

Robust Communications using Wireless Mesh Networks for Safeguarding Water Infrastructures

Saad Khan¹, Asad Amir Pirzada¹ and Marius Portmann^{1,2}

¹Queensland Research Laboratory, National ICT Australia Limited, Brisbane, QLD 4000, Australia

²School of ITEE, The University of Queensland, Brisbane, QLD 4072, Australia
{Saad.Khan, Asad.Pirzada, Marius.Portmann}@nicta.com.au

Abstract

Since ancient times, water has been considered a vital resource for the survivability of nations. It is a resource that calls for impregnable security and incessant protection. Water infrastructures generally consist of dams and associated water-supply systems. These infrastructures are vulnerable to a number of natural and man-made disasters. The threat of natural calamities such as cyclones, earthquakes and tsunamis and man-made disasters like terrorist attacks are now more imminent than ever. In spite of these facts, water infrastructures are still being provided with meagre communication support like land-lines and mobile phones for use in normal and emergency scenarios. These communication resources are in fact vulnerable to the very same catastrophes as those threatening the water infrastructures. In this paper we present a communication infrastructure based on wireless mesh networks, which can satisfy the two main communication requirements of any water infrastructure, i.e. surveillance and crisis communications. This paper has been mainly written with Australian water infrastructures in mind. However, emphasis is made on the application of the proposed communication network being applicable to any water infrastructure. We argue that wireless mesh networks can provide the requisite dual-role communication functionality for water infrastructures, even in the advent of severe calamities or disasters.

Keywords—Security, Wireless Mesh Networks, Communication

1. Introduction

Water infrastructure is a key component of a nation's assets. Damage to or destruction of a nation's water supply infrastructure by natural disasters or terrorist attacks could have disastrous effects, disrupting the distribution of vital human services, threatening public health and the environment, and possibly causing loss of life [1]. There are approximately 500 large dams in Australia with a total storage capacity of almost 170 times the volume of the Sydney Harbour [2], a small percentage providing the majority of supplies. Manned or unmanned, these dams represent a critical element on which the Australian people rely for safety, public health and economic vitality.

So far, water infrastructure safety has mainly been evaluated in terms of structural and hydraulic stability with respect to natural forces [3], such as major storms, earthquakes, cyclones and resulting floods. When considering the risk of deliberate threats, the focus is generally directed towards purposeful acts of vandalism or theft, rather than malevolent threats by terrorists, which is rapidly becoming a concern in today's society. Physical destruction to any of these systems, whether natural or manmade, could include the disruption of operating or distribution system components,

power or electronic control structures, actual damage to reservoirs and pumping stations, or loss of telecommunication systems.

Currently, Australia requires the owners of its dams to implement Dam Safety Management Guidelines under the Australian Water Act 2000 [4] to minimise the risk of a dam failure, and to protect life and property from the effects of such a failure. A Dam Safety Management Program comprises policies, procedures and investigations which minimises the risk of dam failure [5]. This is divided into two sections under the Dam Safety Code provided by the statutory body of Independent Competition and Regulatory Commission [6]. These include:

- Dam Surveillance and
- Dam Safety Emergencies.

Dam Surveillance encompasses routine checks, annual and 5-yearly, along with security surveillance by video cameras and regular inspections. In the event of a Dam Safety Emergency, an Emergency Action Plan (EAP) is carried out that incorporates the evaluation of severity of the emergency and the subsequent notification to relevant parties.

By far the most crucial procedure in this process is the notification of police, emergency services, consulting engineers, department of Natural Resources and Environment, and down stream neighbours. The goal is to prevent or minimise any loss of life and property. In such a case, various authorities need to be notified, located upstream/downstream of the dam, as well as in other potentially affected areas. Under the current common practices in Australia, these warnings are generally delivered through commercial landline-based telephony and mobile phones [7].

There are a number of major challenges associated with the notification process currently implemented in Australia. Loss of communication infrastructure such as communication cables, telephone exchanges, and mobile phone towers during a storm, flood or earthquake leaves the current communication system incapacitated. As has been demonstrated during recent disasters, high traffic demands during large scale emergencies lead to overload and, therefore, unavailability of these telecommunication systems to emergency response personnel and other persons involved in managing the disaster. A further concern is the vulnerability of these telecommunication systems to deliberate attacks by terrorists with the aim to hamper rescue operations.

In this paper, we discuss wireless mesh networks as a potential technology to provide communications services for water infrastructure safety, for both day-to-day operations as well as during emergencies. Requirements for emergency communications as well as existing and alternative systems for

Dam Safety Emergencies and Dam Surveillance across water infrastructure are discussed in Section 2. Section 3 and 4 provide background on wireless mesh network technology and its application to communication for water infrastructure protection, respectively. Finally, conclusions and recommendations are presented in Section 5.

2. Communication Requirements

Natural and manmade disasters typically occur unexpectedly, without much time for the dissemination of warning messages. Organisation and co-ordination of essential recovery services requires rapid response to save lives and restore the community infrastructure. During these events, severe stress is placed on telecommunication systems due to high traffic demands and infrastructure damage.

The Tampere Convention on the Provision of Telecommunication Resources for Disaster mitigation and Relief Operations points out the following in the United Nations Treaty Series [8]:

“The States Parties shall...facilitate the use of telecommunication resources for disaster mitigation and relief. Such use may include, but is not limited to; ...c) the provision of prompt telecommunication assistance to mitigate the impact of a disaster; and d) the installation and operation of reliable, flexible telecommunication resources to be used by humanitarian relief and assistance organizations.”

This illustrates the many dimensions that need to be addressed to achieve an effective solution for emergency telecommunications. The system needs to be robust, demonstrating an ability to recover gracefully from a whole range of failure and overload situations. Inbuilt redundancy within a system and the ability to self-heal are required to be able to provide a reliable and effective communication platform for a wide range of voice and data services.

Interoperability between communication systems used by various emergency response teams and organisations has also been identified as a critical requirement for the efficient management of disaster situations.

The different requirements and problems of existing and alternative approaches to communications for Dam Safety Emergencies and Dam Surveillance are considered below.

2.1 Dam Surveillance

Routine checks of dams are conducted throughout the year by the dam owners, as required by the Dam Safety Management program. Dams require physical security of their structure and components as well as technical security, such as monitoring of sensor data and equipment.

Physical security of dams can be provided through security personnel services or video surveillance. Both of these methods utilise one of the following communication means to relay their information back to the required facility, professional mobile radio (PMR), a local area network (LAN), e.g. Ethernet, or traditional landline-based telephony.

Technical security of dams includes regular inspections and monitoring of physical data and onsite equipment. Inspections are usually carried out by personnel and monitoring is conducted through Supervisory Control and

Data Acquisition (SCADA) systems. Relay of technical security information is typically done through wired local area networks if available or via the public switched telephone network. (phone or fax). Some of these systems lack the bandwidth capacity of data intensive applications such as video surveillance. These communications systems suffer from various limitations and vulnerabilities, as outlined in Table 1.

Table 1; Surveillance Scenarios, communication means and limitations of existing communication infrastructure

Scenarios	Communication Means	Limitations
Physical Security <ul style="list-style-type: none"> ➤ Personnel asset protection service ➤ Video Surveillance 	<ol style="list-style-type: none"> 1. Professional Mobile Radio (PMR) 2. Ethernet 3. Landlines 4. Mobile Phones 	<ul style="list-style-type: none"> ➤ PMR has limited range and suffer from interoperability problems ➤ Limited bandwidth
Technical Security <ul style="list-style-type: none"> ➤ Inspections ➤ Monitoring <ul style="list-style-type: none"> - Equipment - Assets 	<ol style="list-style-type: none"> 1. SCADA network 2. Ethernet 3. Landlines (phone and fax) 5. Mobile Phones 	<ul style="list-style-type: none"> ➤ Mobile phone networks have limited coverage and limited reliability in disaster situations. ➤ All systems are highly vulnerable to tampering ➤ SCADA networks have security problems

PMR systems have limited point to point ranges, and the installation of radio relays is time consuming and costly. Use of incompatible equipment or radio channels provides serious interoperability problems. Landline-based infrastructure as well as wired local area networks are vulnerable to tampering through planned and co-ordinated attacks. The lack of redundancy in these systems limits their ability to recover from failure of individual components. The loss of a single telephony exchange or mobile phone tower can result in the complete loss of communication for a large group of users.

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control chemical, physical or transport processes. These monitoring capabilities are often required by corporate personnel through remote access. This encourages many utilities to establish connections to the SCADA system to enable engineers to monitor and control the system via the corporate network. These connections are often implemented without addressing security risks. Security strategies for utility corporate network infrastructures rarely account for the fact that access to these systems might allow unauthorised access and control of SCADA systems, creating a most vulnerable system [9].

It is thus evident that the currently implemented communication systems used for dam surveillance do not offer the required capacity, reliability, flexibility and interoperability for seamless and efficient transfer of information. We therefore consider Wireless Mesh Networks as an alternative technology that can meet most of these requirements.

2.2 Dam Safety Emergencies

Throughout history, in all parts of the world, dams built to store water have occasionally failed and discharged the stored waters to inflict sometimes great damage in terms of loss of lives and property [10]. The process that takes place during an

emergency follows the particular order: visual recognition of problem, determination of amplitude of problem by authorised personnel, and transmission of relevant information to appropriate parties and authorities upstream and downstream. Determining whether there is a critical emergency or not requires time. Creating a false panic in nearby towns with limited emergency response resources is a costly mistake. The limited amount of time that is typically available to inform emergency response units and decision makers further emphasises the importance of a reliable and efficient communication system.

The communication that takes place in a dam safety emergency follows a pre-described process. Figure 1 shows a simplified generic notification process tree which needs to be followed during an emergency. Often, an observer is first to notify the dam operator, who in turn makes the decision whether or not the dam is in a critical state. If a dam failure is imminent, his/her duty is to notify the upstream and downstream dams, the downstream residents (in part) and the dam manager. The dam manager is then responsible for notifying various other response units and managers and this process continues.

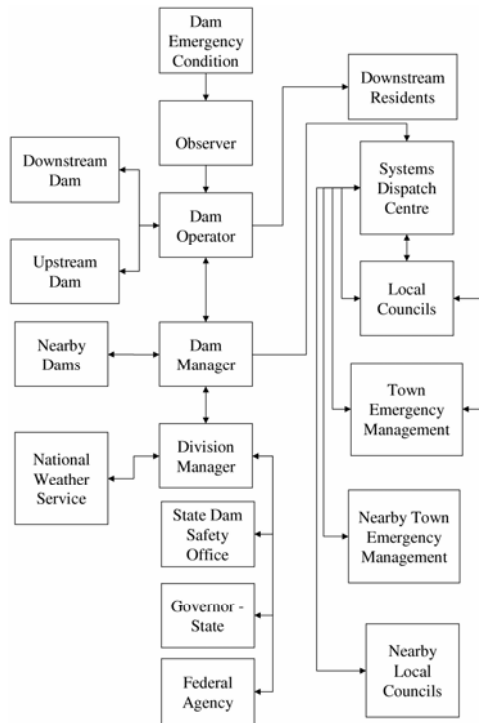


Figure 1: Notification Process Tree during a Dam Emergency

The notification that occurs after the decision about the criticality of the infrastructure needs to occur rapidly. However, the current communication systems that are generally being utilised are local telecommunication lines, mobile phones and in some cases PMR radio systems. These systems have immense infrastructure problems during various emergency situations. The vulnerability issues associated with the common communication facilities provided on water infrastructure, during an emergency, are listed in Table 2.

Generally, the communication systems used for regular Dam Surveillance are the same ones used during Dam Safety Emergencies. This means that most of the vulnerabilities that are present in communication systems used for Dam Surveillance are also present during Emergencies, along with a few more.

Table 2; Emergency scenarios, communication means and vulnerabilities with existing communication infrastructure

Scenarios	Communication Means	Vulnerability
Sunny Day Failure; <ul style="list-style-type: none"> ⇒ Earthquake ⇒ Technical Failure ⇒ Piping Effect 	All scenarios use; <ol style="list-style-type: none"> 1. PMR 2. Landlines 3. Mobile Phones 4. Fax 5. Ethernet - Email 	<ul style="list-style-type: none"> ⇒ Disruption/Destruction of communication infrastructure occurs due to various scenarios ⇒ High traffic demand cause congestion of communication facilities
Cyclone		<ul style="list-style-type: none"> ⇒ Systems are vulnerable to co-ordinated attacks
Flood Event		
Terrorist Attack		

Dam Safety Emergencies, unlike day to day Dam Surveillance, have the risk of natural disasters. Earthquakes cause movement in the ground, potentially destroying landlines and mobile towers leaving the communication facilities incapacitated. Large masses of water from cyclones, flood events or piping failures also contain the potential to eradicate landlines and fixed communication infrastructure, again leaving the communication facilities inadequate for fulfilling their purpose. It is during these times that the communication system is needed the most, and often this is when it fails.

The need for a reliable method to communicate emergency situation information to relevant parties is essential. However, traditional communication systems based on fixed infrastructure fail to meet the reliability requirements during these situations. The current systems also suffer from overload during large scale disaster events.

During emergencies, usage of the public telephone network increases dramatically and results in congestion and service unavailability, which can result in situations where vital information cannot be delivered to its intended destination.

Apart from landline-based phone and mobile phone networks, PMR systems are also used for communication purposes. However, these systems suffer from limited range and interoperability issues, as mentioned previously.

The systems mentioned above do not fulfil the requirements of robustness, redundancy, flexibility and capacity. The current alternate approaches being sought out include the use of satellite phones. However, the cost of these systems is prohibitively high for widespread deployment. Furthermore, they do not provide adequate bandwidth for the transmission of video data and high quality images.

Two different types of satellite phones are currently available in Australia, geostationary services and low earth orbit (LEO) systems. Geostationary service satellite phones are relatively large units and hence have limited mobility. These systems also require a clear view of the sky during use, and can, therefore, become ineffective during an emergency situation.

LEO systems have smaller footprints and utilise high speed satellites. This requires more satellites as frequent handoff occurs depending on which one enters and leaves the field of view [11]. The continuous availability of the communication link, especially for data communication, has been reported as a major problem. Overall, satellite phones are very expensive, lack reliability and the required capacity for high bandwidth applications such as video.

3. Wireless Mesh Networks

Wireless Mesh Networks (WMNs) are a type of wireless ad-hoc networks that do not require a wired backbone infrastructure. Ironically, the biggest cost of deploying a wireless network covering a larger area is the installation of the wired backbone infrastructure that interconnects the wireless access points. In WMNs, the wired backbone is replaced via wireless multi-hop communication. Due to their mesh topology, WMNs have a high level of redundancy. Furthermore, these networks have the ability to self-organise and self-heal, and are, therefore, able to cope with failures and loss of parts of the network.

WMNs consist of two types of wireless nodes, Mesh Routers and Mesh Clients [12]. Mesh Routers typically have minimal mobility and form the backbone of WMNs. Mesh Clients are typically mobile computing devices such as PDAs, with limited computing, communication and power resources. Figure 2 shows an example WMN network, where all links are wireless.

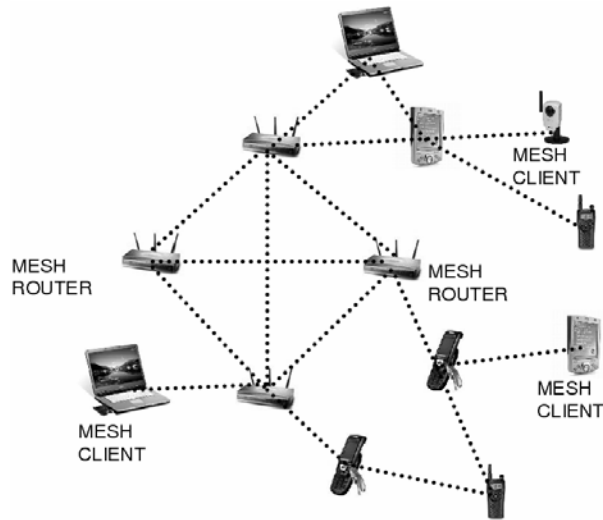


Figure 2: A simplified mesh network

The three main types of WMNs are Infrastructure, Client and Hybrid. Infrastructure WMNs are comprised of passive Mesh Clients that utilise Mesh Routers to access a backhaul network. Thus, all Mesh Clients construct links with Mesh Routers via a single wireless hop and are not involved in the relaying of other nodes traffic. A Client WMN consists exclusively of Mesh Clients communicating with each other directly, without any involvement of Mesh Routers. The most generic type of WMNs is the hybrid WMN. A hybrid WMN is an amalgamation of the two previous types to form a robust and reliable system, providing a network where both Mesh Routers and Mesh Clients are actively involved in the routing and forwarding of packets.

The WMN formation requires no manual intervention or configuration. Its ability to self-organise and self-heal creates an autonomous structure, requiring little attention during times it is needed most. Their ability to integrate into existing networks and communication systems, to provide high data rates under high load and their excellent robustness and failure tolerance make WMNs a promising technology for a wide range of applications [13], including dam safety communication.

4. Water Infrastructure Applications

Currently, basic communication technology is employed for dam surveillance and emergency communication. Table 1 and Table 2 show the communication means utilised and their limitations and vulnerabilities during various scenarios. It is evident that these communication systems have significant deficiencies in a number of aspects for the considered application. WMNs overcome most of these limitations and provide a cost-effective, reliable and robust alternative.

Table 3 provides a summary of the existing limitations of current communication systems and how WMNs are able to overcome these.

Table 3: Application of WMN systems to solve existing limitations in communication systems for water infrastructure protection

Existing Limitations	WMN capability that address limitations	Outcome achieved by implementing WMNs
1. Limited range 2. Limited Coverage	↻ Multi-Hop Wireless Communication	↻ Coverage of large areas
3. Limited Robustness and fault tolerance	↻ Redundancy of mesh topology ↻ Self-healing capability	↻ Provision of continuous communication resources during an emergency
4. High traffic Demands	↻ Ability to support high bandwidth applications ↻ Ability to dynamically adapt and re-configure ↻ Load balancing capability	↻ Reliable support for real-time video transmission
5. Non-interoperability	↻ Integration ↻ Multiple types of network access	↻ Communication with existing systems
6. Security	↻ Layered security	↻ Secure transfer of information within corporate utilities

WMNs can be used for both dam surveillance and dam safety emergencies. Figure 3 shows a simple representation of WMN application in the vicinity of a dam. Dam surveillance is conducted on a regular basis, and often personnel are required to monitor and transfer information through conventional communication means to relevant authorities. Deployment of a WMN would reduce the need for regular personnel checks, which would be replaced by fixed wireless video cameras interconnected via a WMN, as shown in Figure 3.

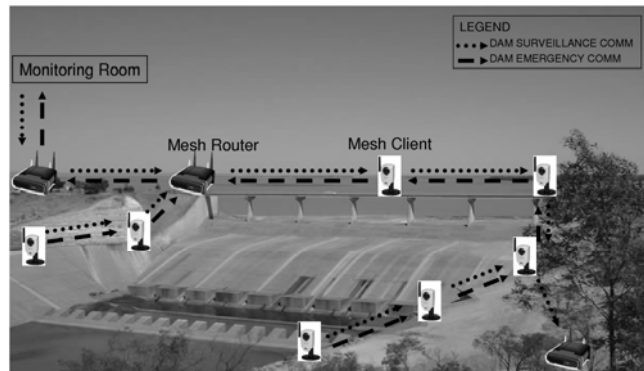


Figure 3: Representation of WMN application in the vicinity of a dam.

The video cameras could then transfer high quality video streaming to a monitoring room. Physical security of the dam structure and its components as well as technical security such as monitoring of data and equipment itself can be achieved through the use of a WMN and wireless video cameras. This would be particularly useful in the case of unmanned dams.

During dam surveillance, mobile phones are often out of coverage due to the remoteness of many dams. As mentioned earlier, WMN offer non-line-of-sight connectivity and routing. Coverage problems are solved by this characteristic of WMN as a client may access the monitoring room and hence video feedback on a PDA by connecting to the nearest router. Due to the multi-hop system, the client need not be directly in-line-of-sight of the monitoring room itself to receive data. The use of the Internet Protocol (IP) as a common platform solves the problem of interoperability and allows integration with a wide range of networks and systems, including SCADA systems.

During surveillance, the existing systems are highly vulnerable to intentional tampering, especially SCADA systems. Along with this, destruction of fixed communication infrastructure such as telephone exchanges or cables can potentially leave a dam site isolated over long time periods during an emergency. WMNs employ a wireless network which is resilient to failure and to intentional tampering. Its high level of redundancy and self-healing ability allows the communication system to choose alternate paths for its communication, allowing it to maintain connectivity in the event of node and link failures.

WMNs also allow for deployment of internal corporate and external security. Security on different levels can allow a SCADA and video surveillance system to work separately from general communication means for all personnel using the same WMN.

Dam safety emergencies present numerous limitations and vulnerabilities of current communications systems which can be largely overcome by WMNs. During an emergency scenario such as an earthquake, cyclone or flood event, disruption or even destruction of communication infrastructure such as landlines can render communication infrastructure incapacitated. In such a case, extending the coverage of a network for limited range devices may be necessary. The multi-hop system of a WMN allows incremental deployment, one node at a time. This means that as more nodes are deployed, the reliability and connectivity for the users increase accordingly. This capability of a WMN permits for a high coverage area network utilising minimal resources.

Due to a wireless infrastructure/backbone, the WMNs form a completely resilient and redundant system. Destruction in part or in whole or any of the system will not effect the communication at all. The system will simply alter the routing of the information to account for the missing or malfunctioned component. Since there are multiple links between the mesh routers, losing one will not affect the transfer of information as an alternate data route can be taken.

During a dam emergency, one of the problems with the communication facilities is their lack of adaptability for high traffic demand. Facilities currently provided for remote dams often lack the ability to facilitate heavy congestion, as thousands of people upstream and downstream are also using the same facilities. Mesh routers can be configured to

perform load balancing and prioritisation to solve the problems incurred during high traffic demand.

Lastly, dam emergencies can also be manmade, and may include co-ordinated attacks. The current communication systems employed for dam emergencies are the same as those for dam surveillance and are prone to intentional tampering and attacks.

Security in WMNs can be implemented via a wide range of existing and proven mechanisms and protocols, and can be applied at multiple layers of the network. Examples include link layer encryption, virtual private networks and application layer security. This along with the high level of redundancy and self-healing capabilities also provide WMNs with resilience against malicious attacks.

5. Conclusions

WMNs provide an alternative communications technology for water infrastructure protection that overcomes many of the limitations of currently used systems. As required by the Tampere Convention; WMNs provide prompt telecommunication assistance to mitigate the impact of a disaster as well as offering a reliable and flexible telecommunication resource to be used by humanitarian relief and assistance organisations. The system is robust; demonstrating an ability to recover gracefully from a whole range of exceptional inputs and situations in a given environment. Redundancy and autonomous execution make WMNs flexible and reliable in a range of given scenarios, adding to their ability to transfer high quality data quickly and efficiently even in high traffic demand situations. Their simple installation and low maintenance are added benefits to their low cost. WMNs can serve a dual purpose, for regular dam surveillance in day to day operations, and their use as a backup system for dam emergency situations. This will solve the vulnerabilities evident in the current communications systems employed on water infrastructure.

References

- [1] C. Copeland and B. Cody, "Terrorism and Security Facing the Water Infrastructure Sector," *Congressional Research Service*, 2005.
- [2] "Water use - Australian economy consumes 50 Sydney harbour's," *Australian Bureau of Statistics*, <http://www.abs.gov.au/ausstats>, 2004.
- [3] R. Grismala, "Infrastructure Safety," *ICF Consulting*, 2005.
- [4] "Water Act 2000," *State of Queensland*, www.legislation.qld.gov.au/LEGISLTN/ACTS/2000/00AC034.pdf, 2000.
- [5] "Dam Safety Management Guidelines," *Queensland Government - Natural Resources and Mines*, 2002.
- [6] "Dam Safety Code," *Australian Capital Territory*, 2003.
- [7] "DAM Safety Emergency Plan " *Department of Sustainability and Environment Victoria*, 2002.
- [8] "Tampere Convention on the Provision of Telecommunication Resources for Disaster mitigation and Relief Operations," *International Conference on Emergency Telecommunications*, 2006.
- [9] R. Inc, "Understanding SCADA System Security Vulnerabilities," 2001.
- [10] FEMA, "The National Dam Safety Program: 25 years of excellence," *U.S. Department of Homeland Security*, 2006.
- [11] N. Chandran and M. C. Valenti, "Three generations of cellular wireless systems," *IEEE Potentials*, vol. 20, pp. 32-35, 2001.
- [12] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Computer Networks*, vol. 47, pp. 445-487, 2005.
- [13] A. A. Pirzada, M. Portmann, and J. Indulska, "Evaluation of MultiRadio Extensions to AODV for Wireless Mesh Networks," *Proceedings of the 4th ACM International Workshop on Mobility Management and Wireless Access (MobiWac)*, pp. 45-51, 2006.