This *red-black* mapping can not be static as nodes, and therewith their attached networks, might roam to another *black* network and get a new *black* address.

Requirements are specified based on a presented scenario, which clarifies the problem area. Our evaluation has shown that current approaches do not meet all requirements, first, and foremost the postulated high level of dynamics within the black networks.

By using the basic principle of the ForCES concept we have designed an architecture which fulfils the identified requirements. Within first implementation steps focusing on IP-based MANETs, promising results have been gathered. We continue to enhance the existing work with regard to the implementation of legacy non-IP networks. At this stage, the addressing of management issues is limited to the initial configuration of nodes within a basic configuration.

In our next steps we will focus on the design of an external management system which supports the required network dynamics and guarantees the integrity of the virtual node itself. As this virtual node is scattered over the elements of a radio network, performance analysis will be an ongoing task based on further evaluation results. Due to enhancing the evaluation process, traffic profiles deduced from more realistic scenarios will be used. We will focus especially on an optimal parametrisation of our approach concerning various MANET protocols in subsequent work.

References

[1] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626 (Experimental), Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), Jul. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[3] J. Moy, "OSPF Version 2," RFC 2328 (Standard), Apr. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2328.txt

[4] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," RFC 5340 (Proposed Standard), Jul. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5340.txt

[5] *Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service*, ISO/IEC Std. 10 589, Nov. 2002.

[6] D. Oran, "OSI IS-IS Intra-domain Routing Protocol," RFC 1142 (Informational), Feb. 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1142.txt

[7] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271 (Draft Standard), Jan. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4271.txt

[8] J. F. Keating and T. M. Schuerman, Eds., *SATURN: The next generation radio for NATO*, Feb. 1991.

[9] *HAVE QUICK I/II*, NATO Std. STANAG 4246.

[10] *Multiservice Communications Procedures for the Single-channel Ground and Airborne Radio System (SINCGARS)*, May 1996.

[11] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Commun. Mag.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[12] M. Ganzinger, W. J. Hymas, and T. Schütt, "Securing broadcast based ad hoc routing protocols," in *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE Computer Society, 2007, pp. 137–144.

[13] J. L. Burbank, P. F. Chimento, B. K. Haberman, and W. T. Kasch, "Key challenges of military tactical networking and the elusive promise of MANET technology," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 39–45, Nov. 2006.

[14] H. Wang, B. Crilly, W. Zhao, C. Autry, and S. Swank, "Implementing mobile ad hoc networking (MANET) over legacy tactical radio links," *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pp. 1–7, Oct. 2007.

[15] T. H. Tran, "Proactive multicast-based IPSEC discovery protocol and multicast extension," in *Proceedings of the MILCOM 2006*, 2006.

[16] I. Gruber, T. Langguth, and H. Schober, "Method and system for adressing and routing in encrypted communication links," German patent application 10 2006 043 156.1, Sep. 14, 2006. [Online]. Available: http://www.wipo.int/pctdb/en/wo.jsp?WO=2008031515

[17] M. Mirhakkak, P. Ta, G. Comparetto, and V. Fineberg, "Modeling and simulation of HAIPE," in *Military Communications Conference, 2006. MILCOM 2006*, Oct. 2006.

[18] M. Garetto, P. Giaccone, and E. Leonardi, "On the capacity of ad hoc wireless networks under general node mobility," in *INFOCOM*. IEEE, 2007, pp. 357–365.

[19] K. Levchenko, G. M. Voelker, R. Paturi, and S. Savage, "Xl: an efficient network routing algorithm," in *SIGCOMM '08: Proceedings of the ACM SIGCOMM 2008 conference on Data communication*. New York, NY, USA: ACM, 2008, pp. 15–26.

[20] L. Yang, R. Dantu, T. Anderson, and R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework," RFC 3746 (Informational), Apr. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3746.txt

[21] O. Hagsand, M. Hidell, and P. Sjödin, "Design and implementation of a distributed router," *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology*, pp. 227–232, Dec. 2005.

[22] B. Zhuge, L. Dong, and W. Wang, "A distributed routing algorithm based on architecture of ForCES," in *ICN*. IEEE Computer Society, 2008, pp. 651–655.

[23] Y. Wang, E. Keller, B. Biskeborn, J. E. van der Merwe, and J. Rexford, "Virtual routers on the move: live router migration as a network-management primitive," in *SIGCOMM*, V. Bahl, D. Wetherall, S. Savage, and I. Stoica, Eds. ACM, 2008, pp. 231–242.

[24] H. Khosravi and T. Anderson, "Requirements for Separation of IP Control and Forwarding," RFC 3654 (Informational), Nov. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3654.txt

[25] "ForCES protocol specification," Internet Draft (expires February 26, 2009), Aug. 2008. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-forces-protocol-15.txt

[26] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," RFC 4306 (Proposed Standard), Dec. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4306.txt

[27] M. Song and Z. Li, "One improved IPSec protocol supporting multicast communication," in *Second International Conference on Digital Telecommunications*, 2007.

[28] S. McCanne and S. Floyd, "ns–network simulator."

[29] P. Barham, B. Dragovic, K. Fraser, S. H, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," 2003.