An Integrated Wireless Communication Architecture for Maritime Sector

Liping Mu, Ram Kumar, and Andreas Prinz

Faculty of Engineering and Science, University of Agder
Jon Lilletuns vei 9, 4879 Grimstad, Norway
{liping.mu,ram.kumar,andreas.prinz}@uia.no

Abstract. The rapid evolution of terrestrial wireless systems has brought mobile users more and more desired communication services. Maritime customers are asking for the same, such as the concepts of "Broadband at Sea" and "Maritime Internet". Quite a lot of research work has focused on the development of new and better maritime communication technologies, but less attention has been paid on interworking of multiple maritime wireless networks or on satisfying service provisioning. To address this, an integrated wireless Communication Architecture for Maritime Sector (CAMS) has been introduced in this article. CAMS is aimed at 1) granting maritime customers uninterrupted connectivity through the best available network and 2) providing them with the best-provisioned communication services in terms of mobility, security and Quality of Experience (QoE). To address mobility challenge, the IEEE 802.21 standard is recommended to be used in CAMS in order to achieve seamless handover. CAMS provides application-level QoE support attending to the limited communication resources (e.g. bandwidth) at sea. Certain security considerations have also been proposed to supplement this architecture.

Keywords: Communication Architecture, Network Integration, Maritime.

1 Introduction

Due to the development of new applications and the fast evolution of wireless communication technologies, maritime customers are demanding better communication solutions to satisfy the increasing user requirements. In this context, concepts like "Broadband at Sea" and "Maritime Internet" have become popular [1].

Newer security and transport related applications such as video surveillance for piracy prevention and real-time updates of navigational data are increasingly being used. Besides, the usage of personal and business purpose applications like telephony and email are also considered while implementing communication systems for ship's management.

Some of these newly envisaged applications demand a strict network Quality of Service (QoS) such as guaranteed bandwidth and lower delays, and some require uninterrupted Internet connectivity. On the other hand, the fast evolution

C. Sacchi et al. (Eds.): MACOM 2011, LNCS 6886, pp. 193–205, 2011.

of wireless communication technologies provides maritime customers opportunity to achieve better and faster ship-to-ship and ship-to-shore communications. For example, maritime mesh networks based on long range wireless technology (WiMAX) [2] is a promising solution, and satellite broadband such as VSAT (Very Small Aperture Terminals) service is changing maritime communications dramatically. At the same time, last-mile wireless access technologies, such as IEEE 802.11, IEEE 802.16, 3GPP standards for cellular access networks, keep contributing to the near-shore communications. In order to efficiently use these wireless communication systems and take advantage of the various available features, procedures to integrate these networks and to automatically select the best underlying network are desired. To satisfy the different maritime communication requirements, network resources have to be utilized reasonably and communication services have to be provisioned and tailored to user requirements. Furthermore, mobility handling mechanisms are necessary so as to achieve a seamless mobility experience when switching between different underlying networks.

In this article, an integrated wireless Communication Architecture for Maritime Sector (CAMS) is introduced to address both application requirements and rapid technology evolution. CAMS is aimed at satisfying always-best-connected requirement and better services-provisioning in terms of mobility, security and QoE.

The rest of the article is organized as follows. In Section 2, maritime customer communication requirements are identified. Section 3 extracts the key system requirements for maritime communication. Then, in Section 4, the integrated maritime communication architecture is presented. Finally, Section 5 concludes this paper and points out future work.

2 Maritime Customer Communication Requirements

Maritime communication is becoming more important in both commercial and research fields, especially in countries like Norway, which has economic dependency on an ocean area about six times the size of its mainland. After having contacted many maritime customers [1], we have acquired a detailed list of user requirements for maritime communication as given below.

2.1 Make Use of Available Bandwidths as Much as Possible

Customers on ship are willing to keep in touch with shore centers and to use Internet anytime, anywhere on any device, and they prefer to have the possibility of being best connected to the available network in terms of bandwidth, quality and cost. For example, when the ship is moving to an area covered by terrestrial communication networks, services provided by these systems are mostly desirable.

2.2 Classify Data Traffic to Optimize the Usage of Bandwidth

Bandwidth is a limited resource especially in the maritime scenario that drastically changes with geography. For example, in harbors WiFi is available to

support high bandwidth with very low price, whereas far out into the sea (far northern area for Norway), only satellites can provide low bandwidth connectivity characterized with high cost and long propagation delays. Therefore, maritime communication resources have to be utilized reasonably and intelligently by classifying and prioritizing the communication traffic.

2.3 Service Continuity at Different Locations and via Different Devices

Continuous land-based assistance and navigation are always in high demand. Service continuity becomes an important topic especially during the switching between different maritime wireless networks. For instance, a customer on-board who fills out an important on-line report to the shore center while the ship moves from communicating via satellite to WiMAX in a port, would want to keep the session uninterrupted during the transition.

2.4 More Secured Information Exchange and Internet Connectivity

It has become a security problem for shipping companies that the crew, while surfing the Internet and often unintentionally, exposes the on-board systems to viruses and hacking attacks. Security is a critical factor in the "Maritime Internet" context. Authentication and authorization mechanisms are needed for preventing attacks to the system. Also, traffic control to some extent is necessary for preventing less important data traffic from clogging the channels so as to enable the critical data to get through.

3 System Requirements for Maritime Communication

If we translate these maritime user communication requirements into system requirements, the target communication system is expected to have the following capabilities: provide optimum connectivity, mobility handling, QoE support and security.

3.1 Connectivity

With respect to maritime communications, almost all of them are based on wireless communication technologies. Compared to terrestrial wireless communication, it is challenging to deploy cellular systems at sea to achieve high data-rate transmission because of the geographic restrictions. So far, Frequency Modulation (FM) radio technology like narrowband Ultra High Frequency (UHF) and Very High Frequency (VHF) are widely used for ship-to-shore communication, with cellular systems used for near port waters. Satellites such as International Maritime Satellite (INMARSAT) are often used for long-range ship-to-ship and ship-to-shore communications. However, due to the fact that FM radio transmission has a low data-rate characteristic and satellite communication is quite

expensive, considerable effort has been devoted to the development of new maritime wireless communication technologies and cheaper satellite services. Maritime mobile WiMAX networks have drawn much attention [2]. Furthermore, advances in antenna technology and satellite coverage have combined to make VSAT Ku Band satellite services very attractive, as they can provide higher data-rate transmission, good Quality of Service, compatibility with IP networks and flat-rate charging.

All in all, the target maritime communication system needs to use these existing or future maritime wireless networks to provide customers basic connectivity services.

3.2 Mobility

There are four types of mobility defined in [3] mainly from the user's point of view: *terminal*, *personal*, *session* and *service mobility*. In [4], four levels of network interworking for mobility handling are distinguished from an operator's perspective:

- *Level A would allow a user to get access to a set of services available in a visited network while relying on his/her home network credentials;*
- *Level B would allow users to be able to get access to specific services located in their home network when connected through a visited network;*
- *Level C does not require users to re-establish active session(s) when moving between networks;*
- *Level D provides seamless service continuity to satisfy service requirements also during mobility.*

An intrinsic characteristic in maritime wireless communication scenarios is heterogeneity, which refers to the coexistence of multiple and diverse wireless networks with their corresponding radio access technologies [4] and network protocols. Therefore, integrating heterogeneous wireless networks in the maritime communication scenario is required in order to take advantage of the different features of each one of them, and all four levels of interworking are desired in the target maritime communication system for mobility handling.

3.3 QoE

Bandwidth at sea is a very limited resource due to the geographical restrictions, which frequently exhibits great variations with the high mobility of maritime communication entities and the switching between different underlying wireless networks. The QoS for an application session is determined by a number of factors, such as the maximum bandwidth that can be allocated to it and the current state of the network. It mainly focuses on the network perspective and attempts to objectively measure the service delivered by the operator: bit rate, delay, jitter, bit error rate and so on. Whereas in the maritime communication scenario, customers have the possibility of choosing from multiple underlying

networks; applications on board often have different capacity, integrity and security requirements related to different traffic types (e.g. distress calls, alert messages transmission, remote navigation assisting, confidential business data transmission and multimedia entertainment applications). Therefore, subjective factors regarding quality of service should be also considered in the target communication system. ITU-T has defined the QoE concept as "*overall acceptability of an application or service, as perceived subjectively by the end-user*" [5]. By considering both QoS and QoE when delivering communication services to maritime customers, application context and user expectations will be fairly treated besides objective QoS provided by the network operator.

3.4 Security

End-to-end security for ship-to-shore communication is vital, as ship-to-shore communications are mainly related to remote operation, navigation and safe shipping in which the integrity of exchanged information is vital. Additionally, business information traveling among maritime partners has to be kept as confidential; individual information for crew use is often sensitive. These confidential or sensitive information cannot be exposed or subjected to malicious intent. Hence, security mechanisms are highly desirable in the target maritime communication system.

4 An Integrated Wireless Communication Architecture for Maritime Sector

Existing maritime wireless networks are often independent systems without interworking between them. Maritime communication service provisioning therefore has to be supported by means of specialized service platforms that could deal with quality, security and mobility simultaneously. In order to accomplish that, the first key step is to design an efficient maritime communication platform architecture.

The Internet architecture was designed to push the intelligence to the end systems with dumb networks to provide fast service provision, but it only works very well when the network qualities are stable. Telecom network architectures are designed to have complex networks to benefit simple terminals and relevantly guaranteed service provisioning, but the services they satisfy are often simple and flat. Nevertheless, it is not difficult to identify the key technologies and marketing strategies within the Internet and Telecom network architectures that have made them so successful. For example, IP technology - a common interconnection element to address heterogeneity - in the Internet paradigm has brought incredible success and rapid growth. Similarly, the combination of mobility handling and QoS provisioning in the Telecom world has attracted ubiquitous users.

Although none of these two architectures apply directly to maritime scenarios, a tailored communication architecture - CAMS - that optimally leverages these two paradigms can best satisfy the maritime communication requirements

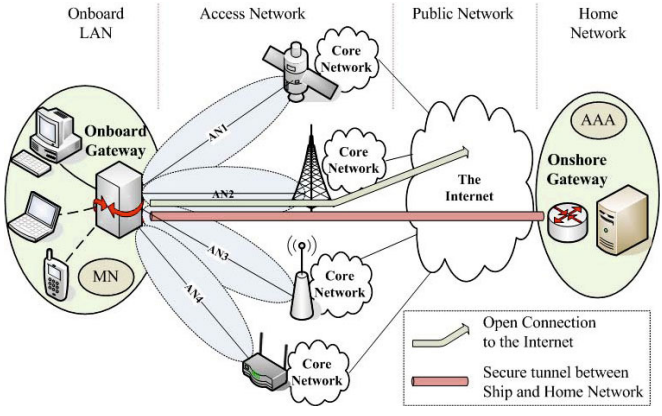

Fig. 1. An Integrated Communication Architecture for Maritime Sector

based on relevantly harsh conditions. The architecture is shown in Fig.1. In this architecture, IP is used as 1) the unifying technology to integrate different access networks 2) to follow the all-IP principle direction in communication evolution. The on-board gateway as a mobile node is equipped with multiple interfaces corresponding to different access technologies (e.g., AN1: satellite networks, AN2: WiMAX networks, AN3: cellular networks, AN4: WiFi networks). It cooperates with the onshore network which behaves like its home network in order to fulfill the mobility handling, QoE support and security enhancement tasks, which will be explained in detail in the following sections.

It is worth mentioning that the selection of this architecture model is not only based on performance criteria, but on its cost and feasibility as well. Any candidate architecture has to be able to backwardly integrate existing infrastructures while at the same time be easily evolved. Hence, two characteristics of our maritime communication architecture in terms of integration ability and scalability are central:

(1): In CAMS, the onshore network behaves like a home network for maritime customers. Therefore, separate subscriptions between customers and any network operator are not required. Customers have direct agreements with our home network, and our home network has separate service level agreements with each network operator.

(2): In CAMS, direct links between different networks are not necessary. Networks are connected with each other via the Internet, which is considered as loose-coupling architecture [6] for network integration. Compared with the tight-coupling model, it allows the independent deployment of each wireless network system.

4.1 Mobility Handling and Security Enhancement

Before finalizing any mobility handling solution, future trends for mobility handling must be considered. Given the mobility management tendencies described in [7], we feel three of them are most important in a maritime scenario:

(1): Different network operators will clearly provide coverage areas for the maritime customers. Hence, it is important for the communication architecture to be independent of administrative concerns.

(2): Existing mobility studies focus on solving issues between two specific technologies and many mobility mechanisms are within specific network architectures, e.g., mobility handling in IP Multimedia Subsystem (IMS) and Ambient Networks. Therefore, it is desirable to have a more general or intelligent mobility handling mechanism that could be used in all heterogeneous maritime wireless networks.

(3): Mobility management is tending towards a cross-layer approach and favoring both user and network requirements. In other words, it will become common to gather an assortment of information from several sources: link to application layer taking into account QoE factors.

These mobility handling tendencies need to be taken care of in our maritime communication architecture. Since handover is the key enabling function for seamless mobility and service continuity, it is necessary to explain handover concept first. *Handover* indicates the process by which the mobile node obtains facilities and preserves traffic flows upon the change from one point of the network attachment to another, and according to [8], there are three primary characteristics of the networks that can serve to categorize handover: subnets, administrative domains, and access technologies. Therefore, six types of handover have been defined: *intradomain*, *interdomain*, *intrasubnet*, *intersubnet*, *intratechnology* and *intertechnology handover*. We will discuss mobility handling for *interdomain*, *intersubnet*, *intertechnology handover* based on interworking-level concept which has been introduced in Section 3. Inter-entity handovers are relevantly more common in the maritime environment and considered more difficult than intra-entity ones.

Interdomain Service Access - Level A and Level B. An interdomain handover involves the switching between different administrative domains, and requires authorization for acquisition or modification of resources assigned to the mobile. In CAMS, the onshore network behaves like a "home network" for maritime customers so as to let them be independent of administrative concerns. Therefore, Level A interworking is required to allow them to get access to services available in all "visited networks". Authentication, authorization, and accounting (AAA) functions need to be implemented in target system (see AAA Server Service and AAA Client Service in Fig.1). AAA functions allow customers to perform authentication and authorization processes in a visited network based on subscription profiles and security credentials. AAA services are known to cause significant overall handover delay. To address this, media-independent pre-authentication interdomain handover optimization [8] can be applied in CAMS for mitigating the total delay.

In order to get access to specific services provided by networks other than the serving one - Level B interworking - requires a data transfer mechanism. Virtual Private Networking (VPN) technology uses data encapsulation to achieve secure data transfer between two or more networked devices which are not on the same

private network and to keep the transferred data private from other devices or other intervening networks. There are different VPN approaches when it comes to wireless VPN. Columbitech has proposed a session-layer solution: using Wireless Transport Layer Security (WTLS) standard [9]. The WTLS solution enables secure and convenient remote access to the corporate network in an environment with multiple wireless access networks. Wireless VPN technology over WTLS standard is desired to be used in CAMS in order to achieve three aims:

- *Enable the transfer of user data between networks in order to give access to specific services provided in a network other than the serving one.*
- *Allow initialized incoming connections when using access networks with Network Address Translation (NAT) function.*
- *Enhance security for ship-to-shore communications based on tunneling technology (e.g., remote assistant and remote maintenance applications which demand high security).*

On-board LAN, onshore home network and onshore head office can constitute a virtual private network, in which AAA mechanism and tunneling technology are both applied. Therefore, security could be enhanced in two aspects. Primarily, only authorized users are allowed to access the ongoing information. Then, encryption can help achieve data integrity by protecting message contents from being modified under transit along the communication path.

Intersubnet Service Continuity - Level C. Service continuity during intersubnet handover often relies on the maintenance of a permanent mobile terminal IP address which can be addressed by Mobile IP or its variants. In Mobile IPv4, a foreign agent which works together with the home agent is needed on the visited network, while in Mobile IPv6, there is no need to deploy special routers as "foreign agents". Also, IEEE 802.21 standard which we will introduce later defines a set of handover enabling functions (for MobileIP) with required functionality to perform enhanced handovers. Therefore, MIPv6 is preferable in CAMS. However, considering that 1) MIPv4 works with IPv4 and MIPv6 was designed for IPv6 2) the slow adoption and migration from IPv4 to IPv6 3) the handover performance comparison between Host Identity Protocol (HIP) and MIPv6 in [10] and 4) HIP supports mobility between different IP address realms and easier NAT traversal [11], it is difficult to say which mobility management policy is better in the maritime context: stick to the current MIPv4 solution and move to MIPv6 when IPv6 is available or embrace HIP-based mobility handling directly. From the literature [10, 11, 12], we could expect that HIP is better than Mobile IP solutions in CAMS, while future testing and evaluation is needed.

Seamless Intertechnology Handover - Level D. Intertechnology handover is also referred to as vertical handover which can be further classified into two types [13]: *downward vertical handover* and *upward vertical handover*. Downward vertical handover is to switch between two networks that are both available. Hence, it often happens for convenience reasons (e.g., user's preference, higher bandwidth, lower delay, etc.), and the communication is still alive if the handover does not happen. Upward vertical handover to another available network

is mandatory in order to keep the communication active, because the mobile customer is moving out of the coverage of the current serving network. In this sense, decision making for downward vertical handover will be much more complex and deserves more effort than the upward one. It is more important because of customers' desire, e.g., when the ship approaches the shore, customers are willing to use WiFi connection. It is more complex because it needs more information for feeding handover decision maker from all involved parts - networks, terminal and user - which is often difficult to get.

In [13], vertical handover process has been divided into three phases: network discovery, handover decision and handover implementation. Handover implementation phase usually involves link establishment, higher layer mobility management and AAA functions. Higher layer mobility performing and AAA functions introduce significant delays during handover because of the difficulty of information collection and the lack of smooth cooperation between link and higher layer functions.

In order to address these deficiencies and help with handover decision making, IEEE 802.21 standard [14] has been introduced. IEEE 802.21 defines an abstraction layer between link and network layer which can be exploited by the IP stack (or any other upper layer) to better interact with the heterogeneous underlying technologies by mapping technology-specific primitives. A new link layer entity called Media-Independent Handover Function (MIHF) is specified in the standard. This MIHF entity mainly aims at exchanging of information and commands between upper and lower layers. The main function of MIHF is to coordinate the exchange of information and commands between the different devices involved in making handover decisions and executing handovers [15]. To upper layers, it provides a media-independent interface in order to collect information from link layer and to control link behavior. Regarding the different link layer technologies, it supports mapping between the common interface and a set of media-specific primitives. MIHF is designed both for terminals and networks; therefore, remote interfaces such as terminal-network and network-network interfaces will work together with local interfaces to aid the interactions among all devices involved in the handover. These interactions are provided by a set of services: event, command and information services [15].

Since the MIHF entities within terminals and networks can talk to each other, handover could be initiated from both sides. In the maritime communication scenario, the initiation is preferred to be done by the terminal (e.g. the onboard gateway equipped with multiple interfaces) for flexibility and prioritizing user's preference. While served by a given access network, the MIHF entity of the mobile terminal can interact with the MIHF entity in the serving network in order to get the information from other available networks, making it possible to initiate an intertechnology handover with desired pre-configuration for the target network [16] to reduce the handover delay. However, it is often necessary to have a list of candidate access networks in the mobile node, and the MIHF entities need to be added within all devices involved in the handover, together with the

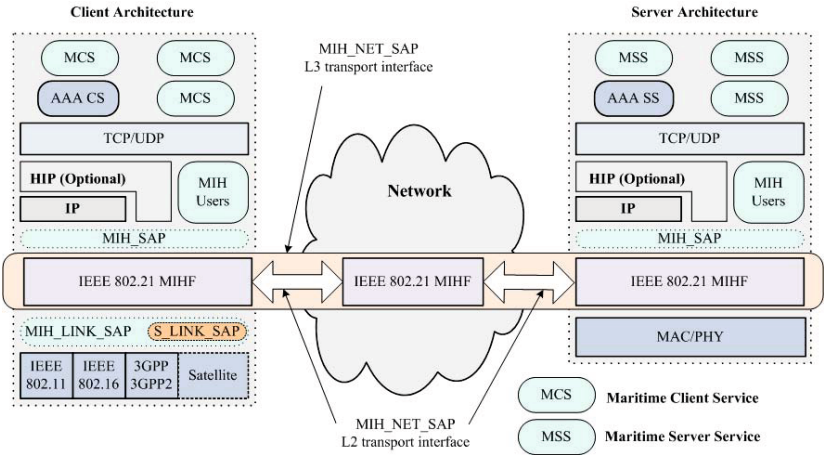

Fig. 2. Maritime Communication Architecture Protocols Stack

relevant protocols. Fig.2 below shows the protocols stack in the client side on board and the server side on shore of our maritime communication architecture.

IEEE 802.21 framework does not standardize the actual handover execution mechanism: handover decision-making or mobility management procedure. It recommends applying the Signal-to-Noise Ratio (SNR) metric for the handover decision-making. However, in the maritime scenario, using only SNR for handover decision-making is not enough since 1) there are different communication applications with different QoE requirements and 2) there are heterogeneous wireless access networks with different QoS characteristics. Therefore, several metrics could be combined together intelligently and dynamically so as to achieve more reasonable handover decision-making: SNR (or received signal strength (RSS)), QoS (e.g., bandwidth, data rate, access delay, losses), QoE (e.g., context information, price, user preferences, power consumption). Furthermore, a back-and-forth (ping-pong) effect should be avoided either by a more robust handover decision-making algorithm or by post-handover mechanisms.

IEEE 802.21 is designed to enable interoperability mainly among IEEE 802, 3GPP, and 3GPP2 networks. Similarly, ETSI has defined a broadband satellite multimedia (BSM) architecture [17] to provide a mechanism to carry IP-based protocols over different satellite networks by adding a satellite independent service access point (SI-SAP) interface layer, aiming to achieve interoperability among these satellite networks with different link layer technologies. BSM does not specify mobility management mechanisms. However, the methodologies of heterogeneity handling between BSM architecture and IEEE 802.21 framework are similar, hiding the differences by adding a common abstraction layer. Therefore, we could integrate SI-SAP within the IEEE 802.21 MIH framework to enable the handover between satellite networks and non-satellite networks in the maritime communication scenario, which is also recommended in [18].

4.2 QoE Support and Security Enhancement

Maritime communications are mainly based on wireless networks which often provide limited bandwidth with different QoS provisioning. Furthermore, maritime customers expect to have applications on board with differentiated parameters in terms of capacity, integrity and security. To address this requirement based on the restricted resources, application-level QoE support could be a good alternative. Application-level QoE support can be done by 1) differentiating applications with different priorities and 2) queuing their connections based on network conditions. The priorities are assigned according to customers preferences and the connection control takes place at the egress of the on-board gateway.

In CAMS, at first, different servers with different IP addresses can be used to separate applications. For example, there are basically two categories of applications: one for administrative system and the other for welfare. Under each category, there are several sub-categories. Within administrative system, there are emergency messaging sending, safety and monitoring data transmission, reporting information exchanging and so on. They could be assigned with secondary priorities. Different traffic types (data, voice, video) can be separated as well, according to different port numbers and protocols, such as real-time and non real-time traffic. They could be assigned with third-level priorities. Therefore, the priority map is chaining different queuing "disciplines" together nicely where ongoing packets are sorted by filtering them on their protocols, ports, sources and destinations. The application-level QoE support mechanism is shown in Fig.3.

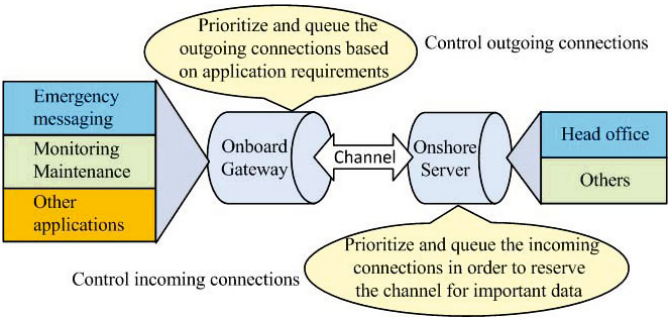

Fig. 3. Application-level QoE Support Mechanism

By adding graphical user interface to the Linux QoS configuration technique, the on-board gateway is able to intelligently allocate limited resources in accordance with prioritized egress connection demands based on customers preferences. However, it has to be carefully implemented to be available only for authorized users. The application-level QoE support is mainly for shaping outgoing traffic. It is difficult to shape incoming traffic from user side, because QoS policy decisions for ingress traffic are controlled outside the on-board network infrastructure. However, the onshore gateway can be used as an ingress

connection "controller" by queuing the incoming connections in order to reserve the channel for important data.

QoE support mechanism allows the customer to configure the system in order to make sure that more important data gets sent first, and various connections are given more fair treatment than usual. Together with our proposed VPN solution including a secure tunnel between the on-board gateway and the home network to carry sensitive information related to, e.g. ship's navigation and management, the on-board gateway has the capability to route certain packets through the encrypted tunnel, while separately forwarding unencrypted packets to the open Internet (see Fig.1). The unencrypted packets belong to value-added services provided to on-board customers who require such connectivity like browsing or multimedia. This two-prong approach helps the architecture to have a fine grained control over the data whilst avoiding home network with unnecessary data and routing information. The secure VPN tunnel connects the two trusted networks (on-board and home) through untrusted networks (access core and the Internet). By combining separation of traffic and VPN technology, security can be further enhanced. However, more detailed security mechanisms will be left for future work.

5 Conclusion and Future work

In this work we have introduced an integrated wireless communication architecture that tries to provide maritime customers ubiquitous services by integrating heterogeneous underlying wireless networks. Solutions for addressing key issues such as quality, security and mobility are covered in this architecture with more detailed discussion of seamless handover. We believe that future maritime communication will benefit much from integration of existing networks, and quality, security and mobility have to be carefully addressed simultaneously considering user preferences. However, future work is required to demonstrate the performance of our proposed architecture:

- A new maritime handover decision-making algorithm will be designed and tested in order to intelligently switch among heterogeneous maritime wireless networks and handover between satellite networks and non-satellite networks will be further studied.
- Application-level QoE support on both on-board and onshore gateways will be tested to prove the efficiency of reasonable utilization of limited resources according to different application requirements.
- Wireless VPN technology and AAA functions will be applied to the maritime scenario for measuring the security improvement.

References

1. MARCOM: Broadband at Sea, Internet for coast, polar regions, offshore and sea farming, `http://www.marcom.no/`
2. Pathmasuntharam, J.S., Jurianto, J., Kong, P.Y., Ge, Y., Zhou, M., Miura, R.: High Speed Maritime Ship-to-Ship/Shore Mesh Networks. In: 7th International Conference on ITS Telecommunications, pp. 1–6 (2007)

3. Schulzrinne, H., Wedlund, E.: Application-layer mobility using SIP. IEEE Service Portability and Virtual Customer Environments, 29–36 (2000)
4. Ferrus, R., Sallent, O., Agusti, R.: Interworking in heterogeneous wireless networks: Comprehensive framework and future trends. IEEE Wireless Communications 17, 22–31 (2010)
5. TU-T Recommendation Std : Vocabulary and effects of transmission parameters on customer opinion of transmission quality. ITU-T, P.10/G.100 (2008)
6. Buddhikot, M., Chandranmenon, G., Han, S., Lee, Y.W., Miller, S., Salgarelli, L.: Integration of 802.11 and third-generation wireless data networks. In: IEEE 22nd Annual Joint Conference of Computer and Communications, vol. 1, pp. 503–512 (2003)
7. Fernandes, S., Karmouch, A.: Vertical Mobility Management Architectures in Wireless Networks: A Comprehensive Survey and Future Directions. IEEE Communications Surveys & Tutorials, 1–19 (2010)
8. Dutta, A., Famolari, D., Das, S., Ohba, Y., Fajardo, V., Taniuchi, K., Lopez, R., Schulzrinne, H.: Media-independent pre-authentication supporting secure interdomain handover optimization. IEEE Wireless Communications 15, 55–64 (2008)
9. Columbitech: Columbitech Wireless VPN - Technical Description (2007)
10. Jokela, P., Rinta-aho, T., Jokikyyny, T., Wall, J., Kuparinen, M., Mahkonen, H., Melén, J., Kauppinen, T., Korhonen, J.: Handover performance with HIP and MIPv6. In: 1st International Symposium of Wireless Communication Systems, pp. 324–328 (2005)
11. Nikander, P., Gurtov, A., Henderson, T.R.: Host Identity Protocol HIP: Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks. IEEE Communications Surveys & Tutorials 12, 186–204 (2010)
12. Ratola, M.: Which Layer for Mobility? - Comparing Mobile IPv5, HIP and SCTP. In: Seminar on Internetworking in the Spring 2004, Espoo, Finland, T-110.551 (2004)
13. Chen, W.T., Liu, J.C., Huang, H.K.: An adaptive scheme for vertical handoff in wireless overlay networks. In: 10th International Conference on Parallel and Distributed Systems, pp. 541–548 (2004)
14. IEEE Draft Std: IEEE Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services. P802.21/D14 (2008)
15. De La Oliva, A., Banchs, A., Soto, I., Melia, T., Vidal, A.: An overview of IEEE 802.21: media-independent handover services. IEEE Wireless Communications 15, 96–103 (2008)
16. Dutta, A., Chakravarty, S., Taniuchi, K., Fajardo, V., Ohba, Y., Famolari, D., Schulzrinne, H.: An Experimental Study of Location Assisted Proactive Handover. In: Global Telecommunications Conference, pp. 2037–2042 (2007)
17. ETSI Std: Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Services and architectures. European Telecommunications Standards Institute, TR 101 984 (2007)
18. Hu, Y.F., Berioli, M., Pillai, P., Cruickshank, H., Giambene, G., Kotsopoulos, K., Guo, W., Chan, P.M.L.: Broadband satellite multimedia. Communications 4, 1519–1531 (2010)