Reconfigurable Radio Systems: Towards Secure Collaboration for Peace Support and Public Safety

Johan Sigholm
Swedish National Defence College, Stockholm, Sweden
johan.sigholm@fhs.se

Abstract: As military priorities are shifting from invasion defense to crisis management and peace support operations, the capability to partake in efficient inter-organizational collaboration is becoming increasingly important for armed forces across Europe. The "solidarity clause" of the Treaty of Lisbon, which entered into force on December 1st 2009, dictates that all EU member states shall act jointly if another member state is the target of a terrorist attack or the victim of a natural or man-made disaster. Sweden has gone even further, stating that it will not remain passive if a member state or another Nordic country is attacked, and expects these countries to act in the same manner if Sweden is attacked. This declaration obligates Sweden to be able to collaborate successfully with allied partners, both within own territories and abroad. Application-based collaboration tools for use in unpredictable settings, requiring high user mobility and network survivability, put high demands on the underlying ICT systems in order to function correctly. Networks employing the TErrestrial Trunked RAdio (TETRA) standard are becoming pervasive as platforms for interagency collaboration in crisis response. Although these networks provide many benefits compared to legacy technology they lack the possibility to offer secure, infrastructure-less and disruption-tolerant communication in challenging environments. Emerging ICT such as MANET-based Reconfigurable Radio Systems (RRS) shows potential for overcoming these problems, in addition to resolving issues of technical heterogeneity. The Common Tactical Radio System (GTRS) is an RRS being developed by the Swedish Armed Forces, intended to be the future ICT system for all parts of the forces, used both in national and international mission settings. However, remaining challenges include threats of node compromisation and adversary network infiltration, as well as the safeguarding of confidential information shared by collaborating parties and preventing information leakage. This paper contributes by (i) giving a summary of recent work in mechanisms for achieving information security in tactical MANETs and Hastily Formed Networks for disaster response. The paper also (ii) presents in-progress work towards the design of a gossip-based cross-layer Distributed Intrusion Detection System (DIDS) for the GTRS system, which takes resource constraints of portable devices into account, and offloads traffic analysis and anomaly detection to more powerful "Big Brother" nodes. An outline of the proposed DIDS architecture is presented, and the paper (iii) suggests future work towards offering a dependable and trustworthy communications platform for efficient and secure inter-organizational collaboration.

Keywords: reconfigurable radio systems, MANET, distributed intrusion detection, hastily formed networks, disaster response collaboration, emergency management communication

1. Introduction

During the last decade, The Swedish Armed Forces has gone through a fundamental transformation process. From investing most of its resources in guarding the country's borders against hostile invasion, the focus has shifted to participation in multinational military ventures, such as international crisis management and peace support operations. These new tasks introduce novel requirements, demanding the adoption of a more flexible mission-orientated organization. As a result of budget cuts and changes in policy, the Swedish Armed Forces have also shrunk considerably in numbers. Where, in 1997, approximately 600 000 people could be mobilized, only 35 000 remain enlisted today, and the amount of active military bases and regiments have decreased by 90%.

As a result of these changes, where fewer people now have to solve more complex tasks, the need for technical support systems and effective collaboration tools has increased dramatically. More efficient collaboration is required between military branches to make good use of the limited resources, but also to allow for work with external parties, such as other national government agencies, or to share information with coalition partners or NGOs during international operations. Collaboration has thus become an important part of the modern defense forces, and there is a growing need to find information and communication technology (ICT) systems and methods which provide support for this important capability.

Looking back at the history of communications systems within the Swedish Armed Forces during the last 50 years, there has been a continuously increasing requirement of efficient and pervasive communications. This demand has led to the procurement of hundreds of different radio systems, ranging from large stationary low frequency systems to handheld "walkie-talkies". In addition, the acquisitions of communications systems have usually not been coordinated between the different

branches of the Armed Forces. The result has many times become painfully obvious, especially during joint exercises, where interoperability issues have lead to time and resource consuming extra work instead of efficient collaboration between Army, Air Force and Navy units (Molin 2003). Managing a large amount of different communications systems also causes costly logistical problems, such as service, maintenance and stockpiling, as well as requiring longer education and training for operators.

2. Collaboration requirements

One of the major challenges in realizing effective collaboration is thus how to achieve inter-organizational interoperability, so that the technical systems can communicate and exchange mission information, and that the collaborating organizations can interact using their equipment. Many times collaborating parties also come from organizations which are not only technically heterogeneous, but may also have different communication cultures and organizational structures. This heterogeneity can prove challenging when responding to a situation which requires collaboration in order to successfully carry out the tasks at hand.

We have seen previous examples of this, where one such incident was the Hurricane Katrina, which hit the coast of Louisiana in 2005, killing almost 2000 people and causing damages in excess of $80 billion (Knabb et al. 2006). There were a large amount of various governmental agencies responding to the disaster, including the police, military units, fire fighters and medical services, and among the non-governmental organizations the American Red Cross alone assembled approximately 250 000 volunteer rescue workers (Becker 2008). Dividing the work load and organizing the information dissemination between all these people proved itself to be a greater challenge than anyone had previously realized, and many post-disaster studies have tried to find a solution for future similar scale disasters.

One of the conclusions drawn in the aftermath of Hurricane Katrina was that the quality of the cooperative response did not depend primarily on pre-incident operation planning or investments in state of the art equipment, but on the quality of the network which came together to provide relief (Denning 2006). This so-called Hastily Formed Network (HFN), consisting of interconnected voice and data communications systems, in combination with the multi-organizational collaborative environment, constitutes the conversation space through which the players interact to fulfill a common, urgent goal. Further studies have shown that one of the key issues in achieving mission success in such HFNs is maintaining a high level of pre-incident technical and social education and training within each organization, both when it comes to operating own ICT equipment and how to interact with other organizations in the network by establishing communities of practice (Törnqvist et al. 2009).

3. Emerging ICT systems for collaboration

The need for an adequate ICT platform supporting collaboration for public safety professions led to the standardization of the TErrestrial Trunked RAdio (TETRA) mobile radio system in the mid-1990s by the European Telecommunications Standards Institute (ETSI), previously also known for the GSM standard. In the Nordic countries the TETRA standard has been employed to create national dedicated radio networks for emergency management services and government agencies, such as the Swedish RAKEL network and the VIRVE network in Finland. These networks provide many benefits, such as inter-agency communication, allowing for collaboration, but they also have some drawbacks such as requiring a fixed infrastructure and new specialized hardware in order to interoperate.

In emerging ICT systems for inter-organizational collaboration, technical interoperability issues are being addressed by the integration of bridging technologies. This allows for establishing hybrid networks, consisting of both modern and legacy systems, so that several different ICT systems can be connected. The advent of Software Defined Radio (SDR) technology has paved the way for the development of RRS (Reconfigurable Radio Systems), also promising decreased lifecycle costs and longer durability for the equipment. RRS equipment has the capability to rapidly interconnect disparate radio networks by merely loading the required waveform and signaling specifications in software. In combination with Cognitive Radio technology, which gives improved spectral utilization by intelligent frequency allocation, RRS equipment has the potential of providing a solid platform for reliable end-to-end communications in challenging and dynamically changing environments.

An example of these emerging RRS systems is the Swedish Armed Forces' currently ongoing development project Common Tactical Radio System (GTRS), a Swedish version of the similar US-developed Joint Tactical Radio System (JTRS). This system seeks to benefit from SDR technologies to implement a tactical IP-based mobile ad hoc network (MANET) as a platform which should fulfill all future military communication needs. The first demonstrator GTRS units were delivered during 2007, and the system is scheduled to be completely deployed during 2014. By implementing internationally standardized waveforms, the system also allows for collaboration with external parties, both national and international. Besides Swedish national waveforms, the GTRS system will also be able to handle the TETRA waveform described above.

In MANET-based networks, data is transmitted from one node to another, by letting other nodes on the path between the sender and receiver relay the message one hop at a time. MANET technology differs from Mesh networks by also letting the nodes move independently in any direction, resulting in a non-static frequently changing connectivity environment. The benefits of using MANET-based ICT systems are that they are very flexible and robust, and they can also be used in areas where no traditional communications infrastructure is available (Asplund et al. 2008).

Scenarios where this technology platform offers leverage over traditional centralized or point-to-point communication methods are during operations in undeveloped areas, or extended areas hit by natural or man-made disasters (Törnqvist et al. 2009). In these situations it is not practical, or economically feasible, to deploy interimistic cover-all solutions, such as container-based mobile telephony systems, microwave links and satellite communication equipment. They might however work in compliment to each other, e.g. traffic generated in a MANET network, destined for an external recipient, may be handed over to available infrastructure at a bridging point for subsequent termination.

4. Security challenges and solutions

As previously mentioned, efficient collaboration, sharing of resources and dividing tasks in a joint mission is very important for future defense forces. In a perfect world the collaborating parties, connected by interoperable ICT systems might easily achieve this by opening up their networks, systems and databases to each other and providing full access to all resources. Naturally, this utopian scenario is not realistic in a real-world situation. The need for control over sensitive or classified data disqualifies completely open systems as an option, in national as well as international collaboration situations. This is especially true on the battlefield, where the threat of disruptive adversary action is also present.

In the TETRA standard there are several mechanisms to provide system security (Roelofsen 2000). Many of these are similar to the ones present in the GSM system, providing confidentiality, integrity and authentication. Besides standard cryptographic algorithms for ensuring end-to-end confidentiality for individual calls, there is also an advanced scheme for authentication. This is used both so that the network can know that all connected mobile stations (phones) are legitimate, but also so that the mobile stations know that the network they are connecting to is trusted, and not a "fake base station" set up by an adversary. A remaining problem in TETRA networks is the lack of protection against interference or intentional jamming attacks. Although the time division slot structure theoretically allows for slow frequency hopping (Politis et al. 2007), this is still not part of the TETRA standard. One of the main reasons for this being that the available frequency region is too small for frequency hopping to give any major improvements (Stenumgaard 2009).

5. MANET security and survivability

MANET-based communications systems do however, besides the challenges present in TETRA networks, also introduce some new demands in order to ensure network survivability. Some of these challenges which a MANET-based collaborative system faces are summarized in Table 1.

Table 1: Challenges for a MANET-based network for collaboration

Challenge	Possible solutions
Traditional information security threats	Encryption, certificates, frequency-hopping
Opportunistic or adversary threats	Reputation-based system, intrusion detection
Disconnectivity	Delay and disruption tolerant protocols (DTN)
Resource constraints	QoS techniques, prioritization, optimization
Unknown network topology	Distributed, gossip-style protocols

The fact that information "jumps" between nodes in a MANET makes it very important to ensure that no intermediate nodes are compromised, or that the network itself is successfully infiltrated by adversary nodes. Furthermore, the network faces challenges such as disconnectivity, resource constraints and lack of central management, as well as traditional information security threats.

Distinguishing whether a detected anomaly is actually an anomaly, or simply something normal, is a problem which has drawn the attention of much previous research within the field of Distributed Intrusion Detection Systems (DIDS). According to a recent survey on MANET survivability (Lima et al. 2009), research efforts have mainly been focused on a few set of preventive and reactive techniques, specialized either on certain types of attacks or only on one layer of the protocol stack. Furthermore, requirements of heterogeneity, efficiency, robustness and self-management are still left to be thoroughly explored.

Survivability in MANETs can be defined through the dimensions *key properties*, *requirements* and *protocol layers*, as shown in Figure 1 (Lima et al. 2009). Tactical MANETs, intended for use in military scenarios, have need for properties and requirements which separate them from corresponding civilian networks. Properties such as resistance, the ability to uphold information security and to repel attacks, and requirements such as robustness and protection are prioritized, leaving interoperability and efficiency as secondary goals (Russert et al. 2009). In order to allow for collaboration, while upholding basic properties and requirements, a method for detecting anomalies is desirable.

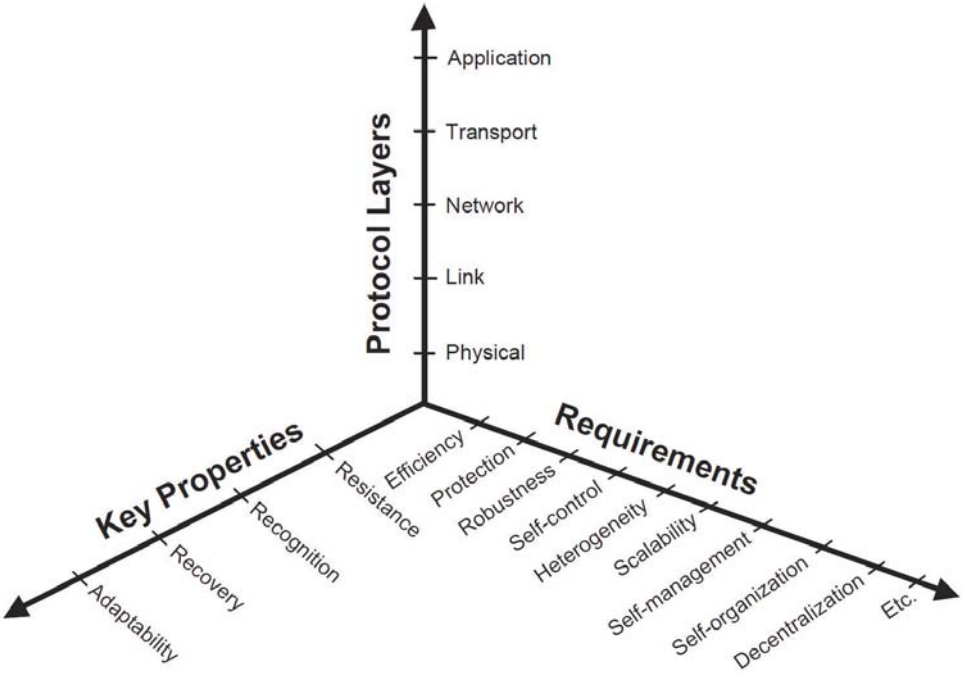

Figure 1: Dimensions of survivability in a MANET (Lima et al. 2009)

6. A MANET DIDS for collaboration

A proposed solution to address some of the security threats related to inter-organizational collaboration is to introduce a concept of "Big Brother" surveillance nodes, containing routines for distributed anomaly detection. This system is based on letting some nodes in the network, which have access to more resources, such as computational capacity, storage space, power and bandwidth, monitor and analyze the network traffic flows, and decide if anomalous or possibly malicious behavior is present, such as intrusion attempts or illegitimate information dissemination between collaborating organizations.

In order to be effective, a DIDS must be able to work on more than one network layer. There have been many previous projects which have studied distributed intrusion detection in MANETs (Huang and Lee 2003)(Yi et al. 2005)(Ma and Fang 2009), but they focus on detecting routing problems or target a given protocol layer. Some cross-layer detection projects exist (Wang et al. 2009), but they still focus on the lower layers. Other research has suggested an IDS for a specific service-oriented architecture (SOA) (Jormakka and Lucenius 2009), but it would be desirable to more generally be

able to monitor traffic on the application layer (OSI layer seven). This would let us analyze which information is being transferred in the network, and to ensure that it conforms to the stipulated security classifications, regardless of which applications are being used to send it.

By utilizing Deep Packet Inspection (DPI), a technology frequently used by commercial Internet Service Providers (ISP) in end-user broadband networks, actual traffic content can be studied. In ISP networks the technology is commonly used for bandwidth throttling (Parsons 2008), but it can also be used for effective wide cross-layer traffic flow categorization and regulation. By tracking network traffic up to the application layer, fine-grained network access control and protocol pattern consistency detection can be realized, e.g. monitoring database requests, web page access or specific e-mail content (see Table 2). This approach has been tested and successfully demonstrated in an industrial SCADA network (Batista et al. 2009), where unwanted traffic in an automation plant, caused by malware, was efficiently detected and consequences mitigated.

Table 2: Some network attack vectors and OSI network layer detection required

Attack vector	OSI layer affected
IP address spoofing	3
Routing attacks	3
Denial of Service attacks	3-4(7)
Port scans	4
Telnet/SSH connection requests	4
Worms	4-7
Viruses and Trojans	7
Disallowed e-mail attachments	7
Malformed HTTP or Web Services requests	7
Database leakage and SQL injections	7
C^4I^2SR application access	7

Although DPI technology seems promising for securing information in critical networks, applying this method in a MANET is not trivial. One of the challenges is that MANET traffic flows are not static, but rather change as nodes move. This requires monitoring nodes to not only listen to traffic they forward themselves, but also to traffic mediated by others within radio range. Another challenge is the absence of a logical network edge to monitor, which calls for collaboration between several monitoring nodes in a best-effort fashion.

Previous research on DIDS has presented solutions for how information can be shared between designated monitoring nodes in a MANET. A possible solution to exclude “misbehaving” nodes from the network is to use reputation a based mechanism (Rajaram and Palaniswami 2009), where nodes are ranked according behavior. “Bad” nodes are excluded from the network according to an election process. Distribution of messages can be done by use of gossip-style protocols, which can spread efficiently over sparse or frequently disconnected networks (Asplund and Nadjm-Tehrani 2009). Gossip-based protocols are also useful when the number of participating nodes is unknown, which may be the case in a collaborative scenario with interconnected sub networks.

In Figure 2 we see a model of a possible setup of an intrusion-aware collaborative MANET. The round vertices of the graph symbolize light-weight clients, such as portable handheld devices, embedded clients or resource-constrained nodes, running only basic security services. The square vertices of the graph represent the surveillance nodes, which except for the basic security services also run the distributed intrusion detection service routines. These nodes are more powerful when it comes to the available resources, and could be hosted on larger platforms.

A Big Brother surveillance node will primarily work as a normal communicating client, forwarding traffic between the light-weight clients, as we see the surveillance node BB_1 doing. Besides this, and while not taking an active part in the communications itself, the Big Brother node can monitor the traffic being transmitted within its radio range. As we see in Figure 2, the traffic between node X and Node Y is not forwarded as supposed, which is noticed and logged by node BB_3. This could be due to a number of reasons, such as temporary interference or lack of battery or processing power in one of the nodes. It could, however, also be a result of a persistent malfunction or an intentional disruption caused by a compromised or infiltrating node.

The different colors of the vertices in Figure 2 represent different collaborating organizations, and as we can see, a message can flow from node A in organization 1 to node B in organization 2. The surveillance node BB_2 is monitoring the traffic which leaves the network, and by using previously mentioned DPI methods, can verify that only legitimate traffic is being delivered into the collaborating partner's network.

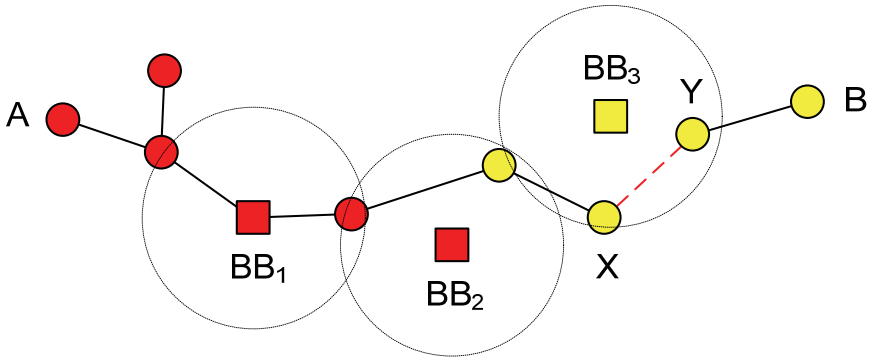

Figure 2: Outline of a collaborative MANET with distributed intrusion detection

Although it might not be easy to immediately distinguish an anomalous or malicious node, detected incidents can be logged, and over a period of time a pattern of deviant behavior can be illuminated. Comparing log data with other surveillance nodes can also help to affirm the patterns, by looking at the node reputation. If misbehavior is recognized, the findings are spread to all other nodes in the network, through network gossip, so that a malicious (or defective) node is eventually banned. This can be achieved by key revocation techniques similar to the one used in the TETRA networks. Other, more aggressive techniques can also be used, if the information flow needs to be terminated immediately. Such methods include inserting specially crafted TCP RST (reset) messages which forces the connection between two nodes to close – a modus operandi known from the Chinese national firewall, "The Golden Shield" (Clayton et al. 2006).

7. Summary and future work

Emerging ICT solutions, such as MANET-based Reconfigurable Radio systems, show potential for becoming strong platforms for future inter-organizational collaboration. However, there are still many challenges, especially concerning meeting information security requirements, which must be adequately addressed before these systems can be considered for military deployment.

An important, not yet addressed issue is that of the security of the DIDS and the Big Brother nodes, which themselves may become lucrative targets for a potential attacker. Future work will include a security analysis of the DIDS and a decision on how adequate system security can be obtained through methods such as pre-shared symmetric keys and policies for ensuring confidentiality, integrity and availability, and a PKI for digital signatures to provide authentication.

This paper has presented an outline of a Distributed Intrusion Detection System for the GTRS system, where designated surveillance nodes gather and analyze information about the collaborating nodes in the network. By using DPI methods, the system is expected to provide a fair level of cross-layer network security. However, since DPI requires a lot of resources, some concerns can be raised as to how costly such a solution would be to implement. Future work will therefore also include a technology demonstrator, implemented in the GTRS system software through the OPNET™ network simulator, with measurements of the performance costs that this functionality comes with. Based on the results of this future study, decision can subsequently be made as to whether a Distributed Intrusion Detection System is of practical use for the GTRS platform.

References

Asplund, M. and Nadjm-Tehrani, S. (2009) "A Partition-tolerant Manycast Algorithm for Disaster Area Networks", in Proc. *28th IEEE International Symposium on Reliable Distributed Systems (SRDS 2009)*, Niagara Falls, NY, USA, September.

Asplund, M., Nadjm-Tehrani, S. and Sigholm, J. (2008) "Emerging Information Infrastructures: Cooperation in Disasters", in Proc. *3rd International Workshop on Critical Information Infrastructures Security (CRITIS'08)*, Rome, Italy, October.

Batista Jr., A.B., Kobayashi, T.H., Medeiros, J.P.S., Brito Jr., A.M. and Motta Pires, P.S. (2009) “Application Filters for TCP/IP Industrial Automation Protocols”, in Proc. *4th International Workshop on Critical Information Infrastructures Security (CRITIS'09)*, Bonn, Germany, October.

Becker, J.C. (2008) “The opportunities and Limits of Technology in Non Profit Disaster Response”, keynote speech at the *5th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2008)*, Washington DC, May.

Clayton, R., Murdoch, S.J. and Watson, R.N.M. (2006) “Ignoring the Great Firewall of China”, in Proc. *6th International Workshop on Privacy Enhancing Technologies (PET 2006)*, Cambridge, UK, June.

Huang, Y. and Lee, W. (2003) “A Cooperative Intrusion Detection System for Ad Hoc Networks”, in Proc. *1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’03)*, Fairfax, VA, USA, October.

Jormakka, J. and Lucenius, J. (2009) “Intruder Detection System Architecture for a SOA-based C4I2SR system,” in Proc. *The First International Conferences on Advanced Service Computing (SERVICE COMPUTATION 2009)*, Athens, Greece, November.

Knabb, R.D., Rhome, J.R. and Brown, D.P.(2006) “Tropical Cyclone Report: Hurricane Katrina, 23-30 August 2005”, National Hurricane Center, National Oceanic and Atmospheric Administration.

Lima, M.N., dos Santos, A.L. and Pujolle, G. (2009) “A Survey of Survivability in Mobile Ad Hoc Networks”, *IEEE Communications Surveys & Tutorials*, Vol 11, No. 1, pp. 66-77.

Ma, C.X. and Fang, Z. (2009) “A Novel Intrusion Detection Architecture Based on Adaptive Selection Event Triggering for Mobile Ad-hoc Networks", in Proc. *Second International Symposium on Intelligent Information Technology and Security Informatics (IITSI 2009)*, Moscow, Russia, January.

Molin, M. (2003) “Flygande Plattformar: Integrering i ett framtida NBF” (Airborne Platforms: Integration in Future Network-Centric Warfare), *Ledningssystemutveckling 03-04*, Dept. of War Studies, Swedish National Defence College, Stockholm. Available at: http://systeminformatik.se/sams/res03/mm.pdf

Parsons, C. (2008) “Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials”, Integrated Research Sub-Project, The New Transparency. Available at: http://www.surveillanceproject.org/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf

Politis, I., Tsagkaropoulos, M. and Kotsopoulos, S. (2007) “Video Transmission over TETRA”, in P. Stavroulakis (ed.) *Terrestrial trunked radio - TETRA: A global security tool*, Springer Berlin Heidelberg, pp. 133-190.

Rajaram, A. and Palaniswami (2009) “A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks”, in *International Journal of Computer Science and Information Security (IJCSIS)*, Vol 6, No. 1, pp. 165-172.

Roelofsen, G. (2000) “TETRA Security”, *Information Security Technical Report*, Elsevier Science, Vol 5, No.3, pp. 44-54.

Russert, S.W., Fleischman, E.W. and Templin, F.L. (2009) “RANGER Scenarios”, IETF Network Working Group Internet-Draft, draft-russert-rangers-01.txt, September.

Stenumgaard, P. (2009) “Robust Wireless Communication for Security and Emergency Management”, Talk given at Linköping University, November 17.

Törnqvist, E., Sigholm, J. and Nadjm-Tehrani, S. (2009) “Hastily Formed Networks for Disaster Response: Technical Heterogeneity and Virtual Pockets of Local Order”, in Proc. *6th International Conference on Information Systems for Crisis Response and Management (ISCRAM2009)*, Gothenburg, Sweden, May.

Yi, P., Jiang, Y., Zhong, Y. and Zhang, S. (2005) “Distributed Intrusion Detection for Mobile Ad Hoc Networks” in Proc. *2005 Symposium on Applications and the Internet Workshops (SAINT 2005 Workshops)*, Trento, Italy, February.

Zhang, Y., Lee, W. and Huang, Y. (2003) “Intrusion Detection Techniques for Mobile Wireless Networks”, ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol 9, No.5, pp 545-556.