International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.3 Issue No: Special 2, pp: 107-111 22 March 2014

Resource Consumption Attacks in Wireless Ad Hoc Sensor Networks

B. Umakanth[1], J. Damodhar[2]
Assistant Professor[1], Assistant professor [2], Department of ECE
Narayanadri Institute of Science & Technology[1],Annamacharya Institute of Technology & Sciences[2],(Autonomous), Rajampet, Kadapa(Dt,) AP,INDIA
[1]Umakanth.info@gmail.com, [2] Damu.aits@gmail.com

Abstract— ***AD hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes and battery power. These Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We proposed a EWMA method to bound the damage caused by these vampire types of attacks during the packet forwarding phase.***

Keywords—AdHocsensor networks, Energy consumption, Routing, Security.

I. Introduction

Wireless Sensor Network (WSN) consists of mostly tiny, resource-constraint, simple sensor nodes, which communicate wirelessly and form ad hoc networks in order to perform some specific operation. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Simplicity in WSN with resource constrained nodes makes them very much vulnerable to variety of attacks. The attackers can eavesdrop on its communication channel, inject bits in the channel, replay previously stored packets and much more. An adversary can easily retrieve valuable data from the transmitted packets that are sent (Eavesdropping). That adversary can also simply intercept and modify the packets' content meant for the base station or intermediate nodes (Message Modification), or retransmit the contents of those packets at a later time (Message Replay). Finally, the attacker can send out false data into the network, maybe masquerading as one of the sensors, with the objectives of corrupting the collected sensors' reading or disrupting the internal control data (Message Injection). Securing the WSN needs to make the network support all security properties: confidentiality, integrity, authenticity and availability.

Attackers may deploy a few malicious nodes with similar or more hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. The sensor nodes may not be tamper resistant and if an adversary compromises a node, it can extract all key material, data, and code stored on that node. As a result, WSN has to face multiple threats that may easily hinder its functionality and nullify the benefits of using its services.

In this paper, we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power draining and resource exhaustion attacks have been discussed before prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control(MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of Particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector ,source routing, and geographic and beacon routing .Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

II.OVER VIEW

We define a Vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1. Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.

In the remainder of this paper, we present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience. In source routing protocols, we show how a malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes who forward the packet based on the included source route. In routing schemes, where forwarding decisions are made independently by each node (as opposed to specified by the source), we suggest how directional antenna and wormhole attacks can be used to deliver packets to multiple remote network positions, forcing packet processing at nodes that would not normally receive that packet at all, and thus increasing network-wide energy expenditure. Lastly, we show how an adversary can target not only packet forwarding but also route and topology discovery phases—if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at every node in the network.

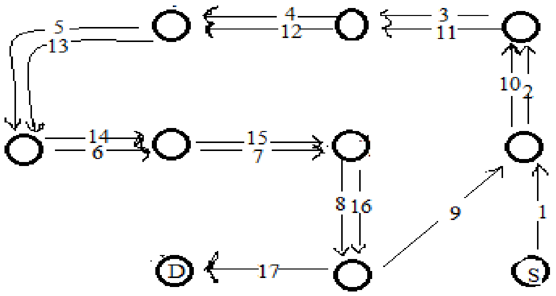

Fig. 1 An honest node would exit the loop immediately from node, but a malicious packet makes its way around the loop twice more before exiting.

In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles as shown in Fig. 1. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We call this the stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination.

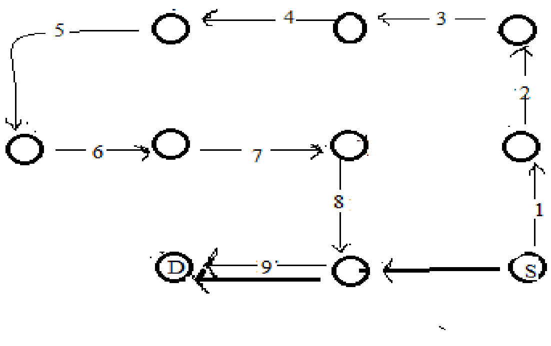

Fig.2.Honest node with thick line and malicious node with thin lines.

An example is illustrated in Fig.2. Results show that in a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overhead packets, we assume that only messages originated by adversaries may have maliciously composed routes.

III. RELATED WORK

We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion can be found as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus deplete their batteries faster. Newer research on "denial-of-sleep" only considers attacks at the MAC layer. Additional work mentions resource exhaustion at the MAC and transport layers but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned, but no effective defenses are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing. Even in non-power-constrained systems, depletion of resources such as memory, CPU time, and bandwidth may easily cause problems. A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the adversary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity (e.g., SYN cookies, which offload the initial connection state onto the client, or cryptographic puzzles). These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting and not always desirable as it punishes nodes that produce bursty traffic but may not send much total data over the lifetime of the network. Since Vampire attacks rely on amplification, such solutions may not be sufficiently effective to justify the excess load on legitimate nodes.

Other work on denial of service in ad hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire attacks, since Vampires do not use or return illegal routes or prevent communication in the short term.

Carousel attack: In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. An example of this type of route is in Fig.3 the thick path shows the honest path and thin shows the malicious path.

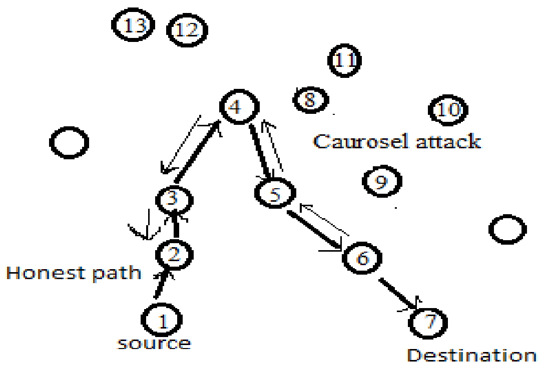

Fig. 3.shows the caurosel attack same node appears in the route many times.

Stretch attack: Another attack in the same vein is the stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. In the example given below honest path shown with thick lines and adversary or malicious path with thin lines. The honest path is very less distant but the malicious path is very long to make more energy consumption.

Per-node energy usage under both attacks is shown in Fig. 5. As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. 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 significantly network-wide energy usage, individual nodes are also noticeably affected,

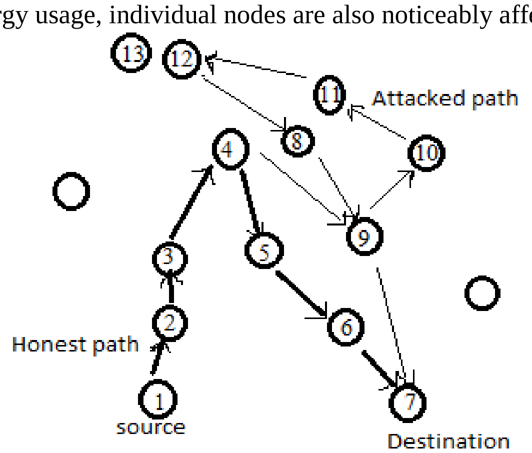

Fig.4 Shows Stretch attack with two different paths from source to destination.(4-9-10-11-12-8-9—long route).

with some losing almost 10 percent of their total energy reserve per message.

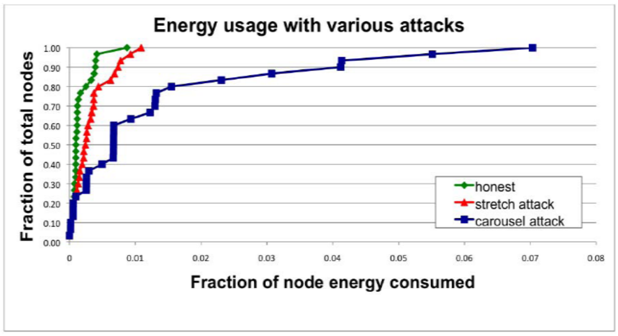

Fig.5.Node energy distribution under various attack scenarios.

IV.ENERGY WEIGHTED MONITORING ALGORITHM

This section focuses on the design details of our proposed protocol EWMA. Where energy of a node gets to threshold level it plays a vital role by performing energy intensive tasks there by bringing out the energy efficiency of the sensors and rendering the network endurable. This pattern based on the energy levels of the sensors.

EWMA functions two phases namely.

1. *Network configuring phase*
2. *Communication phase*

1. *Network configuring phase:* The goal of this phase is to establish a optimal routing path from source to destination in the network. The key factors considered are balancing the load of the nodes and minimization of energy consumption for data communication.

In this phase the node with threshold level energy (attacked node) sends ENG_WEG message to all its surrounding nodes. After receiving the ENG_WEG packets the surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographical position and current energy level. The node upon receiving this stored in its routing table to facilitate further computations.

Now the node establishes the routing path, first the traces the next node by computing the energy required to transmit the required data packet that is suitable energy node and less distant node selected as the next forwarding node in this way it establishes the route from source to destination with suitable energy and less distant.

Thus energy spent by the allotted node suitable to the data packet sent from the node in this way this algorithm avoids data packet dropping and this allotted forwarding node transmits the packets safely to the destination. This algorithm gives prime importance to achieve balancing of load in the network. The suitable energy node will be assigned as a forwarding node as long as this node as this node has the capacity to handle. In this way a multi hop minimal less distant path is established to bound the network damage from vampire attack.

EWMA avoids the collapsing of entire network by dropping the packets in the network. The load is evenly balanced depending upon the capacity of the nodes. In this way multi hop load balanced network is achieved.

2. *Communication Phase*: The main job of communication phase is to avoid the same data packets transmitting through the same node repeatedly to deplete the batteries fastly and leads to network death because of vampire attacks.

The process of repeating the packets is eliminated by aggregating the data transmitting within the forwarding node

International Journal of Engineering Research
Volume No.3 Issue No: Special 2, pp: 107-111
ISSN:2319-6890)(online),2347-5013(print)
22 March 2014

and route the remaining packets safely to the destination. The data aggregation is achieved by first copying the content of the packet that is transmitting through the node. This copied content compares with the data packet that is transmitting through the node if the transmitted packet is same the node stops the data packet transmitting through them. In this way it avoids the redundant packets transmitting through the same node again and protect the depletion of batteries fastly. Then send the required data packets through the established node safely to the destination. The flow chart of the algorithm is given below in fig.6.

Average Energy Consumption for varying message lengths

Fig.7 shows the average energy consumption of the network with variable packet size. In the data communication phase transmitting data at varying message lengths of 8kbits/packet and 10kbits/packet respectively. From the plot it is observed that when message length is 8kbits/packet the energy is less than 1J and the energy consumption is greater than 1J when packet size is 10kbits/packet. That is when the message length is increased the average energy consumption of the sensor network is more. This is quite obvious because of greater overhead involved in aggregating and transmitting a larger sized packet or message. A message length of 8kbits/packet as lesser length message may not be in a position to carry out the desired task and a larger length may unnecessary contribute to addition overhead which can degrade the performance of the network.

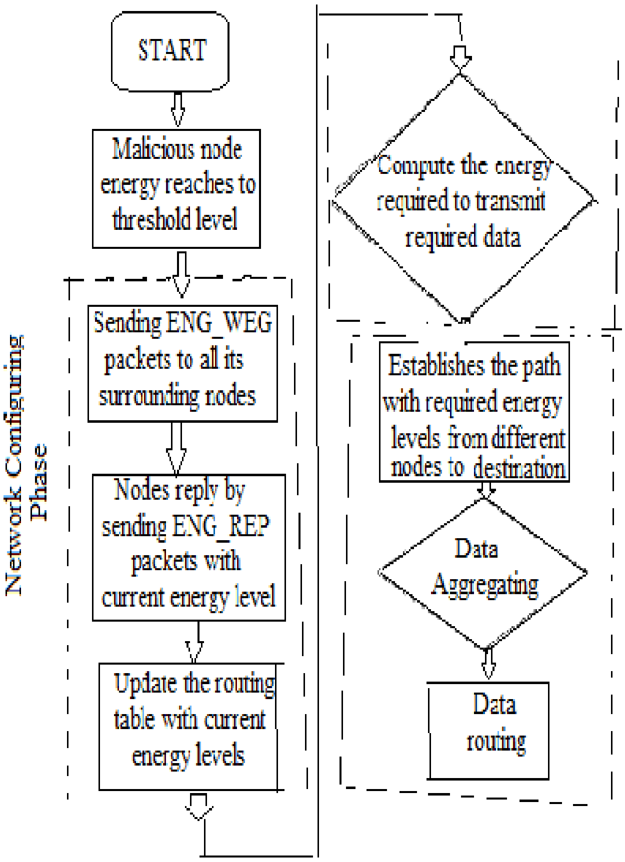

Fig.6.EWMA Algorithm flow chart.

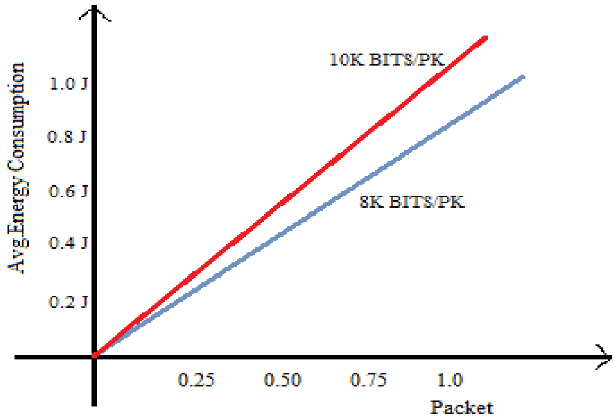

Fig.7.Average Energy Consumption with variable message lengths

Individual Energy Consumption in the network:

Fig .8 shows the individual energy consumption in the network that is the energy consumption of each node is shown in the analysis graph. Totally it is a network of 50 nodes .In the observation it is clear that energy consumption of every node is different. Intially all nodes have the intial energy of 85J. But after network intialisation the node whose energy drains very fastly is attacked with vampire. From the plot the energy of the 30th node is very low that is 15J and it is a malicious node.

Average path length comparison:

Fig.8. shows Average path length comparision of EWMA path length with attacked or malicious path length. In the figure from the observation it is clear that Attacked path length takes a Hop count of approximately 150 but with EWMA it takes only a hop count of 60 for a network size of50 nodes that is a malicious path takes 150 hops for a message to reach its destination but with EWMA we can transfer with 60 hops to reach the destination.

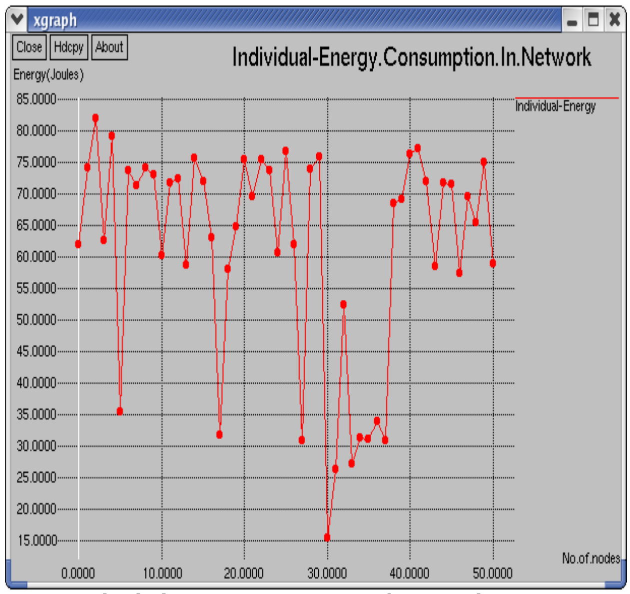

Fig .8.Individual Energy Consumption in the Network

From the analysis of Fig.9 we can easily understood how much energy is consumed to transfer a packet with 150 hops and with 60 hops. The 150 hops takes more energy and delay than the packet travels with 60 hops.

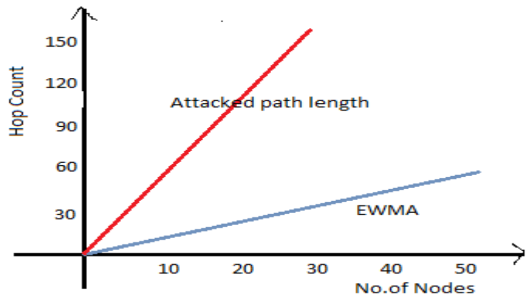

Fig.9.Average path length comparision of EWMA with attacked path.

Effect of adverse nodes on the network:

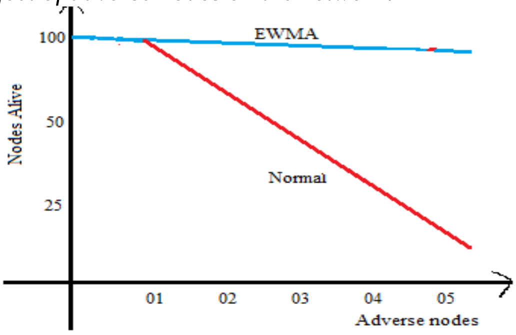

Fig.10. Effect of adversary nodes on the overall network.

In the fig.10 it clearly shows the effect of adverse nodes on the normal nodes. The analysis shows that if a node is malicious it will cause to death of nodes that is the nodes alive are rapidly decreased. As increase in the number of malicious nodes there is increase in the death of normal nodes.

But With EWMA we can increase rate of nodes alive. It is clearly understand that if 5 nodes are affected with vampire it will approximately cause to death of 75 percent of nodes. EWMA concept greatly avoids the death of normal nodes only there are two or three nodes for the overall sensor network. Thus EWMA Concept increases overall lifespan of network by energy efficient routing paths.

V.CONCLUSION

In this paper, we defined 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 using a small number of weak adversaries, and measured their attack success on a randomly generated topology of 30 nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases. Theoretical worst case energy usage can increase by as much as a factor of O (N) per adversary per packet, where N is the network size. The sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible. Derivation of damage bounds and defences for topology discovery, as well as handling mobile networks, is left for future work.

REFERENCES

i. *"The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns,2012.*

ii. *H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.*

iii. *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.*

iv. *J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.*

v. *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.*

vi. *J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Sys*