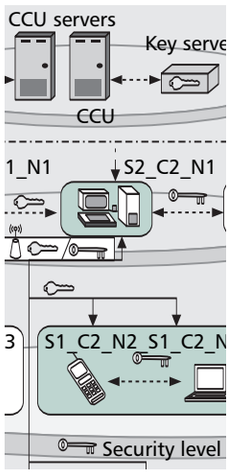
ACCEPTED FROM OPEN CALL

# NETWORKING FOR CRITICAL CONDITIONS

NIRWAN ANSARI, CHAO ZHANG, ROBERTO ROJAS-CESSA, PITIPATANA SAKARINDR, AND EDWIN S. H. HOU, NEW JERSEY INSTITUTE OF TECHNOLOGY
SWADES DE, INDIAN INSTITUTE OF TECHNOLOGY DELHI




To enhance the preparedness of federal and state agencies, the authors propose a hybrid adaptive network that will adopt the currently available off-the-shelf wireless network devices and integrate them quickly into a scalable, reliable, and secure network.

## ABSTRACT

To enhance the preparedness of federal and state agencies to effectively manage federal or state recovery efforts in response to a broad spectrum of emergencies, we propose a hybrid adaptive network that will adopt currently available off-the-shelf wireless network devices and integrate them quickly into a scalable, reliable, and secure network with a minimum of human intervention for configuration and management. This model will serve as the framework for various rescue missions for securing and distributing critical resources. We investigate different technologies and network strategies and integrate them into the proposed network model to provide seamless support to heterogeneous environments including wireline nodes, ad hoc and sensor network nodes, and network devices based on different standards. In this article we present the network architecture and identify the key technical aspects of its management, security, QoS, and implementation.

## INTRODUCTION

In many unexpected critical situations caused by natural disasters, such as hurricanes and earthquakes, or by terrorist attacks, such as the attacks of 9/11, the efficiency and safety of the responders' mission heavily rely on information technology. Usually, the destruction or extremely limited availability of the communications infrastructure of the region in distress exacerbates the rescue and recovery operations. Voice services, used to communicate among responders and with headquarters for control and command, or used by those affected by the emergency situation, may be severely restricted and unreliable even when available. Furthermore, often it is impossible to share and use all the relief resources through advanced information technologies — such as accessing remote databases, Web sites, and Web-based applications — and exchange data with agency headquarters and other field command centers. A new set of communications tools is required to significantly improve the safety of responders and the effectiveness of rescue and recovery operations [1, 2]. Inspired by Federal Emergency Management Agency (FEMA) requirements and incorporating state-of-the-art technologies, we propose a heterogeneous network for critical situations, which is required especially after large-scale disasters in which the existing communication infrastructure may have been destroyed.

The difference between a network for non-emergency situations and the proposed network is that a critical infrastructure network must operate reliably upon deployment, and the desired quality of service (QoS) must be provided during rescue operations. Furthermore, the services provided by such networks are aimed at assisting rescue operations to first avoid fatalities. Considering this, the following are special requirements for the proper and effective operation of critical networks:

- **Rapid deployment**
  - –Planning must be on the fly as minimizing the number of fatalities can be time-dependent, and a formal planning process is not feasible.
  - –Deployment processes must be simple and secure so that highly specialized personnel and complex procedures are not required.
  - –Equipment must be tolerant of faults and capable of rapid deployment, which involves rough treatment due to the short timeframe required for rescue operations.
- **Robustness and scalability**
  - –Suboptimal deployment and a frequently changing environment challenge network functionality. Therefore, the network must be able to report environment changes for proper management or be self-manageable to avoid service disruptions.
  - –The infrastructure must be sufficiently flexible to satisfy a variety of situations and provide support for different types of users, as well as for operations in different environments.
- **Portability**: The deployment of a communication network must be done within a short time due to critical conditions. To make it practical, the network should require less specific facilities and adopt commonly available resources and facilities from different response forces.
- **Security**: Large-scale disasters require responses from multiple federal, state, and local agencies with different charters, and possibly also from military forces. A tremendous amount of sensitive data in the network could be exposed to the transmission media and should be appropriately protected.
- **Cost**: The network should incur reasonable cost for deployment and maintenance, and


1536-1284/08/$25.00 © 2008 IEEE

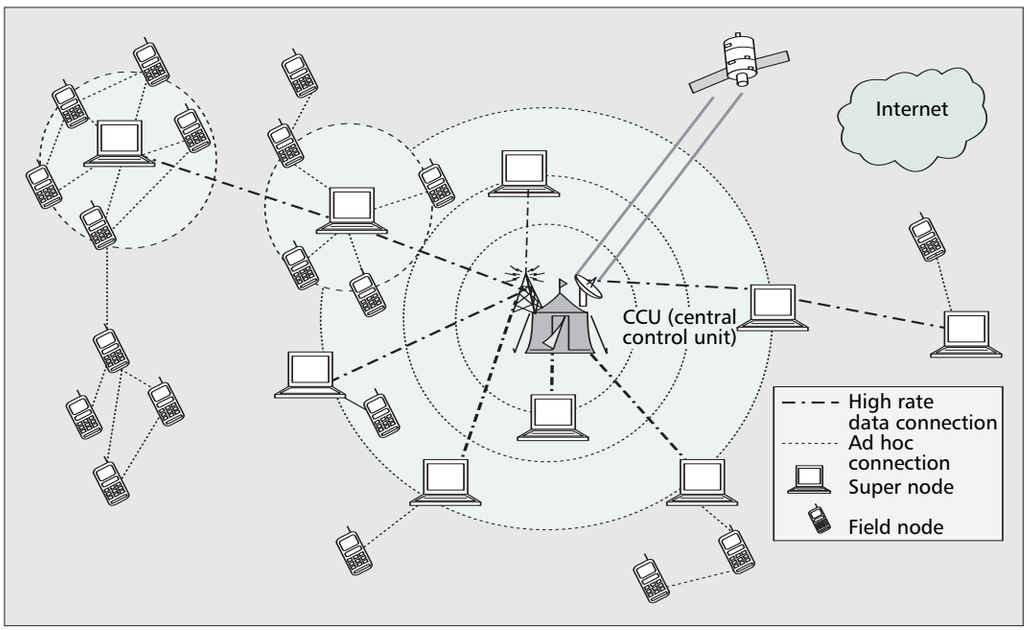



**Figure 1.** *Proposed critical network for safe and reliable response.*

To satisfy the strict requirements of reliability, performance, guaranteed lifetime, and functioning, the architecture of our proposed network for critical conditions (NCC) is based on a hybrid approach using different wireless technologies.

off-the-shelf technologies should be readily adopted.

The networks for disaster and emergency response proposed in [2] can provide up to 120 Mb/s connections between a specifically designed hub and up to eight remote sites. Each site could support a full range of applications for 120–160 users. Their major disadvantages are less scalability and the requirement for specialized devices. The heterogeneous network we propose will be reliable, efficient, scalable, portable, and secure. Portability means that deployment can be achieved within a short time for emergency conditions. Furthermore, to make our proposal practical, we consider the use of commonly available resources and facilities to set up the proposed network, and the implementation of resilient network devices that are specially designed to satisfy the requirements of critical networks. This network is planned to enable communications for data, voice, images, and real-time video to be used by a rescue task force working at the area in distress and with expandable possibilities for use by survivors with elementary and emergency communication requirements. An example of a possible model for this hybrid heterogeneous network is shown in Fig. 1.

This critical network consists of several networks superimposed on each other to make a complete and reliable network. The network comprises a central control unit (CCU), super nodes (SNs), and field nodes (FNs).

The CCU is the heart of the whole network, and is monitored and controlled by the authorities in charge of the area. The CCU can consist of several computers that have very strong computing capabilities and reliable maintenance. These servers act as the processing headquarters and access points to the global Internet. The CCU collects information from the desired nodes and provides required resources to the needy ones.

The SNs are fixed or mobile units that have strong computing capabilities and reliable power supplies. Each SN communicates with the CCU at a high data rate and provides connectivity to all FNs nearby through wireless network connections (802.11 WLAN, 802.15 WPAN, or 802.16 WiMAX).

The FNs are personal computers, notebook computers, personal digital assistants (PDAs), and other portable network devices used by the responders. They can also be sensor nodes deployed to monitor the environment. Several nearby nodes form a cluster and communicate with outside cluster nodes through a cluster head (CH). The CH could be an SN or FN.

In the following sections the main focus is on presenting a general network design overview and a detailed discussion of its security aspects. Due to space constraints, the key technical aspects of other components of the design (e.g., management, interconnectivity, and QoS) are introduced briefly.

## Flexible and Robust Network Architecture for Critical Conditions

To satisfy the strict requirements of reliability, performance, guaranteed lifetime, and functioning, the architecture of our proposed network for critical conditions (NCC) is based on a hybrid approach using different wireless technologies. For the different requirements, the NCC uses the following three networks in the same geographical area with specific lifetimes based on response requirements and deployment complexity:

- **First response network (1RN)**, deployed within 12 hours of an event and with an initial lifetime of the first 24 hours or longer. Strategically placed access point nodes, based on the

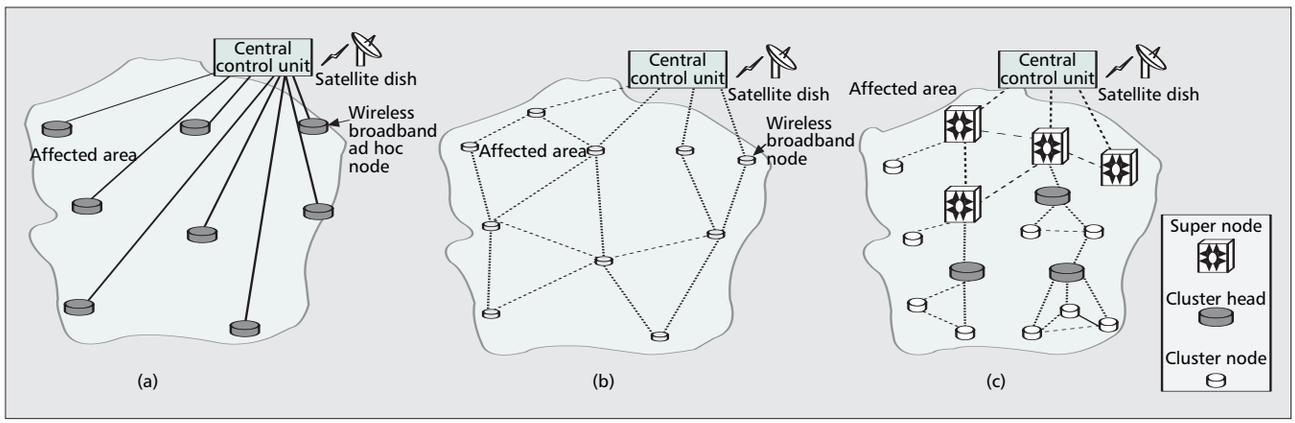



**Figure 2.** *Flexible and robust network architectures: a) 1RN with static ad hoc 802.16 nodes; b) 2RN with (possibly mobile) ad hoc 802.11 nodes; c) 3RN with static and mobile heterogeneous nodes.*

IEEE 802.16 standard, form a point-to-point wireless network with a star topology. This network ensures limited but effective and reliable communication with a small setup overhead as required in the first wave of response. Figure 2a shows an example of this network, in which all access points can directly communicate with the CCU through single-hop transmissions. These access points are used by rapid action agents to show signs of existence and place emergency requests, and by rescue personnel to communicate directly with rescue mission headquarters.

• **Second response network (2RN)**, deployed within the first 24 hours of an event and with an initial lifetime of 48 hours. Since 1RN is designed for first emergency communications independent of the available energy resources in the critical geographic area, the battery life of 1RN is expected to last a short time. 2RN is a power-aware network, where critical information is transmitted for communications that are critical but have a lower level of emergency. The architecture of this network is supplemented by wireless and possibly mobile nodes defined by the 802.16 standard. The deployment of 2RN is performed during (although with higher costs) or after the deployment of 1RN. In the latter case the placement of 2RN nodes can be performed with high efficiency by using the collected information from the 1RN phase. Figure 2b shows an example of such a network.

• **Third response network (3RN)** is deployed within 72 hours of an event and with a lifetime of five days or longer. The architecture of this network is a cluster-based wireless network consisting of ad hoc wireless LAN (802.11) nodes and sensor nodes (802.15 wireless personal area network, WPAN), as well as WiMAX (802.16) nodes. This network must be supported by portable energy sources or energy supplies from the affected region, because this network is expected to operate during the time of restoration of service of the affected geographical area. This network is required to transmit voice, multimedia, and data, and provide other computation services for a distributed and deployed rescue mission. This network is also expected to assist during the restoration phase of the affected place; therefore, the life span would be limited to the duration of the requirement. During the deployment of 3RN, power can be supplemented to 1RN and 2RN as needed, thus enhancing the coverage, connectivity, and QoS support of the NCC. Figure 2c shows the concept of 3RN, which is explained in greater detail in the next section. Since the 3RN is the last stage of deployment, 1RN and 2RN are also included.

There are two levels of redundancy in 1RN, 2RN, and 3RN that increase system reliability. The first level of redundancy is at the deployment level. 2RN provides system redundancy to 1RN, and 3RN provides system redundancy to 1RN and 2RN.

The phased deployment of the NCC inherently addresses network reliability. 1RN provides basic network connectivity in the affected region. Deployment of 2RN reduces the need for long-haul communication links and hence slows battery drainage by introducing a multihop communication capability. Finally, 3RN infrastructure further improves the robustness of an NCC by clustered information processing and communication capability, as well as helping replenish the battery life of nodes deployed in the 1RN and 2RN phases.

At the second level, each node in 1RN, 2RN, and 3RN is built with fault-tolerant architectures to avoid node substitution and failure risks. The nodes run test routines during deployment and use low-power hardware redundancy on critical systems, such as processor and monitoring software. To provide some degree of connectivity to the network in such conditions, these nodes are designed to have gracefully decreasing functionality in case of unrecoverable failures. For example, some nodes may not be used to initiate a connection but instead to assist in forwarding information from other nodes and therefore increase network lifetime through energy savings. This node design simplifies deployment because the nodes require minimum human intervention for configurability.

Beyond architectural and deployment strategies, protocol-level optimization for heterogeneous QoS support (discussed in a later section) addresses network lifetime, which further enhances the reliability.

## MANAGEMENT OF THE HETEROGENEOUS CLUSTER-BASED WIRELESS NETWORK

The CCU, the headquarters for the rescue operations, should be set up quickly at the onset of the rescue mission. At the same time, some SNs can be deployed at selected locations. These SNs will connect to the CCU directly or through other SNs via broadband wireless links. Other FNs will join this network around these SNs in an ad hoc manner.

During the rescue work, the network topology will morph frequently as new field nodes may join, nodes may move or leave, and nodes may be disabled. It requires a rapidly responsive clustering mechanism to organize the network at the work site. Based on the special conditions of the critical network, we proposed a novel design for building a secure NCC by integrating a simple clustering and multiprotection mechanism together. The clustered architecture has been used for routing, frequency and code distribution, and to provide an individual node a view of the network. A few nearby FNs will form a cluster. A more reliable node with strong computing ability will be elected as the CH. Communications between nodes outside the cluster and a cluster member go through the CH. The CHs communicate to the CCU in a multihop fashion via the SNs. The SNs store the information of the CHs in their neighborhood.

The associative relations among the nodes are kept in a hierarchical manner. The CCU stores only the relation of SNs with other nodes (including CHs). Therefore, a node (FN or CH) can be identified quickly by the SN to which it belongs. Likewise, an SN keeps track of the relation between its CHs and their corresponding FNs. The architecture is shown in Fig. 2c. Therefore, this heterogeneous architecture provides a very easy way to locate a node or retrieve information from areas of interest.

The management of an NCC is conducted mainly at the cluster level, involving a fraction of the total number of nodes in the network. More stable and reliable SNs play an important role in ensuring the reliability and robustness of this network. The CCU records the information of all nodes and possesses the big picture of the topology of the whole network. An SN maintains information for all of the nodes belonging to it and similar information from next-hop neighboring SNs. At each CH, the information of all the cluster members as well as the information from next-hop neighboring CHs is maintained. The information maintained at each level of node is shown in Fig. 3. This provides efficient service management of the entire rescue operation.

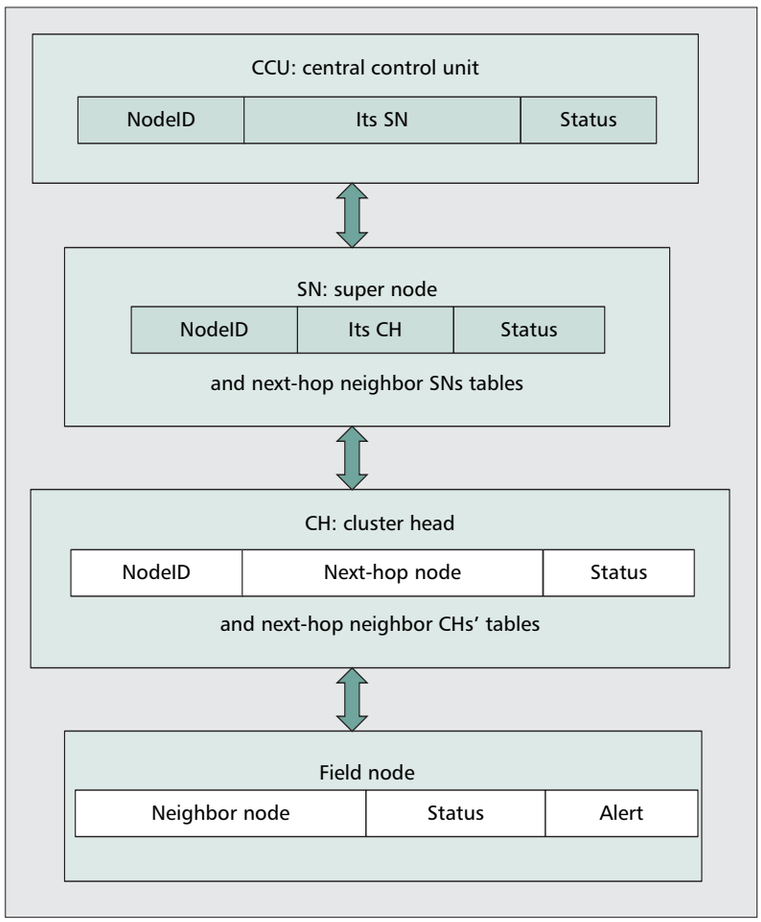



**Figure 3.** *Structural information maintained at each node level.*

## SEAMLESS INTERCONNECTIVITY FOR CRITICAL NETWORKS

To ensure a reasonable cost for deployment and maintenance, our proposed NCC adopts different off-the-shelf technologies such as WLAN, WiMAX, and WPAN for wireless networks, or layer 2- or layer 3-based networks for possible wireline connections. Services are thus provisioned via a tandem of network elements using different technologies. Thus, the data transmission overheads inevitably increase dramatically because each kind of technology defines its own control and signaling policy in a relatively independent way. To ensure seamless and optimized delivery of services across this heterogeneous network, it is important that the services are mapped according to the capabilities of the employed technologies, as well as those of the devices [3]. In other words, the formats and rates of the services are dynamically controlled according to the specific technologies and user devices [4]. The objective of this adaptation function is to guarantee service delivery without violating QoS requirements, and simultaneously ensure that network resources (i.e., bandwidth, channel capacities, and buffers) are efficiently utilized.

We propose to design a network interconnection platform to interconnect the heterogeneous parts of the communications systems together seamlessly. Figure 4 shows a system architectural view of this interconnection platform, where the services interconnection module, QoS interconnection module, and medium access control (MAC) interconnection module are embedded at each network interface for different technologies. The core part of this platform is a policy control module (PCM) at the SNs that maintains the possible service level abilities of all the

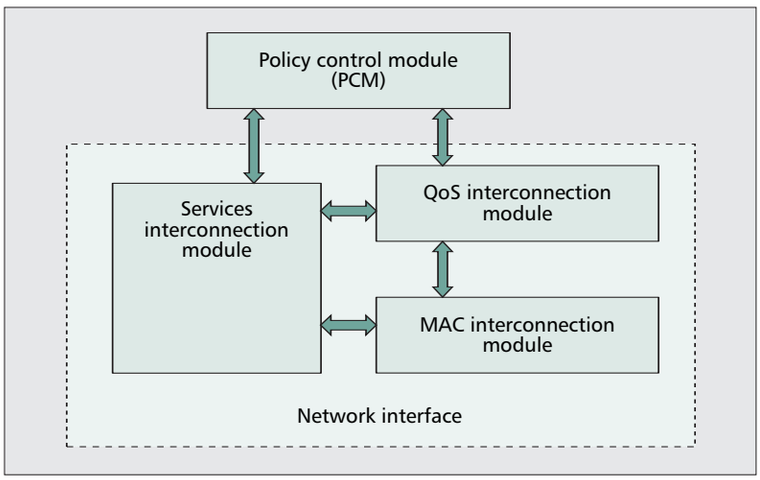



**Figure 4.** *Logical view of the network interconnection system.*

nodes belonging to it and the current network transportation status. The network management at each network interface makes appropriate decisions according to the information from the PCM and the policy rules. The PCM provides appropriate information to the services and QoS interconnection modules at the appropriate network interface. At each network interface, the MAC interconnection module allocates the network resource depending on the decision derived by the services and QoS interconnection modules.

## Heterogeneous QoS Support

The ability to provide seamless and adaptive QoS in a heterogeneous environment is fundamental for the success of an NCC [5, 6]. The services provided by our proposed critical communication network are data services, such as image file transfer and short message services (SMS) and real-time and near-real-time services, such as voice/video telephony, interactive multimedia, and video streaming. The requirements for both classes of services must be satisfied efficiently. Currently, most end-user wireless network equipment is embedded with 802.11 technologies. This kind of wireless device will be the dominant choice of response forces. In the following subsection we outline two major problems associated with the existing approaches and seek novel solutions to them.

### TCP Fairness in Ad Hoc Networks

Although IEEE 802.11 is known mainly as the MAC protocol used in Wi-Fi networks (infrastructure networks with a point coordination function [PCF] mode of operation), this standard is also designed to be implemented in ad hoc networks (infrastructureless networks, with a distributed coordination function [DCF] mode of operation). However, in many recent studies [7, 8], it has been shown that 802.11 does not work well in ad hoc mode, especially in terms of supporting TCP flows. It causes unstable throughput, an unfairness problem in the TCP layer, and overall inefficient bandwidth utilization.

The cause of these problems resides in the following. First, 802.11 does not coordinate packet transmission when there is more than one node that has packets to send. Second, the exponential backoff algorithm gives the node that most recently had a successful transmission a higher priority over a node that had a failed transmission, which eventually results in unfairness in TCP flows. Third, when a node that is blocked from transmission receives a request to send (RTS), it cannot respond to the sender until the channel is clear. This may result in the sender of the RTS mistakenly thinking that the destination node is unreachable, which could lead the network layer to search for a new route, hence causing more delay in transmission and a waste of network resources.

We propose to address the TCP unfairness issue at the MAC layer, which in turn affects the network and scheduling layer performances. The basic structure of the bi-channel MAC protocol is composed of two separate channels, one for control messages and another for data transmission [9]. Nodes always listen to both channels and are able to send/receive control messages even during data transmission or reception. In addition to the two control messages, RTS and clear to send (CTS), in 802.11, two more control messages are added to the protocol: request for access (RFA) and wait for clearance (WFC). Because the transmission of control packets does not interfere with data transmission, nodes can send control packets freely. This provides each node with more information about the status of its surrounding nodes and therefore enables the nodes to better coordinate with each other.

We assume the control packets are very small, and therefore the probability of collision is very low. Hence, simple carrier sense multiple access (CSMA) is used in the control channels. The purpose of the two new control messages, RFA and WFC, is to inform the active nodes of data transmission attempts from other blocked nodes. Therefore, after the currently active nodes have finished their data transmission, they back off for a longer period of time so that the blocked nodes have a chance to seize the media. The nodes operate based on the following rules:

- When a node has a data packet to send and the data channel is idle, it sends RTS.
- When a node has a data packet to send and the data channel is busy, it sends RFA.
- When a node receives an RTS and the data channel is idle, it sends CTS.
- When a node receives an RTS and the data channel is busy, it sends WFC.
- When a node receives a CTS or WFC while it is active, it keeps sending/receiving data and sets its backoff timer value so that it is longer than the contention window.

Note that the fourth rule eliminates the occurrence of a sending node mistakenly thinking the destination node is unreachable. Because the destination node responds to the sender upon reception of an RTS regardless of the data channel condition, the sender is well informed of the reachability of the destination node. The fifth rule is to reduce the unfairness problem in 802.11. When a blocked node has a packet to transmit, it is not required to wait until the data

transmission is over and try to obtain the access by chance. Instead, it can send an RFA to the nodes that are currently sending or receiving data, which will cause these nodes to back off longer after their transmission is over to allow the blocked node to gain access to the channel.

## Energy-Aware QoS Support for Delay-Tolerant Traffic

Besides the fair allocation of channel resources and traffic load balancing, optimum use of limited energy resources for data forwarding is important for the longevity of an NCC. Especially for delay-tolerant data forwarding, there may be alternative optimal choices.

Conventionally, in multihop packet data networks a transmitting node selects one of its neighbors based on certain criteria, such as proximity to the destination and the remaining energy to forward a packet [10]. Such forwarding approaches require that a list of all local neighbors be maintained at each node. However, the ad hoc nodes could be mobile, or the energy-constrained sensor nodes could go into sleep mode asynchronously to save power. Thus, due to mobility and the energy conserving tendency of nodes, maintaining updated local neighborhood information at a node could be costly.

An alternative to transmitter-side relay selection is a forwarding scheme in which the transmitting nodes do not decide which of their neighbors would relay their data packets; rather, all relay candidates contend among themselves to relay the packets [11–13]. We refer to this contention resolution process as receiver-side relay election (RSRE). In RSRE, similar to 802.11 DCF (or 802.15.4 contention mode), an RTS/CTS (or beacon/response) message exchange is done between the transmitter and a potential forwarder before data packet forwarding. However, unlike in 802.11, the RTS message is broadcast to all local neighbors, and a forwarder CTS response is suitably delayed to minimize potential contention.

The effectiveness of the RSRE process is best characterized first by the quality of the elected relay with respect to a chosen optimality criterion and second by the level of vulnerability of the election process to collisions. However, priority-dependent MAC contention probability and the related delay in the successful relay election process were not considered in previous research. Accordingly, we investigate the MAC contention in RSRE and the associated network QoS performance trade-offs with respect to parameters such as end-to-end delay, throughput, and energy efficiency. In the following we present the concept of a basic election process using time delay for contention resolution. For the sake of theoretical insight, we consider a network of uniformly random distributed nodes with a relaxed assumption of independent and asynchronous sleeping behavior.

A node desiring to send data packets first sends a broadcast RTS packet containing the optimality criteria and location information of itself and the final destination. After receiving the RTS packet, every eligible relay candidate $i$ schedules a reply time $\chi_i = g(\Omega_i)$, where $\Omega_i$ is the quality measure of node $i$ computed based on a given criterion used by the forwarding scheme. $g(\cdot)$ is a mapping function that implements the prioritization of the election process, and its nature determines the quality of the elected relaying neighbor with respect to the set of optimality criteria and the vulnerability of the election process to collision among two or more best candidates. Next, every relay candidate $i$ listens to the wireless medium between time 0 and $\chi_i$. If node $i$ overhears a CTS transmission during its waiting period, it assumes a better relaying candidate was found, and thus does not compete to relay. Otherwise, node $i$ considers itself the winner of the election process and sends a CTS packet with its signature to the transmitting node.

Upon correctly receiving a CTS, the transmitter sends the data packet to the relay. In case of any CTS message collision, all relay candidates give up in that contention cycle, and, as in 802.11 DCF MAC contention resolution, we assume the transmitter re-initiates the election process by broadcasting another RTS packet after a timeout.

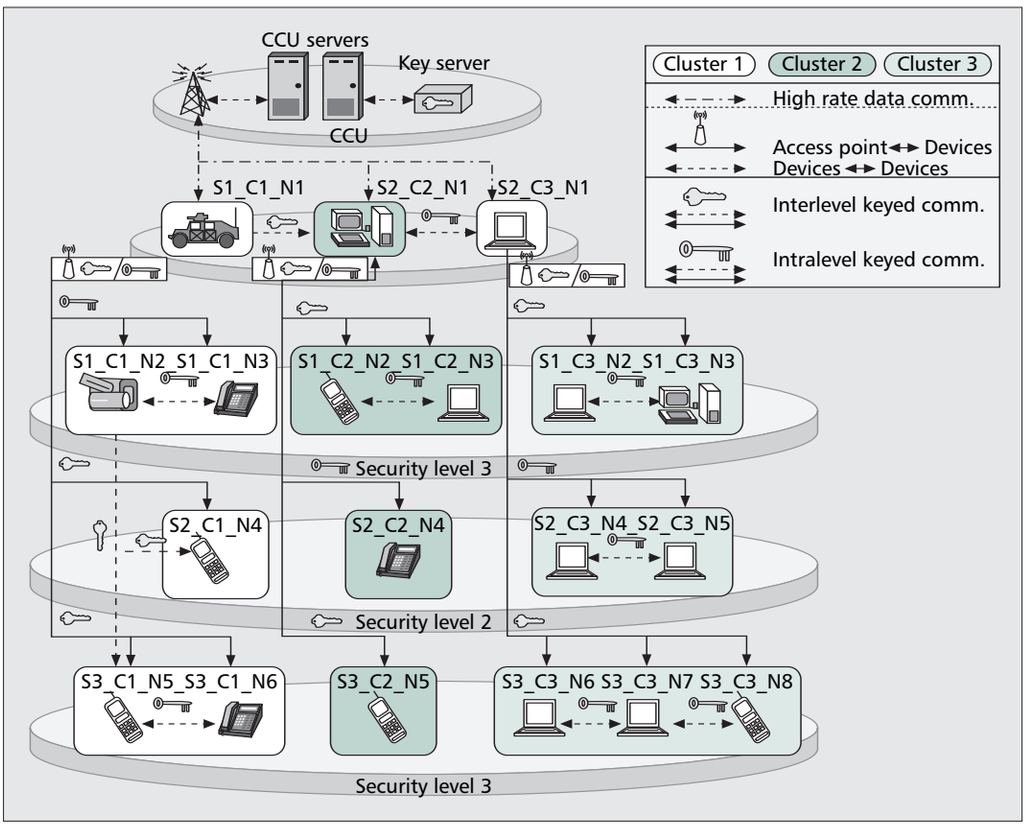
## Security Issues under Critical Situations

In addition to guaranteeing seamless interconnectivity and adaptive QoS support, security must be considered in designing a network [14]. Although an NCC is used mainly under critical situations, nevertheless a few threats exist that are detrimental to network performance. Because rescue workers may come from various organizations with different levels of responsibility and expectations (e.g., civilian, military, and/or international), access to appropriate information distributed in the network must be meticulously assigned, especially for a wireless ad hoc network a hostile user easily can intercept, login, and access. We propose a multilevel protection scheme by incorporating standard security solutions such as WiFi protected access (WPA2), secure sockets layer (SSL), and Radius to provide enhanced security solutions to our proposed NCC, as follows:

- The proposed critical network offers authentication, authorization, and access (AAA) control security through several fundamental services such as key management, digital certificate, digital signature, and encryption. All network devices must be authenticated by the CCU before joining the network. The CCU sets up the node profile, which includes member ID, group ID, security level, and group access privileges, of this new node, and then sends this information to the new node and the associated SN. The SN stores the node profile of all members under its supervision in its database. All nodes are categorized into several groups based on security levels and tasks. The group access privilege determines which task group a node can access. The security level determines which part of the information distributed in the task group the node can access. The security level and group access privilege-based communications are illustrated in Fig. 5.
- The proposed critical network offers detection of malicious nodes. It is difficult to detect a malicious node because it can act like a normal

In addition to guaranteeing seamless interconnectivity and adaptive QoS support, security must be considered in designing a network. Although an NCC is used mainly under critical situations, nevertheless a few threats exist that are detrimental to network performance.

The concept of group key management and discrete logarithm-based key exchange is expanded and incorporated into the network to make the transmission of packets and the distribution of keys more secure.




■ **Figure 5.** *Security-level-based communications in NCC.*

node for a period of time to avoid being detected, but then starts to act maliciously at other times. We propose a novel technique by combining a simple clustering mechanism and a voting mechanism. A clustering mechanism is used to facilitate security services (particularly for key management and group signature), and the voting mechanism supports the decision making process in the cluster. The group signature service enables an FN to sign the packet on behalf of the group with a group signature from which only the receiver can determine to which group the sender belongs. In case of a dispute, the receiver can determine the actual sender with help from the CH and SN.

Furthermore, we apply an adaptive trust-based network management in this network that can alleviate the problem of a single point of failure and a point of target. A trust and reputation system is widely used as a countermeasure against threats that attempt to deceive other users by impersonating legitimate users, or dropping, fabricating, and modifying packets. We enhance the performance of the voting system by gradually adjusting the average trust and reputation value that indicates the forwarding performance of each FN. The additive increment and multiplicative decrement strategy can be applied to sharply decrease the average trust and reputation value if a node acts maliciously, and to slowly increase the average trust and reputation value [15].

- The concept of group key management and discrete logarithm-based key exchange is expanded and incorporated into the network to make the transmission of packets and distribution of keys more secure.

All keys used in the network are generated from the key server, which is a part of the CCU. When a cluster is formed and the CH is chosen, the key server generates corresponding keys as shown in Fig. 6, where $C(\cdot,\cdot)$ is the cluster information, $S(\cdot,\cdot)$ is the security level information, $X$ and $Y$ are the security level indices for each node, and $M$ and $N$ are the cluster IDs for each node.

We categorize the communications in an NCC into four groups based on the encryption keys, as illustrated in Fig. 6. The following are two samples of communications between two nodes that are either in the same group or different groups and have either the same security level or different levels:

- Communications between two nodes that belong to the same security level and are located in the same cluster, such as S1_C1_N2 and S1_C1_N3:
  - –The intralevel intracluster key for cluster 1, $K_{C(1,1)}^{(Sl,1)}$, is used to encrypt and decrypt the packets exchanged on the path (S1_C1_N2 ↔ S1_C1_N3).
- Communications between two nodes that belong to different security levels but are located in the same cluster, such as S1_C1_N2 and S3_C1_N5:
  - –The interlevel intracluster key $K_{C(1,1)}^{(Sl,3)}$ is used to encrypt and decrypt the packets exchanged on the path (S1_C1_N2 ↔ S3_C1_N5) between the two nodes.

Because the cluster size is limited to a small

number, most of the decisions are made involving only a small number of nodes, with little effect on overall network performance. Note that we assume that all communications may be encrypted with the end-to-end key, which is not shown in Fig. 5.

To support rapid deployment, security mechanisms can be deployed as follows:

- Security-level-based communication is first applied to 1RN.
- Group key management can then be enhanced for 2RN.
- The voting mechanism and adaptive network management (with the trust and reputation concept) can be later added to 3RN.

Since 1RN corresponds to the first emergency task, the CCU can directly assign all the required security elements such as keys or signatures to all nodes. When 2RN is deployed, information from 1RN can be adopted to reduce the large overhead from initial establishment of group key management, as well as the time delay that might otherwise have caused 2RN to halt its operation during key management setup. Similarly, because groups were formed during the deployment of 2RN, information about the behavior of each node can be collected by designated nodes and the CCU to easily and quickly apply the trust and reputation mechanism to 3RN.

Therefore, configuration overheads from group establishment, key management, and voting mechanisms can be minimized, and rapid deployability can remain intact.

The information within the network from different sources can be safeguarded via standard solutions enhanced with our proposed multilevel protection schemes.

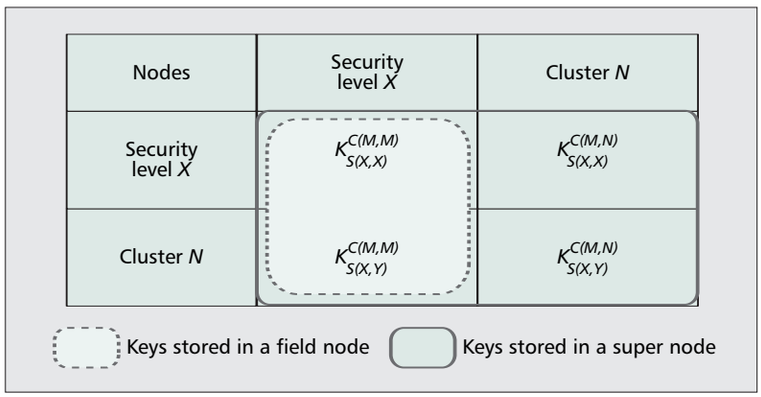



**Figure 6.** *Logical key structure.*

## SUMMARY

The proposed hybrid and heterogeneous network model integrates different technologies and network strategies. It can quickly adopt the currently available off-the-shelf wireless network devices and integrate them quickly into a scalable, reliable, and secure network with minimum human intervention for configuration and management under critical situations, such as natural or human-induced disasters. The proposed network provides seamless support to heterogeneous environments including wire line nodes, ad hoc and sensor network nodes, and network devices based on different standards. The security of the network will be enforced by means of multilevel protection of the network. This model will serve as the framework for various rescue missions in securing and distributing critical resources.

## REFERENCES

[1] FEMA homepage; http://www.fema.gov/library/ita.shtm
[2] S. F. Midkiff and C. W. Bostian, "Rapidly Deployable Broadband Wireless Communications for Emergency Management," Nati'l. Digital Government Research Conf., May 2001.
[3] M. Moustafa *et al.*, "QoS-Sensitive Broadband Mobile Access to Wireline Networks," *IEEE Commun. Mag.*, vol. 40, no. 4, 2003, pp. 50–56.
[4] J. Shin, J. W. Kim, and C. C. J. Kuo, "Quality-of-Service Mapping Mechanism for Packet Video Indifferentiated Services Network," *IEEE Trans. Multimedia*, vol. 3, no. 2, June 2001, pp. 19–231.
[5] M. Fischer, "QoS Baseline Proposal for the IEEE 802.11E," IEEE Doc. 802.11-00/360, Nov. 2000.
[6] B. Zhang and H. T. Mouftah, "QoS Routing for Wireless Ad Hoc Networks: Problems, Algorithms, and Protocols," *IEEE Commun. Mag.*, vol. 43, no. 10, Oct. 2005, pp. 110–17.
[7] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?" *IEEE Commun. Mag.*, vol. 39, no. 6, June 2001, pp. 130–37.
[8] Y. Tian, K. Xu, and N. Ansari, "TCP in Wireless Environments: Problems and Solutions," *IEEE Commun. Mag.*, vol. 43, no. 3, Mar. 2005, pp. S27–S32.
[9] Z. Cai, M. Lu, and X. Wang, "Channel Access-Based Self-Organized Clustering in Ad Hoc Networks," *IEEE Trans. Mobile Comp.*, vol. 2, no. 2, Apr.–June 2003, pp. 102–13.
[10] M. Mauve, J. Widmer, and H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Sensor Networks," *IEEE Network*, vol. 15, June 2001, pp. 30–39.
[11] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," *IEEE Trans. Mobile Comp.*, vol. 2, no. 4, Oct.–Dec. 2003, pp. 337–48.
[12] H. Fubler, J. Widmer, and M. Kasemann, "Contention-Based Forwarding for Mobile Ad Hoc Networks," *Elsevier Ad Hoc Networks*, vol. 1, no. 4, Nov. 2003, pp. 351–69.
[13] S. De, "On Hop Count and Euclidean Distance in Greedy Forwarding in Wireless Ad Hoc Networks," *IEEE Commun. Lett.*, vol. 9, no. 11, Nov. 2005, pp. 1000–02.
[14] V. Varadharajan, R. Shankaran, and M. Hitchens, "Security for Cluster-Based Ad Hoc Networks," *Comp. Commun.*, vol. 27, no. 5, Mar. 2004, pp. 488–501.
[15] P. Sakarindr and N. Ansari, "Adaptive Trust-Based Anonymous Network," *EIC Int'l. J. Sec. and Networks*, Special Issue on Computer and Network Security, vol. 2, no. 1–2, 2007, pp. 11–26.

## BIOGRAPHIES

NIRWAN ANSARI [S'78, M'83, SM'94] (nirwan.ansari@njit.edu) received a B.S.E.E. (summa cum laude) from the New Jersey Institute of Technology (NJIT), Newark, in 1982, an M.S.E.E. degree from the University of Michigan, Ann Arbor, in 1983, and a Ph.D. degree from Purdue University, West Lafayette, Indiana, in 1988. He joined NJIT's Department of Electrical and Computer Engineering as an assistant professor in 1988 and has been a full professor since 1997. He has also assumed various administrative positions including his current appointment as the Newark College of Engineering's Associate Dean for Research and Graduate Studies at NJIT. His current research focuses on various aspects of broadband networks and multimedia communications. He authored *Computational Intelligence for Optimization* (Springer, 1997, translated into Chinese in 2000) with E. S. H. Hou, and edited *Neural Networks in Telecommunications* (Springer, 1994) with B. Yuhas. He also has contributed approximately 300 technical papers including over 100 refereed journal/magazine articles. He is a Senior Technical Editor of *IEEE Communications Magazine* and also serves on the editorial board of *Computer Communications*, the *ETRI Journal*, and the *Journal of Computing and Information Technology*. He was the founding general chair of the first IEEE International Conference on Information Technology: Research and Education (ITRE '03); was

instrumental, while serving as its Chapter Chair, in rejuvenating the North Jersey Chapter of the IEEE Communications Society, which received the 1996 Chapter of the Year Award and a 2003 Chapter Achievement Award; served as chair of the IEEE North Jersey Section and in the IEEE Region 1 Board of Governors during 2001–02; and has been serving in various IEEE committees such as Vice-Chair of IEEE COMSOC Technical Committee on Ad Hoc and Sensor Networks and (TPC) Chair/Vice-chair of several conferences/symposia. He has been invited frequently to deliver keynote addresses, distinguished lectures, tutorials, and talks. His awards and recognitions include the NJIT Excellence Teaching Award in Graduate Instruction (1998), IEEE Region 1 Award (1999), and designation as an IEEE Communications Society Distinguished Lecturer.

Chao Zhang [S'07] (cz2@njit.edu) received an M.S. degree in physics from Fudan University in 1997 and an M.S. degree in computer science from NJIT in 2002. He is currently a doctoral candidate in electrical engineering at NJIT. His current research interest focuses on wireless networking with emphasis on ad hoc and sensor networks.

ROBERTO ROJAS-CESSA [S'97, M'01] (rojasces@njit.edu) received a B.S. degree in electronic instrumentation from the University of Veracruz, Mexico. He graduated with an honors diploma. He received an M.S. degree in electrical engineering from Centro de Investigacion y de Estudios Avanzados del Instituto Politecnico Nacional, Mexico City, an M.S. degree in computer engineering, and a Ph.D. degree in electrical engineering from Polytechnic University of New York, Brooklyn. He was at the Sapporo Electronics Center, Japan, for a Microelectronics certification. Currently, he is an associate professor at the Department of Electrical and Computer Engineering, NJIT. He has been involved in ASIC design for biomedical applications, scheduling schemes for high-speed packet switches, and switch reliability. His research interests include high-speed and high-performance switching, computer networks, fault tolerance, and implementable scheduling algorithms for packet switches/routers. He is also a member of the Institute of Electrical, Information and Communications Engineers (IEICE).

SWADES DE (swadesd@hotmail.com) received his B.Tech in radiophysics and electronics from the University of Calcutta, India, in 1993, his M.Tech in optoelectronics and optical communication from the Indian Institute of Technology (IIT) Delhi, in 1998, and his Ph.D. in electrical engineering from the State University of New York at Buffalo in 2004. Before moving to IIT Delhi in 2007, where he is an assistant professor of electrical engineering, he was an assistant professor of electrical and computer engineering at NJIT (2004–2007). His research interests include performance study, resource efficiency in multihop wireless and high-speed networks, integrated wireless technologies, and communication and systems issues in optical networks. He also worked as a post-doctoral researcher at ISTI-CNR, Pisa, Italy (2004), and has five years industry experience in India in telecommunication hardware and software development (1993–1997).

PITIPATANA SAKARINDR [S'05] (ps6@njit.edu) received his B.E. from King Mongkut's Institute of Technology, Ladkrabang, Bangkok, Thailand, in 1999, and his M.S. in computer engineering from NJIT in 2002. Currently, he is pursuing a Ph.D. degree in electrical engineering from NJIT. His current research focuses on various aspects of network security, including secure group communications, security enhanced QoS, anonymous networks, and trust and reputation systems.

EDWIN HOU [S'82, M'89, SM'98] (hou@njit.edu) received a B.S. degrees in electrical engineering and computer engineering from the University of Michigan in 1982. He received an M.S. degree in computer science from Stanford University in 1984 and a Ph.D. degree in electrical engineering from Purdue University in 1989. He joined the NJIT faculty that year as an assistant professor and is now an associate professor in the Department of Electrical and Computer Engineering. Since 1999 he is also the associate chair for undergraduate studies of the department. His research interests include autonomous vehicles, nonlinear optimization, network intrusion detection, infrared imaging, genetic algorithms, scheduling, computer arithmetic, and neural networks. He has authored or co-authored more than 50 technical papers and book chapters in his research areas. He is also a co-author of the book *Computational Intelligence for Optimization* (Kluwer, 1997). He has participated in research grants in excess of $1 million as PI or co-PI. He was the recipient of the 1999-2000 NJIT Excellence Teaching Award in Graduate Instruction and the 2004 Newark College of Engineering Excellence in Advising Award. He is a member of Sigma Xi, IEEE, Tau Beta Pi, and Eta Kappa Nu.