

Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks

Anjum Naveed

School of Computer Science and Engineering
University of New South Wales
Sydney, Australia
anaveed@cse.unsw.edu.au

Salil S. Kanhere

School of Computer Science and Engineering
University of New South Wales
Sydney, Australia
salilk@cse.unsw.edu.au

Abstract—In order to fully exploit the aggregate bandwidth available in the radio spectrum, future Wireless Mesh Networks (WMN) are expected to take advantage of multiple orthogonal channels, with nodes having the ability to communicate with multiple neighbors simultaneously using multiple radios (NICs) over orthogonal channels. Dynamic channel assignment is critical for ensuring effective utilization of the non-overlapping channels. Several algorithms have been proposed in recent years, which aim at achieving this. However, all these schemes inherently assume that the mesh nodes are well-behaved without any malicious intentions. In this paper, we expose the vulnerabilities in channel assignment algorithms and unveil three new security attacks: Network Endo-Parasite Attack (NEPA), Channel Ecto-Parasite Attack (CEPA) and low-cost ripple effect attack (LORA). These attacks can be launched with relative ease by a malicious node and can cause significant degradation in the network performance. We also evaluate the effectiveness of these attacks through simulation based experiments and briefly discuss possible solutions to counter these new threats.

I. INTRODUCTION

Wireless Mesh Networks (WMN) are emerging as the key future technology for providing wireless broadband access. A typical WMN consists of traffic aggregation nodes that serve the purpose of access points for client nodes, and gateway nodes that provide the connectivity with the wired Internet. To increase the available bandwidth, each WMN node is equipped with multiple radios (NICs) each using the orthogonal channels to ensure simultaneous and interference free communication. Dynamic channel assignment is required to assign the channels to the network links to ensure the optimum channel usage. Various joint channel assignment and routing algorithms have been proposed for Multi-Radio Multi-Channel WMN (MRMC-WMN) [1]–[5]. Some of these algorithms [1] use a centralized approach, which requires global information about the channel assignment of all the nodes, while others use distributed algorithms [2], which only requires neighborhood information, in order to make efficient channel assignment. However, all these algorithms assume that the mesh nodes are well-behaved. Therefore, a node does not verify the channel assignment information communicated by its neighbors and in fact uses the same for making a decision

about its own channel assignment. This assumed trust amongst the neighboring nodes makes these algorithms vulnerable to security attacks.

An effective attack, which exploits the dynamic channel assignment in MRMC-WMN, is to force mesh nodes within the same interference domain to use fewer channels. Consequently the increased interference reduces the throughput of the network. Similarly, the channel assignment dependency between neighboring nodes can be exploited to trigger a series of channel assignment changes, forcing the network into a quasi-stable state. In this paper, we expose the vulnerabilities in dynamic channel assignment algorithms and propose three Novel attacks, namely *Network Endo-Parasite Attack (NEPA)*, *Channel Ecto-Parasite Attack (CEPA)* and *Low-Cost Ripple Effect Attack (LORA)*. The NEPA and CEPA attacks maliciously switch the links in the network to heavily loaded channels using the compromised node. Such malicious switching increases the interference, which in turn decreases the bandwidth of the network. On the other hand, the channel assignment dependency between the neighboring nodes is exploited by LORA, whereby maliciously calculated false information about channel assignment is transmitted to neighbors resulting in premature and frequent channel adjustments of other nodes forcing the network into a quasi-stable state. To best of our knowledge, this work is the first to analyze the security vulnerabilities of dynamic channel assignment algorithms in MRMC-WMN.

The rest of the paper is organized as follows. Section II introduces different channel assignment algorithms with a particular focus on [2] (*Hyacinth*). We also discuss certain known security attacks. Section III covers *NEPA*, *CEPA* and *LORA* attacks while Section IV summarizes the experimental results. Section V outlines the basis for solutions to the security vulnerabilities in channel assignment algorithms. We present the road map for future work and conclude in Section VI.

II. RELATED WORK

A. Channel Assignment Algorithms

Various techniques have been proposed to utilize multiple interfaces and increase the bandwidth of MRMC-WMN [1]–[6]. Use of multiple radios per node to increase the bandwidth of WMN was first proposed in [6]. The routing algorithm (MR-LQSR) requires the nodes to have global information about the bandwidth, loss-rate and channel assignment in order to select the optimum routing paths. Centralized channel assignment and routing algorithms have been proposed in [1]. The proposed neighbor partitioning scheme and the load-aware channel assignment requires the nodes to maintain channel assignment information of the neighboring nodes. The available information at the nodes in these schemes can be used to launch network partitioning, black-hole and DoS attacks.

A distributed channel assignment algorithm for WMN has been proposed in [2] (*Hyacinth*). We use it as the target algorithm/architecture to model our attacks, primarily due to its highly practical and scalable architecture. However, we propose the attack algorithms general enough to be applicable to any channel assignment and routing algorithm for MRMC-WMN. *Hyacinth* nodes use bandwidth usage, hop-count distance from the wired gateway and the channel assignment of the neighboring nodes to decide the channel assignment for their interfaces. Interfaces of each node are divided into UP-NICs and DOWN-NICs used to communicate with parent nodes and the child nodes respectively. Channel assignment for UP-NICs of the node is the responsibility of its parent while the node assigns channels to its DOWN-NICs only. The channels used by the links closer to the wired gateway have higher priority. The cost associated with channel usage for a particular link is determined by the aggregate bandwidth usage of the channel within its interference domain. A node uses the least loaded channel that is not being used by any higher priority node within its interference domain. Nodes periodically exchange their channel usage information with their interference domain neighbors using CHNL_USAGE message.

B. Related Attacks

Security vulnerabilities in wireless networks, possible attacks and the solutions have been discussed in [10]–[13]. For example, [10] proposes DoS attacks in wireless ad-hoc networks, exploiting the RTS-CTS mechanism in IEEE 802.11 MAC. Attacks exploiting routing vulnerabilities have been analyzed in [14]. The attacks proposed in this paper are significantly different from all these attacks because vulnerabilities in channel assignment algorithms are exploited instead of routing vulnerabilities or MAC layer control mechanisms. The role of dynamic channel assignment in WMN is comparable with the role of Border Gateway Protocol (BGP) in the Internet. Similar to attacks that exploit BGP, tampering with the channel assignment can change the routing topology and seriously disrupt the service of WMN and partition the network into

segments. Security vulnerabilities in BGP have been analyzed in [9] among others. Although the objective and the effect of the attacks is similar, our technique and the exploited vulnerabilities for Low-cost Ripple effect attacks are different from ripple effect attacks on BGP.

III. ATTACK METHODOLOGIES AND ALGORITHMS

A. Assumptions

- The attacks assume a compromised node exists in the target network. Compromising the node is fairly easy in case of wireless networks even in presence of authentication mechanisms.
- Since the channel used by a particular link is associated with only one node (The node using DOWN-NIC in *Hyacinth*), we associate the channel with link or the node interchangeably, without loss of generality.
- The channels used on the links closer to wired gateways are heavily loaded as well as high priority ones (refer [2]). We, therefore, use the term high priority heavily loaded channel without loss of generality.

B. Critical Weakness in Channel Assignment Algorithms

The proposed attacks exploit the following two critical weaknesses of channel assignment algorithms. First, dynamic channel assignment algorithms require WMN nodes to exchange their channel assignment and usage information with their interference domain neighbors to make efficient channel assignment decision. Consequently, a node has up-to-date information of channel assignment within its interference domain neighborhood that can be exploited by malicious node. Second, these algorithms assume that the nodes are well-behaved hence each node makes an independent decision about its channel assignment and inform its neighbors about the decision which is not verified by the neighbors. In fact, the neighboring nodes adjust their channel assignments based on the information from any node, to minimize the interference. Such adjustments are expected to occur infrequently.

C. NEPA - Methodology and Algorithm

The objective of NEPA and CEPA is to increase the interference at heavily loaded high priority channels. Most of the time, the effected links are along the routing path from the malicious node towards the wired gateway, hence the attacks take the name of parasite attacks. Under normal channel assignment operation, a node assigns the least loaded channels to its interfaces and transmits the latest information to its interference domain neighbors. A compromised node launches NEPA by assigning its interfaces, the higher priority channels. The node transmits this information to the child nodes to ensure the change in channels takes place. However, it does not inform its neighbors about this change, i.e. in *Hyacinth* CHNL_USAGE message is not modified to incorporate up-to-date channel assignments. Since the transmitted information is not verified by neighbors, the network remains unaware of change. This results in hidden usage of heavily loaded channels, hence the attack takes the name *Endo-parasite* which

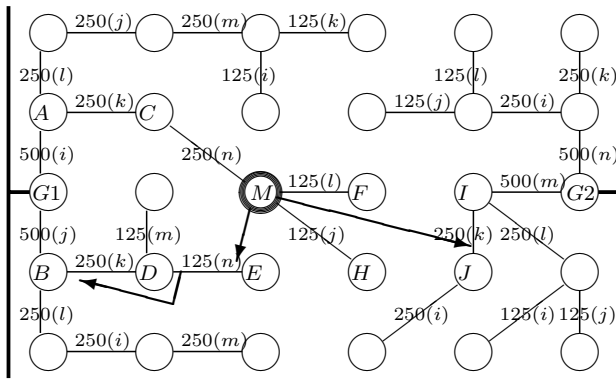


Fig. 1. Example WMN with routers physically arranged in grid topology. G1 and G2 are wired gateways. Edges show routing topology and labels along edges are [bandwidth in kbps(channel)]. For simplicity, $k + 1$ -hop neighbors include immediate physical neighbors only. Arrows show propagation of ripple effect attack from compromised node M.

refers to internal/hidden parasites. The links using these channels experience interference, decrease in available bandwidth and continuous degraded performance.

Consider a simple example shown in Figure 1. Suppose node M (hop-count distance of 3 from gateway) is the compromised node. Within its $k + 1$ -hop neighbors (refer [2]), channel k and n are heavily loaded channels (500kbps and 375kbps). If node M maliciously switches link MF to channel k and link MH to channel n, links AC, BD, DE and CM will all experience interference. Note that all the affected links are associated with higher priority nodes (hop-count distance of 1 and 2 from gateway). This will affect the sub-trees following nodes A and B resulting in degraded performance. Algorithm 1

Algorithm 1 NEPA Algorithm

```

1: Store current channel assignment.
2: loop
3:   Wait  $T_c$  time units to receive neighbor information. {See Hyacinth for time  $T_a$ }
4:   Sort channel assignment and usage information in decreasing order.
5:   if Highest priority channels have changed since last iteration then
6:     Assign highest priority channels in decreasing order to interfaces. {DOWN-NICs in Hyacinth}
7:     Transmit information to effected children.
8:   end if
9:   Transmit Stored channel assignment to neighbors.
10: end loop

```

depicts the pseudo-code for NEPA attack and is similar to *Hyacinth* channel assignment algorithm with differences on lines 6 and 9 only. At line 6, the compromised node assigns the channels to its interfaces (DOWN-NICs in case of *Hyacinth*) in decreasing order of priority and cost of usage (instead of normal operation of assigning channels in increasing order of cost). Line 9 shows that the out dated channel assignment information prior to the attack is transmitted to neighbors. The loop keeps the network under continuous attack.

D. CEPA - Methodology and Algorithm

CEPA is a special case of NEPA with slight modification in the attack strategy. A compromised node launches CEPA by switching all its interfaces to the channel that is being used by the highest priority link. For example, Node M (Malicious node) in the network of Figure 1 will switch links MF and MH to channel k (Bandwidth usage of 500kbps). Rest of the procedure is same as NEPA. Consequently, the complete sub-tree following the effected links (AC and BD in Figure 1) will experience severe performance degradation because of extensive hidden use of the channel. However, the severe nature of attack makes the detection easy, hence the attack is named Ecto-parasite meaning external/visible. Pseudo-code for CEPA is listed as algorithm 2 and is same as the algorithm for NEPA with the only change on line 6 where all the interfaces are assigned the highest priority channel.

Algorithm 2 CEPA Algorithm

```

1: Store current channel assignment.
2: loop
3:   Wait  $T_c$  time units to receive neighbor information. {See Hyacinth for time  $T_a$ }
4:   Sort channel assignment and usage information in decreasing order.
5:   if Highest priority channels have changed since last iteration then
6:     Assign highest priority channel to all interfaces. {DOWN-NICs in Hyacinth}
7:     Transmit information to effected children.
8:   end if
9:   Transmit Stored channel assignment to neighbors.
10: end loop

```

E. LORA - Methodology and Algorithm

The attack LORA is different from NEPA and CEPA because the channel assignment of the compromised node is not actually changed (hence low-cost attack). The objective of the attack is to force the network in quasi-stable state by imposing premature channel adjustment on other nodes repeatedly. The attack is relatively more severe than NEPA and CEPA because the affect is propagated to a large portion of the network beyond the neighbors of the compromised node, disrupting the traffic forwarding capability of various nodes for considerable time duration. Note that, most of the dynamic channel assignment algorithms (specifically *Hyacinth*) prevent the ripple effect to propagate within the network from the parent to the child nodes, but the effect can still propagate in the reverse direction.

The attack is launched when the compromised node transmits misleading channel assignment information, forcing the other nodes to adjust their channel assignments. This may generate a series of changes even in the channel assignment of non-neighboring nodes. For example, compromised node M (Figure 1) launches the attack by informing neighbors that it has switched link MF to channel k and link MH to channel n, without actually changing the channel assignment. Consequently, node I will find channel j more suitable for link IJ (aggregate bandwidth usage for channels k and j before malicious information are 375kbps and 250kbps respectively

excluding IJ link and after switching are 250kbps and 375kbps respectively). Similarly, link DE will be switched to channel l from channel n. This will further propagate to link BD which will be switched to channel n from channel k. A similar effect will be observed for channel assignments of C and A and so on. It is obvious that a considerable portion of the network is affected by the misleading information from a single compromised node. Algorithm 3 enlists the LORA

Algorithm 3 LORA Algorithm

```

1: loop
2:   Wait Random period of time. {Network stabilizing time}
3:   Receive neighbor information.
4:   Sort channel assignment and usage information in decreasing order.
5:   Randomly select normally loaded channels.
6:   Construct channel assignment information message with selected channel assignments for the node interfaces. {CHNL_USAGE message in Hyacinth}
7:   Transmit constructed message to neighbor nodes.
8: end loop

```

pseudo-code algorithm which works independently in parallel with the channel assignment algorithm. Lines 5 and 6 form the core of attack where middle priority channels are selected and message (CHNL_USAGE in [2]) is constructed showing the fake assignment of these channels to interfaces. Note that, normally loaded channels are selected instead of heavily loaded ones and an illusion of heavy load on these channels is created, which results in propagation of change upwards in the routing tree. Heavily loaded channels are not selected because such selection will affect the links closer to gateway resulting in quick adjustment to the change and hence no ripple effect will be created.

IV. EXPERIMENTAL RESULTS

We have evaluated the proposed attacks through NS-2 simulation based experiments. We used the grid topology for physical placement of twenty five WMN nodes, each equipped with two NICs. We generated variable routing topologies and traffic load to test the attacks extensively. Different hop-count distances were selected for the compromised node and the affect was observed. Different topologies and traffic load resulted in different level of performance degradation, while the compromised node at hop-count distance of 3 from the wired gateway resulted in most affective attacks. A sample experiment for each of the three attacks is shown in Figure 2, comparing performance under normal channel assignment and under attack. Low traffic load was used where bandwidth requirements of all the links were satisfied under normal channel assignment. Figure 2(a) shows the sample experiment for NEPA. Since each WMN node is equipped with two NICs, one of which is used to communicate with the child node, we created the effect of NEPA using two compromised nodes. The graph in Figure 2(a) shows a decrease to 85% (1.45mbps compared to 1.7mbps) in the aggregate bandwidth when NEPA is launched on the network. The experimental results confirm the hypothesis that NEPA induces relatively lesser damage and hence remains undetected for considerable time duration. Note

that, the traffic load on the network is very low (1.7mbps only) yet the attack is affective. For extensive load on the network, we measured the performance degradation of up to 65% at the most for NEPA.

Figure 2(b) shows the sample experiment for CEPA. The graph shows that the aggregate bandwidth decreases to 53% (0.9mbps compared to 1.7mbps) when CEPA is launched on the network. Our experiments show that the available aggregate bandwidth can be limited to 40% if the compromised node is closer to the wired gateway. This shows the severe nature of CEPA, making it more detectable. Figure 2(c) shows the effect of LORA on the aggregate bandwidth. While the performance degradation caused by NEPA and CEPA was dependent on the network topology and the bandwidth requirements, the affect of LORA appeared to be controlled by the internal parameters. Random time selection for the iteration on line 2 and the random selection of channels to be attacked on line 5 of the algorithm 3 make LORA a tuneable attack. The graph shows two iterations of the attack. The decrease in available bandwidth was dependent on the propagation of the ripple effect and varied from 90% to 60% within a time duration of 8 seconds.

V. CHANNEL ASSIGNMENT ATTACKS - PREVENTION AND DETECTION

Our research shows that the problem of security vulnerabilities in joint routing and channel assignment algorithms needs to be addressed from two dimensions. First, preventive measures in form of secure routing and channel assignment algorithms can reduce the possibility of the network being targeted by attacks. Second, proper detection and automated response mechanisms to make the network self-heal should form a necessary operational component of MRMC-WMN.

Routing and channel assignment algorithms in wireless mesh networks need to be evolved with a focus on security. A possible solution is to establish the trust between nodes through authentication and use encryption to secure messages. However, this will result in increased complexity and the problem of compromised nodes is not necessarily solved. We alternatively propose the modification in routing and channel assignment algorithms to address the issues within algorithms. The aforementioned attacks can effectively be barricaded if the WMN nodes verify the channel assignment of neighboring nodes through channel scanning whenever they need to change their channel assignment, revealing the hidden usage of channel (which lies at the base of NEPA and CEPA) as well as false announcement problem (the base of LORA). Since the channel assignments remain stable over a longer time duration and changes only when there is a significant change in network topology or usage, the overhead of scanning will be negligible.

No prevention mechanism guarantees complete security, therefore, proper detection mechanism is mandatory to enhance the security of any system. We direct our research to redefine the metrics for Intrusion Detection Systems (IDS) to incorporate the dynamic channel assignment and its impact on routing. A distributed IDS which divides the network into

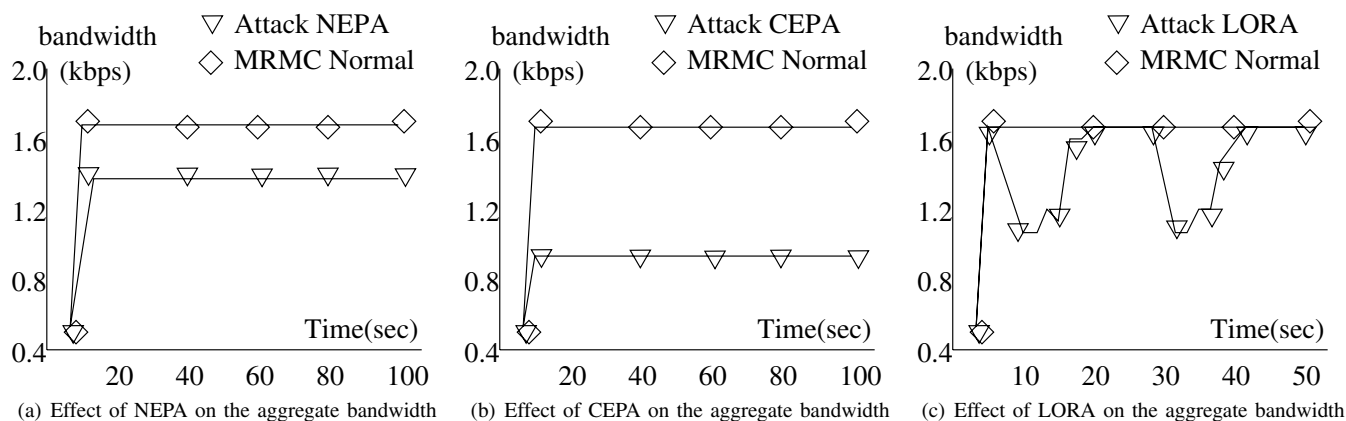


Fig. 2. Simulation results

zones with a randomly selected controller within each zone can be effective. An example of such IDS is [7] which can be modified as mentioned above. The controller node can scan the channels at regular intervals and verify the announcements of the nodes within its neighborhood to identify any irregularities in channel assignment. IDS can also verify the channel change information to ensure that correct decision is taken by the node which may reveal the misbehaving node. Furthermore, frequent channel change information can easily be identified as an anomaly, which can then generate a response from the IDS in form of the scanning and healing process.

VI. CONCLUSION AND FUTURE WORK

In this paper we exposed the vulnerabilities in dynamic channel assignment algorithms. We presented three novel attacks NEPA, CEPA and LORA. Even though we have used the *Hyacinth* algorithm as an example to illustrate the attacks, the attack strategies are general enough to be applicable to other dynamic channel assignments. On the one hand, in NEPA and CEPA the channel assignment of the compromised node is changed resulting in hidden usage of heavily loaded channels. On the other hand, in LORA, the compromised node disseminates misleading information about its channel assignment resulting in a series of channel assignment changes in other WMN nodes. Our experiments showed that NEPA can result in a decrease in available aggregate bandwidth from 92% to 65% while CEPA is relatively more severe with the decrease in available aggregate bandwidth ranging from 80% to a maximum of 40% in some cases. LORA is a tuneable attack and the performance degradation is dependent on selected value of interval between iterations.

There are several avenues that we intend to explore in the future. We intend to quantify the severity of the damage caused by the attacks on wireless networks in general and the proposed attacks in particular. We also intend to propose secure routing and channel assignment algorithms for MRMC-WMN. We will also explore the defense mechanisms outlined in section V to develop the intrusion prevention, intrusion detection and the automated response systems which to ensure

that future WMNs are self healing.

REFERENCES

- [1] Ashish Raniwala, Kartik Gopalan, Tzi-cker Chiueh. *Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks*. In ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), April 2004
- [2] Ashish Raniwala, Tzi-cker Chiueh. *Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network*. In proceedings of IEEE InfoCom. March 2005
- [3] Murali Kodialam, Thyaga Nandagopal. *Characterizing the capacity region in multi-radio multi-channel wireless mesh networks*. In proceedings of Mobile Computing and Networking. August 2005
- [4] Mansoor Alicherry, Randeep Bhatia, Li (Erran) Li. *Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks*. In proceedings of Mobile Computing and Networking. August 2005.
- [5] Pradeep Kyasanur, Nitin H. Vaidya. *Capacity of Multi-Channel Wireless Networks: Impact of number of channels and Interfaces*. In proceedings of Mobile Computing and Networking. August 2005.
- [6] Paramvir Bahl, Atul Adya, Jitendra Padhye, Alec Wolman. *Reconsidering the Wireless LAN Platform with Multiple Radios*. In SIGCOMM Computer Communication Review (CCR), July 2004.
- [7] Yi-an Huang, Wenke Lee. *A cooperative intrusion detection system for ad hoc networks*. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Pages: 135 - 147, October 2003.
- [8] Timothy R. Schmoyer, Yu Xi Lim and Henry L. Owen. *Wireless Intrusion Detection and Response: A case study using the classic man-in-middle attack*. In proceedings of Wireless Communications and Networking Conference (WCN), Pages: 883 - 888, March 2004.
- [9] S. Murphy, *BGP Security Vulnerabilities Analysis*. Jan 2006. RFC 4272.
- [10] V. Gupta, S. Krishnamurthy, and M. Faloutsos. *Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks*. In Proceedings of Milcom, 2002.
- [11] Y. Zhang and W. Lee. *Intrusion detection in wireless ad hoc networks*. ACM MOBICOM, 2000.
- [12] Chunxiao Chigan, Leiyuan Li, Yinghua Ye. *Resource-aware self-adaptive security provisioning in mobile ad hoc networks*. In proceedings of Wireless Communications and Networking Conference, Pages: 2118 - 2124, March 2005.
- [13] Rupinder Gill, Jason Smith, Mark Looi and Andrew Clark. *Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless*. In proceedings of Auscert2005, Jan 2005.
- [14] Yi-an Huang, Wei Fan, Wenke Lee, Philip S. Yu. *Cross-feature analysis for detecting ad-hoc routing anomalies*. Proceedings. 23rd International Conference on Distributed Computing Systems, Pages: 478 487, May 2003.