Detection and Overcome of Energy Draining attacks in Wireless Ad-Hoc Sensor Networks

Jasti Sri Harsha
is currently pursuing masters degree program in Telecommunication Networks in SRM University, India,

V Ramkishore
Assistant professor in Telecommunication Networks in SRM University, India,

***Abstract*— The widespread growth of Ad-hoc device networks represents future evolution of internet having the power to assemble, analyze, and distribute knowledge that may turn knowledge into information, knowledge, intelligent higher cognitive process and ultimately for future prediction. This latest progressive sensing, computing and communication system don't seem to be only dynamical client expectation in people's everyday lives however step by step taking them nearer to the long run era of connected everyday things, mistreatment mixtures of wired and wireless property. There are millions of protocols established to safeguard from DOS attack, however it's not dead doable. One such DOS attack is lamia attack. This lamia attack may be a resource depletion attacks at the routing protocol layer, that for good disconnect the networks by quickly exhausting nodes' battery power. These "Vampire" attacks don't seem to be specific to any specific protocol, however rather rely on the characteristics of the many well-liked categories of routing protocols. It's a troublesome task to see these attacks except causation solely protocol-compliant messages and discover it. Sometimes, one lamia will increase network-wide energy usage by an element of O (N), wherever N within the range of network nodes. Ways to discover and secure knowledge packets from vampires throughout the packet forwarding part is mentioned.**

Index Terms — DOS, node, packet, PLGP, routing protocol, sensor, vampire attacks.

1. INTRODUCTION

A network consists of nodes every of that has computing power and may transmit and receive message over communication links, wireless or cabled. In Wireless networks every node use radio signal with alternative nodes. A wireless ad hoc device network consists of variety of sensors unfold across a geographic area. Every device has wireless communication capability and a few level of intelligence for signal process and networking of the information. The essential characteristic of ad-hoc device network is that the communication among nodes of network with none pre-existing infrastructure. Wireless ad hoc device Network became terribly essential in communication surroundings. Owing to distributed nature of those networks and their preparation in remote areas, these networks area unit vulnerable to many security threats which will adversely have an effect on their correct functioning. Ad hoc device network guarantees pervasive computing, instantly deployable communication for military and continuous property, for making a replacement application in future. Resource constrains is one in all the most characteristic of a Wireless device networks Simplicity in WSN with resource forced nodes makes them greatly at risk of denial of service , attacks on routing infrastructure, and reduction of quality attacks.

Routing techniques area unit needed for sending information between device nodes and base station for communication. There is a unit many ways to classify the routing protocols. The majority of the routing protocols are often classified as data-centric, ranked and site based mostly in keeping with the network structure. In data-centric routing all nodes area unit generally assigned equal roles or practicality. In hierarchical-based routing but, nodes can play completely different role within the network. In location based mostly routing device node's positions area unit exploited to route information within the network. The wireless medium is inherently less secure as a result of its broadcast nature makes eavesdropping straightforward. Any transmission will simply be intercepted, altered, or replayed by associate degree someone. The wireless medium permits associate degree offender to simply intercept valid packets and simply inject malicious ones. Though this downside isn't distinctive to device networks, ancient solutions should be tailored to with efficiency execute on device networks. Developing energy-efficient routing protocol on wireless device networks is one in all the necessary challenges. Therefore, a key space of WSN analysis is to develop a routing protocol that consumes low energy. Unfortunately, current routing protocols suffer from several security vulnerabilities. Already several solutions are planned to defend attack that live for brief period on the network. However these solutions don't defend permanent resource depletion attack. The battery power consumption attacks at routing layer protocol to fully disable networks, by depleting node's battery power and it's outlined as lamia attacks. These attacks ne'er flood the network with great deal of information instead it drains node's life by delaying the packets. Protocols like SEAD, Ariadne, and SAODV are a unit firmly designed however does stop the lamia attacks existing security theme area unit restricted to alternative layers like medium access management or application layers however to not the routing layer to secure lamia attacks.

2 PROPOSED WORK

We made three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing infrastructure, and so existing

secure routing protocols. We will assume that a node is permanently disabled once its battery power is exhausted, let us briefly consider nodes that recharge their batteries in the field, using either continuous charging or switching between active and recharge cycles. In the continuous charging case, power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge. Assuming that packet processing drains at least as much energy from the victims as from the attacker, a continuously recharging adversary can keep at least one node permanently disabled at the cost of its own functionality.

Advantages of proposed system

- Cannot optimize out malicious action like maximize power efficiency of network, which is inappropriate.
- Ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbor of the previous route hop.

In this paper, we have a tendency to square measure attending to discuss regarding the actions of the vampire spirit attacks in the wireless ad hoc networks. These sorts of attacks not directly link with the protocols; it links with the properties of the routing protocols in the communication networks. This attack affects the properties such as relation state between the nodes, remoteness vectors between the nodes, resource and placement primarily based routing. The vampire spirit attack in the WSN is not straight forward to discover and to predict. Due to the solitary vampire spirit attack in the networks, total force goes down and ends up in the entire systems to the collapse. The vampire spirit attacks is classified has 2 sorts. There are: one is Carousel attack and alternative is Stretch attack.

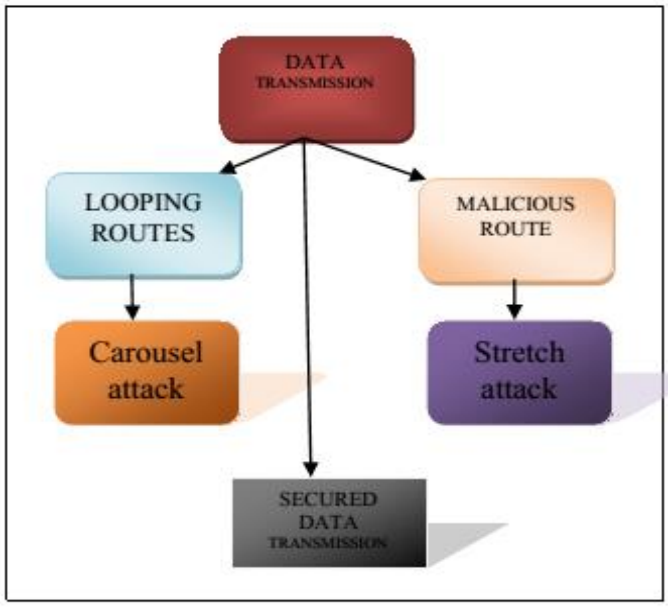


Figure 1: Architecture of our proposed system

3 RELATED WORK

3.1. Jelly Fish Attack

This type of assailment is used for closed-loop system flow like transmission control protocol. A important vigor of the Jelly Fish Assailment is that it maintains compliance with all management plane and information plane protocols so as to form detection and diagnosing pricey and time overwhelming. The key principle is that Jelly Fish attack use to facilitate is targeting end-to culminate congestion management.

3.2. Black Aperture Attack

This type of assailment is used for open loop management flows. Black Aperture nodes participate all told routing management plane operations. However, once methods are established, Black Holes merely drop all packets.

3.3 Path Quality observance

They style associate degreed analyze path-quality observance protocols that faithfully raise an alarm once the packet-loss rate and delay exceed a threshold, even once associate degree somebody endeavors to inequitableness observance results by selection delaying, dropping, modifying, injecting, or preferentially treating packets.

3.4. Routing infrastructure attack

Routing infrastructure fixates on minimal-energy routing, that aims to utilize borderline energy to transmit and receive packets and by utilizing borderline energy methods to transmit packets, but utilizing such schemes might cut back the network property and lifelong of the network. To shun such quandaries, associate degree energy wakeful routing protocol, that uses sub- optimum methods, was introduced. Several routing methods are gift wherever the protocol culls one predicated on probabilistic values. During this case, each routing path is given an opportunity to transfer packets therefore enhancing the network lifespan.

3.5. Resource depletion attacks

Resource depletion attacks fixate on reducing the amount of resources utilized by nodes like battery power, storage, recollection etc therefore reducing the general capability of the network. There are several forms of attacks like carousel attack, stretch attack, aerial attack, and malicious revelation attack. Several strategies like loose F. Coordinate and Beacon Protocols

3.6 Coordinate and Beacon Protocols

The two samples of coordinate and beacon protocols are GPSR and BVR. These protocols use physical coordinates or beacon distances for routing. In GPSR a packet might encounter a dead finish (i.e. target divided by a wall or obstruction).The packet is then pleased till a path to the target is offered .They do not take path length under consideration once routing around native obstructions. In BVR the packets are routed towards a node (beacon) proximate to the target. Every node makes freelance forwarding choices thence the lamia attacks (draining node life) are spoken to be forced.

4 ENERGY DRAINING ATTACKS ON STATELESS AND STATEFUL PROTOCOLS

In the DSR source node designates the entire route in the packet header to a destination, so intermediate node's do not make independent forwarding decisions, instead of a route designated by the source. To forward a message, the intermediate node finds itself in the route and transmits the

message to the next hop. The fardel is on the source to ascertain that the route is valid at the time of sending, and that every node in the route is a physical neighbor of the anterior route hop. Both the carousel and stretch assailments are evaluated in an arbitrarily engendered 30-node topology. It causes delay as well as increase communication overhead and energy consumption in resource inhibited networks .The effect of denial or degradation of accommodation on battery life and other finite node resources has not generally been a considered securely. We consider the effect of Vampire attacks on link-state, distance-vector, source routing and geographic and beacon routing protocols, as well as a logical ID-predicated sensor network routing protocol. While this is by no denotes an exhaustive list of routing protocols which are vulnerably susceptible to Vampire attacks.

3.1 Carousel attack

In this assailment, a maleficent node forward a packet with a route included a chain of loops, such that the packets traverse an abundance of times in the same route. This strategy can be used to increase the route length beyond the number of nodes in the network An example of this type of route is in Fig.3 the thick path shows the veracious path and thin shows the malignant path.

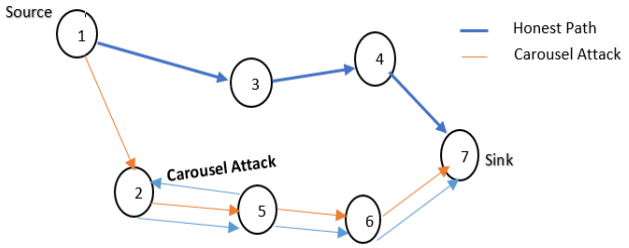


Fig. 2 shows the caurosel attack same node appears in the route many times from source to destination, (1-2-5-2-5-6-7--- as the routing loop).

3.2 Stretch attack

Another attack in the same layer is the stretch attack, where a maleficent node constructs mendaciously long source routes, causing packets to traverse a longer than optimal number of nodes. In this example given below veracious path shown with thick lines and adversary or maleficent path with thin lines. The veracious path is very less distant but the maleficent path is very long to make more energy consumption. Per-node energy utilization under both attacks is shown in Fig.5. As expected, the carousel attack causes exorbitant energy utilization for a few nodes, since only nodes along a shorter path are affected.

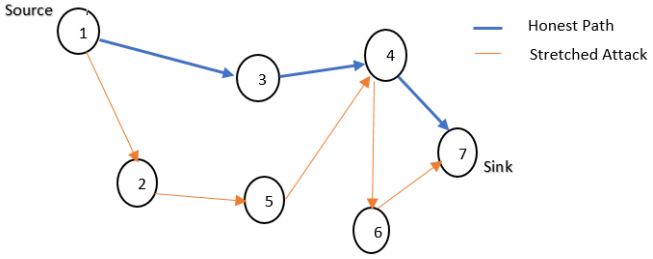


Fig. 3 Shows Stretch attack with two different paths from source to destination.(1-2-5-4-6-7—long route).

In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks drastically network-wide energy utilization, individual nodes are additionally saliently affected, with some losing virtually 10 percent of their total energy reserve per message. Two paramount classes of Stateful protocols are link state and distance-vector. In link-state protocols, such as OLSR, nodes keep a record of the up-or-down state of links in the network, and flood routing updates every time a link goes down or an incipient link is enabled. Distance vector protocols like DSDV keep track of the next hop to every destination, indexed by a route cost metric, e.g., the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated. Routes in link-state and distance-vector networks are built dynamically from many independent forwarding decisions, so adversaries have circumscribed power to affect packet forwarding, making these protocols immune to carousel and stretch attacks. In GPSR, a packet may encounter a dead end, which is a localized space of minimal physical distance to the target, but without the target authentically being reachable. The packet must then be diverted until a path to the target is available. In BVR, packets are routed toward the beacon most proximate to the target node, and then move away from the beacon to reach the target. Each node makes independent forwarding decisions, and thus a Vampire is circumscribed in the distance it can divert the packet. These protocols withal fall victim to directional antenna attacks in the same way as link-state and distance-vector protocols above, leading to energy utilization increase factor of O(d) per message, where d is the network diameter. Moreover, GPSR does not take path length into account when routing around local obstructions, and so malevolent misrouting may cause up to a factor of O(c) energy loss, where c is the circumference of the obstruction, in hops.

5 PLGP

We showed vary a spread a of proof-of-concept attacks against representative samples of existing routing protocols practice somewhat range of weak adversaries. We tend to tend to projected against a number of the forwarding-phase attacks and against a number of the forwarding-phase attacks and pictured PLGP-a.

Propose PLGP with attestations PLGP-a

PLGP-a uses this packet history in conjunction with PLGP' s tree routing structure so every node can firmly verify progress that stops any important adversarial influence on the path taken by any packet that traverses a minimum of 1 honest node .These signatures kind a sequence connected to every packet and permits any node receiving it to validate its path. to form positive that the packet has never cosmopolitan faraway from its destination inside the logical address house, every forwarding node verifies the attestation chain. PLGP-a satisfies no-backtracking- All messages unit of measurement signed by their originator. aggressor can entirely alter packet fields that unit of measurement changed linear measure route, so entirely the route attestation field square measure usually altered, shortened, or removed entirely. Use simplex signature

chain construction to prevent truncation. PLGP-a never floods and its packet forwarding overhead is favorable. It demonstrates further just routing load distribution and path diversity. Even whereas not hardware, the science computation required for PLGP-a is tractable even on 8-bit processor.

PLGP-a satisfies no-backtracking

To show that our modified protocol preserves the no-backtracking property, we tend to tend to stipulate a network as a group of nodes, a topology, property properties, and node identities, Honest nodes can broadcast and receive messages, whereas malicious nodes could use directional antennas to transmit to (or receive from) any node within the network whereas not being overheard by any different node. Honest nodes can compose, forward, accept, or drop messages, and malicious nodes could haphazardly transform them. Our mortal is assumed to control m nodes in associate N-node network (with their corresponding identity certificates and different secret science material) and has wonderful data of the constellation. Finally, the mortal cannot have a bearing on property between any a pair of honest nodes. Since all messages unit of measurement signed by their originator, messages from honest nodes can't be haphazardly modified by malicious nodes need to remain undiscovered. Rather, the mortal can entirely alter packet fields that unit of measurement changed linear measure route (and so unit of measurement not authenticated), so entirely the route attestation field are going to be altered, shortened, or removed entirely. To forestall truncation, which allow Vampires to hide the particular indisputable fact that they are moving a packet faraway from destination. For the wants of vampire attacks, we tend to tend to stand live unconcerned regarding packets with discretionary hop counts that unit of measurement never received by honest nodes but rather unit of measurement routed between adversaries.

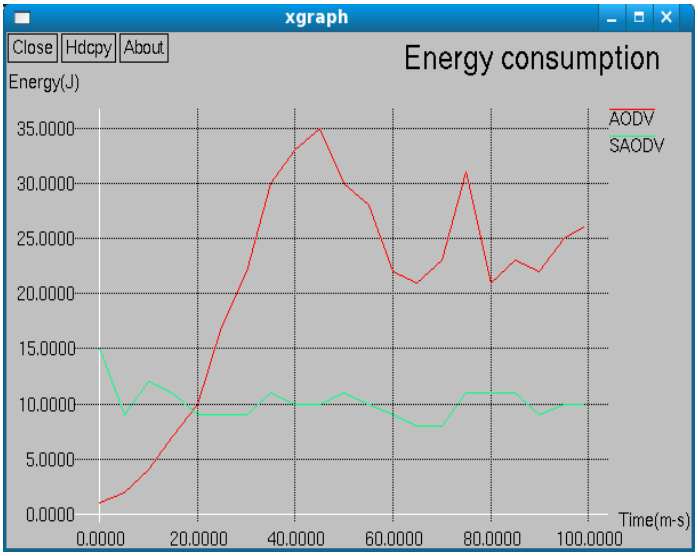
6 SIMULATION RESULTS

The simulation environment is implemented in the NS-2, a network simulator that provides support for simulating wireless networks. NS-2 is written using C++ language and uses the Object Oriented Tool Command Language (OTCL). It is an extension of the Tool Command Language (TCL).

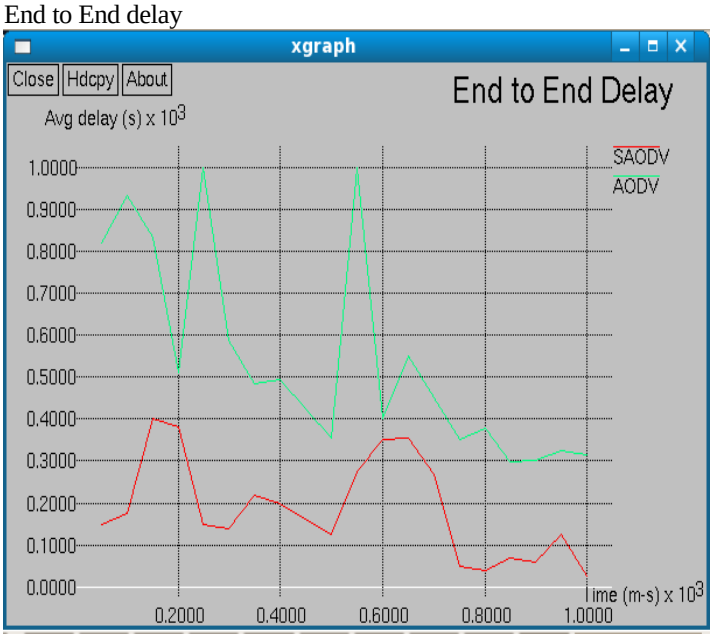
Detection of Vampire Attack

We have evaluated both the carousel and stretch attack. A randomly generated 15 node topology for carousel attack and 15 node topology for stretch attack is taken. A single randomly selected malicious AODV agent, using ns2 network simulator is evaluated and also we choose the honest path by using SAODV protocol. The constant energy set is 15J. For the stretch attack and carousel attack the energy consumed by the system is above 15J.

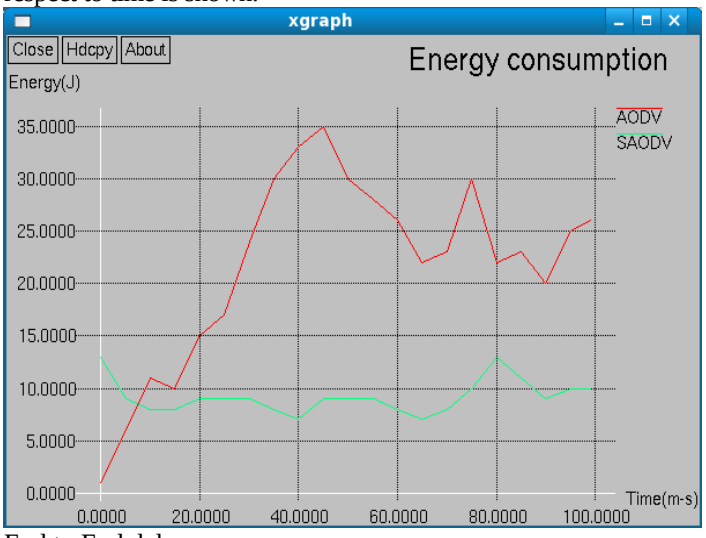
Energy calculations for carousel attack and end to end delay with respect to time is shown.



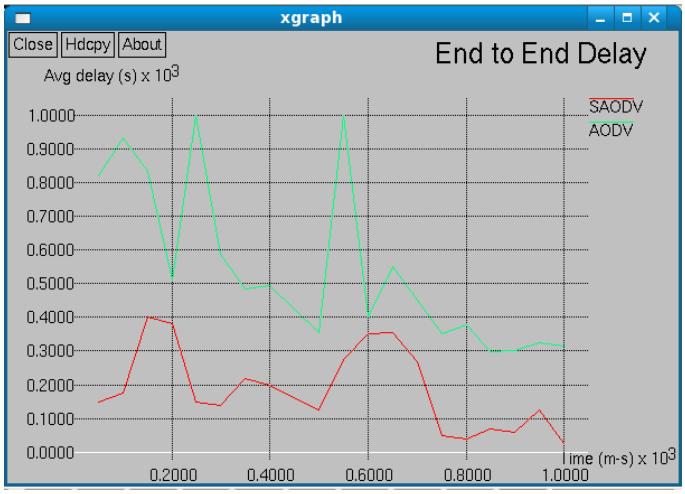
End to End delay



Energy calculations for stretched attack and end to end delay with respect to time is shown.



End to End delay



7 CONCLUSION

In this paper, we define Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. We also saw how to overcome these attacks by increasing the energy of the node in the network. Vampire attacks has been defined as a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. Defenses against some of the forwarding-phase attacks has been proposed and PLGP-a, the first sensor network routing protocol that reduces the damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The routing protocol has been used at the time of routing to make efficient energy utilization during the packet forwarding phase. But it has not offered the satisfactory solution during topology construction which is left for future work.

7 REFERENCES

[1] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security, 2002.

[2] Acs .G, Buttyan .L and Vajda .I, "Provably Secure On demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 5, No. 11, pp. 1533-1546, 2003.

[3] Suriadi .S, Stebila .D, Clark .A and H. Liu, "Defending Web Services against Denial of Service Attacks Using Client Puzzles", IEEE International Conference on Web Services, 2011.

[4] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

[5] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12,no. 4, pp. 609-619, Aug. 2004.

[6] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.

[7] L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks, "Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[8] V. Rodoplu and T.H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE J. Selected Areas in Comm., vol. 17, no. 8, pp. 1333-1344, Aug. 1999.

[9] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks" Ad Hoc Networking, Addison-Wesley, 2001.

[10] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[11]. Yih-Chun Hu, Perrig Adrian, and Johnson. David B., Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002

[12] R. Govindan and A. Reddy, "An Analysis of Internet Inter-Domain Topology and Route Stability," Proc. IEEE INFOCOM,1997.