ISSN 2229-5518

# Secure Multicast Routing in Wireless Mesh Networks against Sybil Attack

Dhivya.J Assistant Professor
*Department of Electronics and Communication Engineering*
*Tagore Engineering College, Chennai.*
*dhivijana5@gmail.com*

**Abstract**— **Wireless Mesh Networks (WMNs) have become one of the important domains in wireless communications. They comprise of a number of static wireless routers which form an access network for end users to IP-based services. In this paper, an efficient and secure multicast routing on such wireless mesh networks is concentrated. This paper identify novel attacks against high throughput multicast protocols in wireless mesh networks through S-ODMRP protocol. Recently, Sybil attack is observed to be the most harmful attack in WMNs, where a node illegitimately claims multiple identities. This paper systematically analyzes the threat posed by the Sybil attack to WMS. The Sybil attack is encountered by the defense mechanism called Random Key Predistribution technique (RKP). The performance of the proposed approach which integrates the S-ODMRP and RKP is evaluated using the throughput performance metric. It is observed from the experimental result that the proposed approach provides good security against Sybil attack with very high throughput.**

**Index Terms**—**Random Key Predistribution, Sybil attack, WMS,S-ODMRP, throughput.**

## 1 Introduction

Wireless Mesh Networking is a rising technology since it offers low-cost high bandwidth community services that supports several vital applications such as Internet access provisioning in rural areas, municipal and metropolitan networking for emergency and disaster recovery, security surveillance, and information services in public transportation systems [1],[2]. The main components of a WMN comprises of wireless mesh routers, wireless hosts (e.g., PCs, laptops, etc.,), and access points (or gateways) that act both as Internet routers and wireless mesh routers. The mesh routers in a WMN offer multihop connectivity from one host to another, or to the Internet through the access points. The routers automatically set up and maintain mesh connectivity among themselves, making WMNs dynamically self-organized and self-configured networks [3]. This characteristic feature brings several advantages to WMNs such as low installation cost, large-scale deployment, reliability, and self-management.

Multicast is a vital technology for future wireless networks [4]. It offers competent communications among a group of nodes, and assists at minimizing the bandwidth consumption of several applications and services such as service discovery, videoconferencing, distributed gaming, etc. This is especially suitable in wireless environments where bandwidth is limited and several users are sharing the same wireless channels. Especially, for WMNs, multicast can denote a vast improvement of the network capacity by considering the benefit of links which can be shared by multiple users to receive the same data, which is transmitted only once.The nodes occasionally send probes to their neighbors to compute the quality of their adjacent links in a classic high-throughput multicast protocol. High-throughput protocols [5], [6] need the nodes to collaborate to derive the path metric, thus depending on the assumption that nodes behave correctly during metric computation and propagation.But, this hypothesis is hard to assure in wireless networks that are vulnerable to attacks due to nature of the medium and the multihop characteristic of the communication. Several vulnerabilities are present in the protocols foe WMNs. These vulnerabilities can be utilized by the attackers to decrease the performance of the network. The nodes in a WMN depend on the cooperation of the other nodes in the network. As a result, the MAC layer and the network layer protocols for these networks generally assume that the participating nodes are trustworthy and well-behaving with no malicious intentions. But, certain nodes in a WMN may act in a selfish manner or may be compromised by malicious users. The lack of accountability due to the absence of a central administrator make the MAC and the network layer protocols vulnerable to several types of attacks.

This paper mainly focuses on the Sybil attacks in WMNs. In the Sybil attack [7], a malicious node behaves as if it were a larger number of nodes, for instance by impersonating other nodes or simply by claiming false identities. In the worst case, an attacker may construct a random number of additional node identities, using only one physical device.

There has been various research work on using high throughput metrics to enhance performance in wireless networks but the investigations on the security implications is relatively rare. The earlier researches mainly concentrated on vulnerabilities of unicast routing protocols that use hop count as a metric [8], [9] and [10]. This work focuses on the secure high-throughput multicast routing in WMNs through S-ODMRP and Random Pre Key distribution (RKP).

## 2 Literature Survey

Security in WMN is critical for the deployment of various wireless services. Jing Dong et al., [11] focused on providing data confidentiality for group communications in WMNs. The author proposed a novel protocol framework called Secure Group Overlay Multicast (SeGrOM) that make use of decentralized group membership, supports localized communication, and utilizes the wireless broadcast nature to attain competent and secure group communication. The author examined the performance and discussed the security properties of the protocols. The author demonstrated through simulations that the proposed protocols provide good performance and incur a significantly smaller overhead than a baseline centralized protocol optimized for WMNs.

## 3 Routing Techniques in High-Throughput Multicast Networks

A multihop wireless network is considered where nodes take part in the data forwarding process for other nodes. A mesh-based multicast routing protocol is considered which sustains a mesh connecting multicast sources and receivers. Path selection is carried out depending on a metric considered to maximize throughput.

### 3.1 Overview of Metrics to attain High-Throughput

Conventionally, routing protocols have used hop count as a path selection metric. In static networks, this metric is observed to attain suboptimal throughput as paths likely to include lossy wireless links [13] and [14]. Thus, recently, the focus has shifted toward high-throughput metrics that look for to maximize throughput by choosing paths depemding on the quality of wireless links [15]. In such metrics, the quality of the links to/from a node's neighbors is calculated by periodic probing. The metric for a whole path is attained by aggregating the metrics reported by the nodes on the path.

Several high-throughput metrics [16] for multicast were available in the literature. Most of these metrics are adaptations of unicast metrics to the multicast setting by considering the basic differences between unicast and multicast communication. Transmissions in multicast are less consistent than in unicast for several reasons. A packet in unicast is sent reliably using link-layer unicast transmission, which comprises of link-layer acknowledgments and probably packet retransmissions; but in multicast, a packet is sent unreliably using link-layer broadcast, which does not include link-layer acknowledgments or data retransmissions. Additionally, unicast transmissions are preceded by a RTS/CTS exchange where as in multicast, there is no RTS/CTS exchange, which increases collision probability and decreases transmission reliability. Thus, this research mainly focuses on the multicast transmission and its security. Security has become a vital factor in multicast routing. Several attacks are available in the WMNs. This research mainly focuses on the Sybil attack and its defense mechanisms.

### 3.2 High-Throughput Routing in Mesh-Based Multicast Networks

Mesh based multicast protocols (e.g., ODMRP [17]) generate more resilient data paths, but have higher overhead due to redundant retransmissions. ODMRP is an on-demand multicast routing protocol for MWNs, which uses a mesh of nodes for each multicast group. The source periodically recreates the mesh by flooding a JOIN QUERY message in the network to refresh the membership information and update the routes. In this approach, a protocol called ODMRP-HT which enhances ODMRP with high-throughput metrics is proposed.

ODMRP-HT and ODMRP are different in the following ways: rather than selecting routes based on minimum delay (which results in choosing the fastest routes), ODMRP-HT chooses routes based on a link-quality metric, and moreover, ODMRP-HT uses a weighted flood suppression mechanism to flood JOIN QUERY messages instead of using basic flood suppression.

### 3.3.Secure Multicast Routing Protocol (S- ODMRP)

This paper uses a secure multicast routing protocol, S-ODMRP through a novel defense scheme RateGuard to accommodate high-throughput metrics.S-ODMRP assures the delivery of data from the source to the multicast receivers even in the existence of Byzantine attackers, provided the receivers are reachable via non-adversarial paths [1].

In order to attain this, S-ODMRP uses a integration of authentication and rate limiting approaches against resource consumption attacks and a novel approach, RateGuard, against the more tough packet dropping and mesh structure attacks, comprising metric manipulations and JOIN REPLY dropping.

Source message authentication is used by the S-ODMRP to eliminate processing non-authenticated messages. This avoids a variety of attacks.The attacks on the mesh structure and packet dropping attacks are more challenging to defend, especially, in the context of high-throughput metrics. RateGuard defense scheme is used by the S-ODMRP approach to defend against the attacks. RateGuard depends on the study that in spite of of the attack approach, either by dropping JOIN REPLY, metric manipulations, or by dropping packets, attackers do not affect the multicast protocol unless they cause a drop in the Packet Delivery Ratio (PDR). A reactive technique is adopted in which attacker nodes are identified via a measurement-based detection protocol component, and then isolated through an accusation-based reaction protocol component.
Finally, in order to deal with the metric poisoning effect due to metric manipulation attacks, the metric in the whole network is refreshed shortly after attack detection. In SODMRP, the metric refreshment is achieved automatically through the periodic JOIN QUERY messages.

### 3.4 Mesh Creation in S- ODMRP

The source node S occasionally broadcasts to the whole network a JOIN QUERY message to refresh the membership information and to update the routes. The JOIN QUERY message is signed by S and is propagated through a weighted flood suppression approach. Nodes that have legitimate signatures alone process JOIN QUERY messages and that are obtained from nodes not accused presently.The JOIN REPLY messages are then sent from receivers back to S along optimal paths as defined by the high throughput metric, leading to the creation of the FORWARDING GROUP (the multicast mesh). This guarantees that good paths are still used, even if legal nodes on these paths are incorrectly accused.

### 3.5 Limitations of S-ODMRP

S-ODMRP limits a node to blame at most one other node at a time. This shows that attacker nodes should be a minority in the network. Alternatively, some attacker nodes will be left unaccused and will be susceptible to attacks and deny service to many receivers through metric manipulation. Moreover, this approach is not suitable for the Sybil attacks. To overcome the above limitations, this research work uses Random Key Pre-distribution (RKP) technique is integrated with the S-ODMRP to defend against the Sybil attacks.
This paper provides the details against high-throughput multicast protocols.

## 4 Sybil Attack Overview

Sybil attack is defined as a malicious device illicitly taking on multiple identities. A malicious device's additional identities are referred to as Sybil nodes. In order to better understand the implications of the Sybil attack taxonomy is developed of its different forms. Three orthogonal dimensions such as direct vs indirect communication, fabricated vs stolen identities, and simultaneity are considered in this approach.

Dimension I: Direct vs. Indirect Communication

Direct Communication: One way to carry out the Sybil attack is for the Sybil nodes to communicate directly with legitimate nodes. When a genuine node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Similarly, messages sent from Sybil nodes are in fact sent from one of the malicious devices.
Indirect Communication: In this version of the attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed via one of these malicious nodes, which make up to pass on the message to a Sybil node.

Dimension II: Fabricated vs. Stolen Identities
A Sybil node can obtain an identity in one of two ways. It can make a new identity, or it can take an identity from a genuine node.
Fabricated Identities: In some scenarios, the attacker can simply generate random new Sybil identities. For instance, if each node is identified by a 32-bit integer, the attacker can simply allocate each Sybil node a random 32-bit value.
Stolen Identities: Given a method to identify genuine node identities, an attacker cannot fabricate new identities. For instance, suppose the name space is deliberately limited to prevent attackers from inserting new identities. In this scenario, the attacker requires to assign other legitimate identities to Sybil nodes. This identity theft may go undetected if the attacker demolishes or temporarily disables the impersonated nodes.
This section describes about the Sybil attack that can be used to attack several types of protocols in WMNs. There are various types of attacks available in the literature. For example, the attacks on distributed storage algorithms are similar to the algorithms described by Douceur [17] in the peer-to-peer environment. Then, attacks on routing algorithms are described by Karlof and Wagner [18]. The novel attacks on data aggregation, voting, fair resource allocation, and misbehavior detection algorithms are also present in the literature.
This paper mainly focuses on the Sybil attacks on routing. Karlof and Wagner [18] described that the Sybil attack can be used against routing algorithms in WMNs. One vulnerable method is multipath routing where apparently disjoint paths could in fact go through a single malicious node presenting many Sybil identities. Another vulnerable mechanism is geographic routing [19],[20] where rather than having one group of coordinates, a Sybil node could appear in more than one place at once.

### 4.1 Defense Mechanism

In order to defend against the Sybil attack, it is essential to validate that each node identity is the only identity presented by the equivalent physical node. There are two ways to validate an identity. The first type is direct validation, in which a node directly tests the validity of another node identity. The second type is indirect validation, in which nodes that have previously been verified are permitted to guarantee for other nodes. With the exception of the key pool defense, the mechanisms are presented for direct validation. This paper proposes a new defense called Random Key Pre distribution against the Sybil attack in WMN.

i. *Random Key Pre-distribution (RKP)*

Recently, researchers proposed a capable approach for key distribution in WMNs: random key pre-distribution [21]. These approaches facilitate nodes to create secure links to other nodes. In this section, the mechanism of the key distribution scheme is presented that is used to defend against the Sybil attack.
In random key pre-distribution, a random group of keys or key-related information to each node is assigned, so that in the key set-up phase, each node can discover or compute the common keys it shares with its neighbors; the common keys will be used as a shared secret session key to ensure node-to-node secrecy.
The main contributions and notions are:
1. Associating the node identity with the keys assigned to the node.
2. Key validation, i.e., the network being capable of verifying segment or all of the keys that an identity claims to possess.
As a result, given a inadequate collection of captured keys, there is slight probability that an randomly generated identity

is going to work, for the keys connected with a arbitrary identity are not likely to have a major intersection with the compromised key set, making it tough for the fabricated identity to pass the key validation.

Again, for key validation, indirect and direct validation is present. In the scenario of direct validation, each node challenges an identity using the inadequate knowledge it possesses and makes a decision independent of other nodes. Thus nodes may not reach a globally consistent decision. With indirect validation, nodes could collaborate in validating a node, thus it is likely to arrive at a globally consistent decision. Obviously, the validation task can be delegated to a central trusted party such as a base station. Indirect key validation is much more costly in terms of communication overhead than the direct case, because in case of direct key validation, if node $ID_i$ tries to validate $ID_j$, messages only need to be exchanged between $ID_i$ and $ID_j$; while in the indirect key validation, it will also involve exchanging messages between other parties. Also indirect validation, if done improperly, could become the victim of blackmail attacks.

But, indirect validation usually offers higher defense against the Sybil attack, because of the memory constraint of WMNs, each individual node has restricted knowledge that it could use to pose a challenge to an identity.Various existing random key pre-distribution approaches comprises of the fundamental key pool approach [21], the single-space pairwise key distribution approaches, and the multi-space pairwise key distribution approaches [22]. So far, researchers have analyzed these approaches in the context of creating secret keys between neighboring nodes. But, in this approach, the above mentioned techniques are used for the purpose of defending against the Sybil attack. An extension to the basic key pool approach is proposed to permit it to defend against the Sybil attack. These techniques are analyzed and studied to show the effectiveness of several key predistribution schemes in defending against the Sybil attack.

The key pool approach randomly assigns k keys to each node from a pool of m keys. During the initialization phase, if any two neighboring nodes identify that they share q common keys, they can set up a secret link.In order to use this approach to defend against the Sybil attack, suppose that each node's identity is the indices in sorted order of the keys that it holds. The main limitation with this technique is that if an attacker compromises multiple nodes, the attacker can use every combination of the compromised keys to construct new identities.

Let $\Omega(ID)\ =\{\mathrm{K}_{\beta 1},\mathrm{K}_{\beta 2},\ldots.,\mathrm{K}_{\beta k}\}$ be the group of keys allotted to ID, where ID represents the identity of node, $\beta_i$ denotes the index of its ith key in the key pool. Now suppose that the group of keys that node ID possesses are determined by $\beta_i = \mathrm{PRF}_{\mathrm{H(ID)}}\,(i)$, where H denotes a hash function, and PRF is a pseudo random function. Thus, the index of a node's ith key is found out by a pseudo random function with H (ID) as the function's key, and $i$ as its input. Similar techniques of selecting keys have been proposed before as an optimization [15]. It is shown that this technique helps to defend against the Sybil attack.

An attacker may try to construct new identities to use in the Sybil attack. For this the attacker will need to capture genuine nodes and read off the keys, thus establishing a compromised key pool S. The attacker will then try to fabricate usable Sybil identities. If a made-up identity $ID'$ can participate in the WMN without being detected in the key initialization phase, it is called as a usable Sybil identity. A usable Sybil identity must be able to pass the validation by other nodes. In order to validate an identity, the verifier challenges the identity by requesting it to prove that it possesses one or more keys it claims to have. If $\exists K_i; K_i \in \Omega\ (ID'); K_i \notin\ S$, and if some genuine entity E in the WMNs knows $K_i$, then E can identify that ID' is cheating by challenging ID' using $K_i$.

### *ii. Single-space Pairwise Key Distribution*

In the random key pool distribution approach, keys can be issued multiple times out of the key pool, and node-to-node authentication is not possible [5]. In the meantime, if an attacker succeeds in capturing a adequate number of nodes, it could compromise a sufficient fraction of keys so that the task of constructing a usable Sybil identity will become trivial.The random pairwise key distribution scheme proposed by Chan et al. guarantees perfect resilience against node capture, i.e., any number of captured nodes show no data about the pairwise keys between genuine nodes. Thus, an opponent cannot fabricate new identities given any number of captured nodes. But, the price is that the network size will be strictly limited by each node's memory constraint the probability that any two nodes are connected p.

### *iii. Multi-space Pairwise Key Distribution*

Recently, researchers have proposed the concept of multiple key spaces to improve the security of single-space techniques. The idea of introducing multiple key spaces can be considered as the grouping of the fundamental key pool approach and the above single space approaches. The setup server randomly constructs a pool of m key spaces each of which has unique private information. Each WMN will be assigned k out of the m key spaces. If two neighboring nodes have one or more key spaces in common, they can compute their pairwise secret key using the equivalent single space approach.

In preventing the Sybil attack, the multi-space scheme exhibits the following properties:

Without validation: Provided a number of captured nodes, if at least one key space is compromised, the node could make up a random number of new identities that could directly communicate with the rest of the network. If none of the key spaces are compromised, it is almost not possible for the opponent to make up any new usable identities to establish a direct communication Sybil attack. But, the network is still prone to the indirect-communication variant of Sybil attack if no validation approach is present.

With validation: If a opponent maintains to have key space $T_i$ which it has not compromised, then a node $ID'$ could challenge the opponent if e $ID'$ has $T_i$ . To do this, $ID'$ simply has to verify whether the opponent has the pairwise key of $T_i$ between the two nodes. Similar to the key pool approach, here indirect validation is essential to guarantee a globally consistent outcome, for it is not assured that any node could successfully challenge an identity given the restricted number of spaces it owns. If full validation is performed, the opponent at least has to compromise k key spaces to make an identity that could pass validation.

## 5 Experimental Results

In this section, we demonstrate the vulnerability of byzantine and Sybil attacks and look into the effectiveness of our defense mechanism.

Simulation setup: we implemented S-ODMRP-RKP using network simulator-2(ns-2).ns-2 is a packet level simulator and a discrete event scheduler [23] which is used to simulate wired and wireless network.ns-2 is a standard experiment environment in research community which uses Tool Command Language (TCL) as its scripting language. We simulate a network environment with 50 nodes among them 20 nodes are randomly chosen as multicast group members for this experimental evaluation and one randomly selected node among them as the data source. Attackers are randomly selected among nodes that are not group members. Group members join the group in the beginning of the simulation. At second 100, the source starts multicasting 512-byte data packets for 400 seconds at a rate of 20 packets/second. The performance is evaluated based on the Packet Delivery Ratio.

The following scenarios are considered for the experimental evaluation.

- No-Attack: The attackers do not perform any action in the network. This denotes the ideal scenario where the attackers are discovered and completely isolated in the network, and serves as the baseline for evaluating the impact of the attack and the performance of the defense mechanism.
- Sybil attack and Byzantine attack.

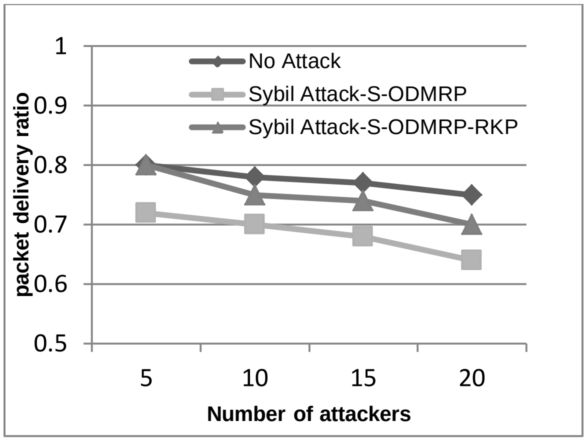


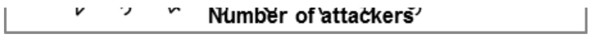
Figure 1: Effectiveness of S-ODMRP--RKP for Sybil attack

When Sybil attack is considered, S-ODMRP approach delivers a packet delivery ratio of 0.72, 0.7, 0.68 and 0.64 when the number of attackers is 5, 10, 15 and 20 respectively.

Figure 1 shows the effectiveness of the defense mechanism namely S-ODMRP-RKP against Sybil attack. The performance is compared with the S-ODMRP approach. It is observed that the proposed pre-key distribution approach with the S-ODMRP provides higher packets delivery ratio when compared with the S-ODMRP approach.

When the number of attackers increases, the packet delivery ratio decreases gradually. When there is no attack, it is observed that the packet delivery ratio is 0.8, 0.78, 0.77 and 0.75.

But, when the proposed S-ODMRP-RKP approach is considered, the packet delivery ratio is high when compared with S-ODMRP approach.



Attackers Vs PDR

## 6 CONCLUSION

This paper proposes a security suggestion of using high throughput metrics in multicast protocols in wireless mesh networks against the Sybil attacks. The Sybil attacks are found to degrade the performance of the network to a greater extent. Especially, the delivery ratio of the network is greatly affected due to the Sybil attack. This paper proposes a novel technique to counter the Sybil attacks. The proposed defense approach overcomes the challenges posed by the Sybil attacks through the combination of S-ODMRP with the random pre-key distribution approach. The simulation results are performed to reveal the performance of the prposed defense approach. It is observed from the simulation results that the proposed approach provides better delivery ratio.

## REFERENCES

[1] Jing Don and Reza Curtmola and Cristina Nita-Rotaru “Secure High-Throughput Multicast Routing in Wireless Mesh Networks”, IEEE Transactions on Mobile Computing, Vol. 10, No. 5, 2011.

[2] I. Akyildiz, X. Wang, W. Wang, “Wireless mesh networks: A survey, Computer Networks” 47 (4) (2005) 445–487.

[3] Uyen Trang Nguyen, “On multicast routing in wireless mesh networks”, Computer Communications, Vol. 31 pp.1385–1399, 2008.

[4] S. Paul, “Multicast on the Internet and Its Applications”, Kluwer Academic Publishers, 1998.

[5] H. Lundgren, E. Nordstrom, and C. Tschudin, “Coping with Communication Gray Zones in IEEE 802.11b Based Ad Hoc Networks,” Proc. Fifth ACM Int’l Workshop Wireless Mobile Multimedia (WOWMOM ’02), 2002.

[6] D.S.J.D. Couto, D. Aguayo, J.C. Bicket, and R. Morris, “A High-Throughput Path Metric for Multi-Hop Wireless Routing,” Proc. ACM MobiCom, 2003

[7] J. R. Douceurm, “The Sybil attack. In First International Workshop on Peer-to-Peer Systems (IPTPS '02)”, Mar. 2002.

[8] P. Papadimitratos and Z. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), pp. 27-31, Jan. 2002.

[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[10] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E. Belding- Royer, “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 10th IEEE Int’l Conf. Network Protocols (ICNP), 2002.

[11] Jing Dong; Ackermann, K.E.; Nita-Rotaru, C.; “Secure group communication in wireless mesh networks”, International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Page(s): 1 – 8, 2008.

[12] Curtmola, R.; Nita-Rotaru, C.; “BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks”, 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07), Page(s): 263 – 272, 2007.

[13] D.S.J.D. Couto, D. Aguayo, J.C. Bicket, and R. Morris, “A High-Throughput Path Metric for Multi-Hop Wireless Routing,” Proc. ACM MobiCom, 2003.

[14] R. Draves, J. Padhye, and B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks,” Proc. ACM SIGCOMM, 2004.

[15] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, “A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks,” Proc. First Int’l Conf. Broadband Networks (BroadNets ’04), 2004.