What is a Nanomesh Network?

A macro-mesh network is an array of active RF-based repeaters, or hot points. The hot points are each stand-alone wireless systems that can search for and communicate with one another, and also with up-line devices at a distance of 1000 yards or more.

A nanomesh network is the same as a macro-mesh network of active wireless devices, but tremendously scaled down.

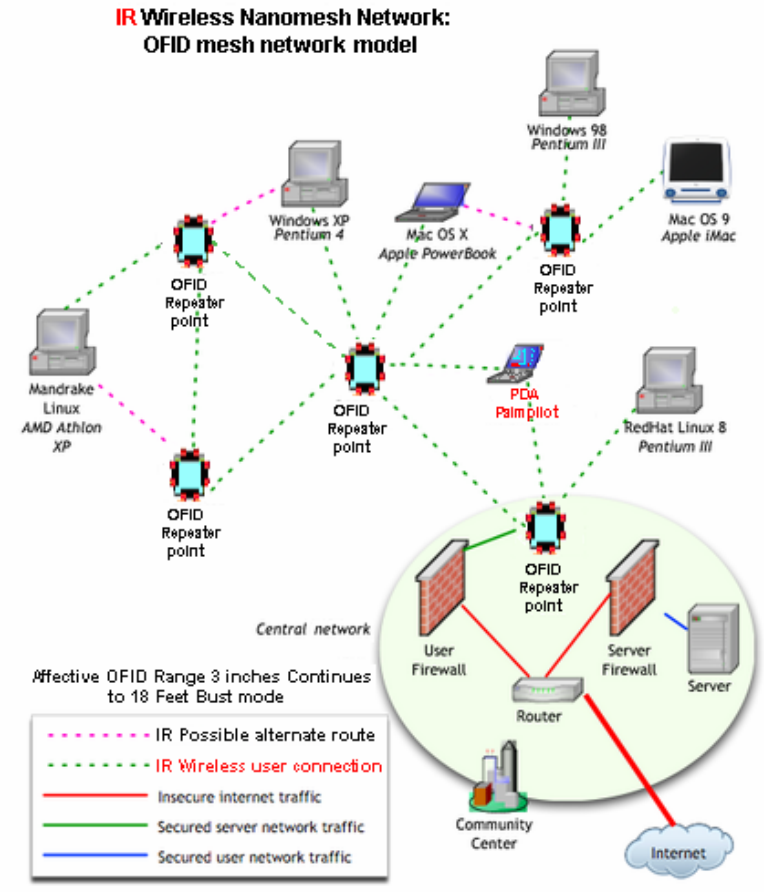
How do you make a mobile nanomesh sensor network (MNSN) that works in the real world?

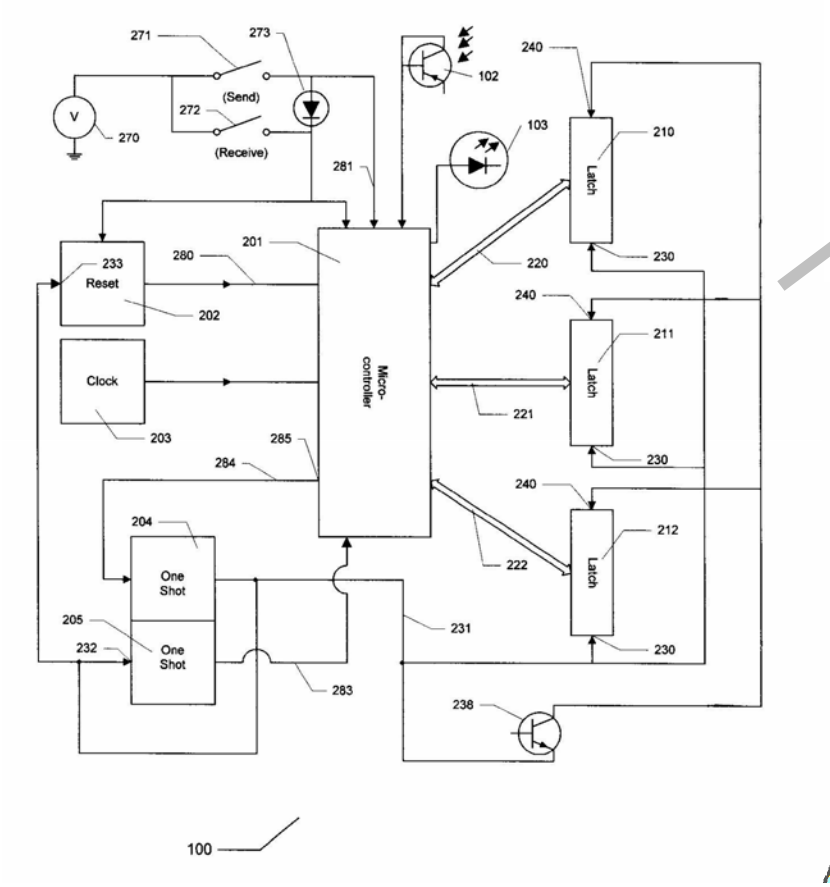
Active RF devices will not work. *Why?*
Not Scalable due primarily to antenna
Use too much power
Have too many support components
Need more processing power to support two erasable memories

A mobile nanomesh sensor network could be created with an array of active *optical frequency identification* "OFID" micro-devices that are built around a single circuit secure memory architecture.

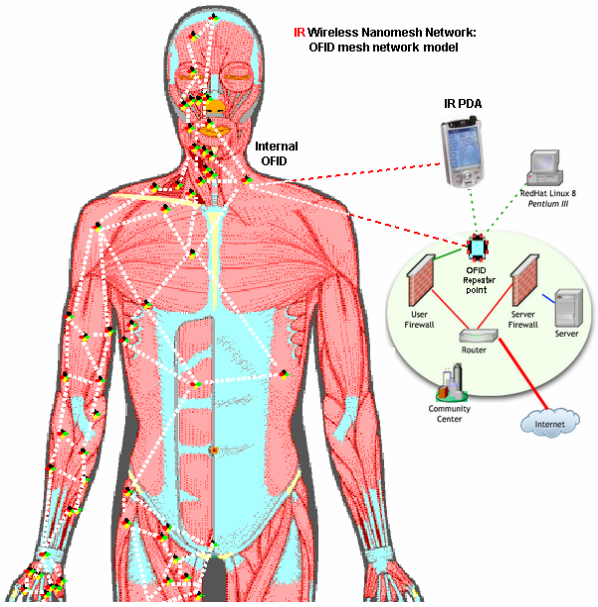
- uses very low power *infrared* emitters and detectors instead of antennae,
- requires far less processing power than active RF devices because the operating system serves only one memory space that is non-erasable and does not burden the CPU to confirm a transaction.
- requires fewer components than active RF devices
- point to point transmission from 3 inches in continuous mode, up to about 18 feet in burst mode.
- infrared transmission can penetrate translucent materials.
- cost continuously and dramatically goes down as the device shrinks in size
- entire device is scalable down to "smart dust"

To reduce collisions between data streams, the nanomesh can either use hardware with multiple emitter and detector frequencies, or process transactions via software. The single nonerasable memory of the active OFID will fill over time, and the device will thereby cease to function. This design can provide limited operational cycles for deposable nanomesh networks.





Mobile nanomesh sensor network of Active OFID micro-devices



Swapcard has invented and patented a "Secret Partner System" of data authentication especially for the single circuit secure memory architecture, which uses two private keys instead of handshakes.

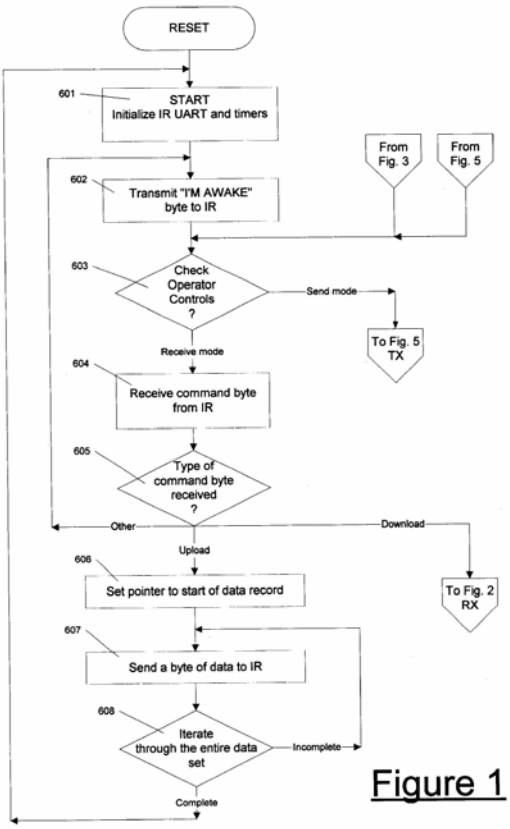


Figure 1

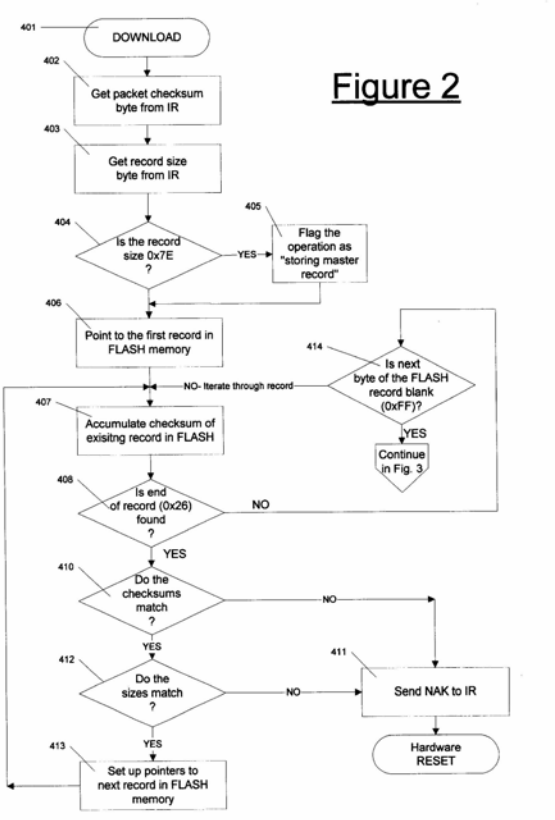


Figure 2

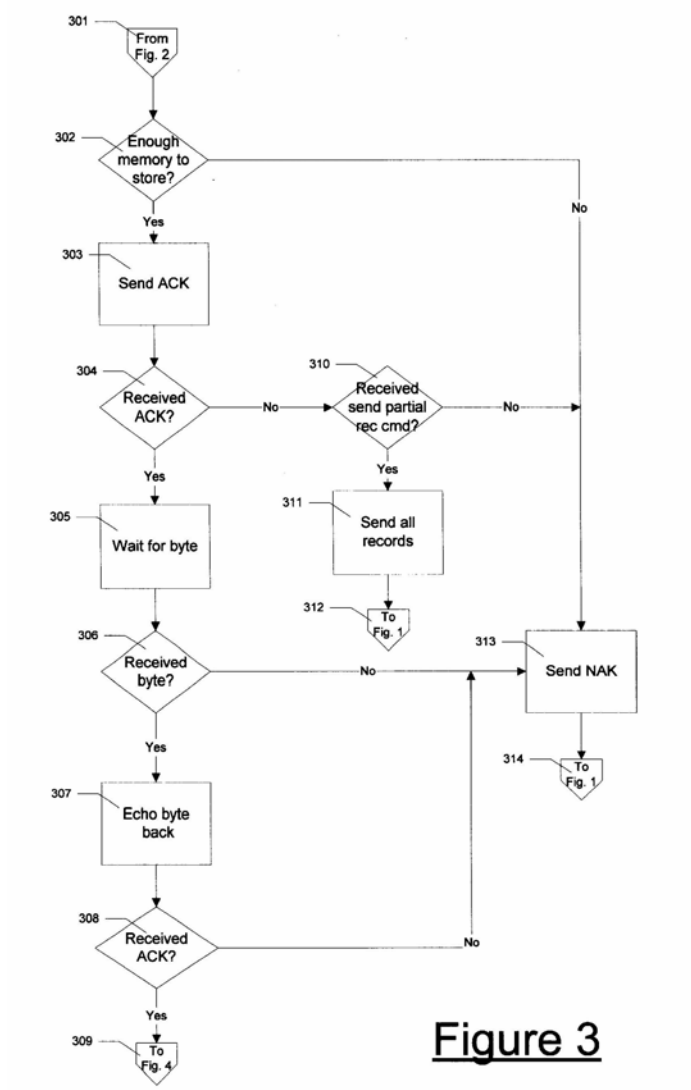


Figure 3

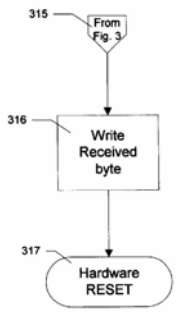


Figure 4

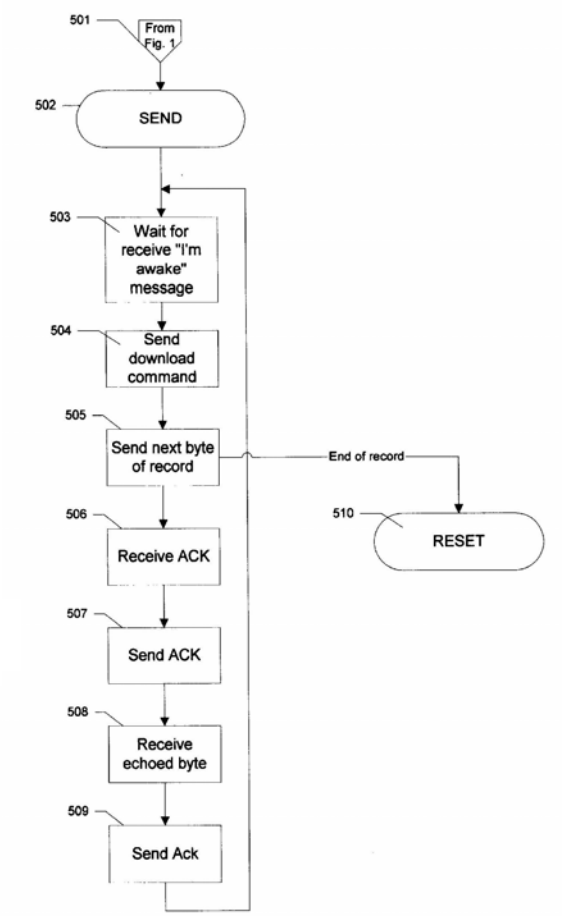


Figure 5

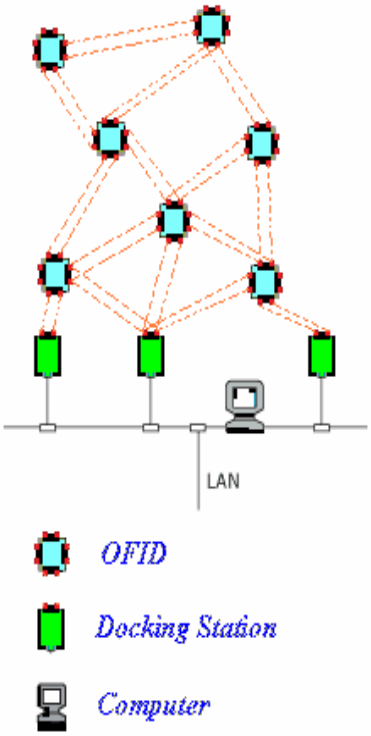
What is a single circuit secure memory and why is it an important innovation?

Almost all types of digital device that record data have read-write memories, such as the familiar hard disks or battery-backed CMOS memories. Many such devices also have volatile or RAM, *"Used as scratch pad or Stored",* memories and a further non-volatile memory such as PROM, EPROM and Flash. Thus existing devices *"use a two circuit secure memories i.e. scratch pad and a Stored"* either have read-write memories or multiple non-volatile memories each of which may be adaptable to a multitude of purposes and this flexibility is generally regarded as an advantage. In contrast, Swapcard, Inc., a Santa Cruz, CA start-up, has recently received a patent for a new class of integrated circuits, a *single circuit secure memory* **(US Patent #6553481).** The Swapcard single circuit secure memory has only *one non-volatile* memory space and that memory space is self-, one-time only-, programmable (SOTOP™), defining a single circuit memory architecture. The SOTOP™ memory is writable, but only under its own control program, and is not re-writable at all. The two primary novelties are that data is written while the processor is held in reset without an external programming system, and a co-operating peer computer assists in programming. These two novelties allow for the elimination of one of the memories. Thus, authentication systems based on this single circuit memory architecture use a proprietary software "secret partner" system of data authentication instead of the software handshake system commonly used with two circuit read-write secure memory devices. The secret partner security system is designed to complement the non-rewritability of the single circuit memory space.

Swapcard has incorporated its single circuit secure memory into an active (i.e. battery powered) optical frequency identification micro-device (OFID) as a verification of concept. The active OFID's can

be used for a mobile nanomesh sensor network (MNSN) as a proof of concept. Active OFIDs with single circuit secure memories have a number of distinct advantages over active radio frequency devices (RFIDs) using two circuit read-write memory architectures. These advantages include point to point data transmission, greater security, greater scalability, lower power requirements, and a very much lower cost. Swapcard's active infrared based active OFID can communicate wirelessly with other active OFIDs, desktops, laptops, servers and PDAs directly or through infrared docking stations. The active OFID can use and manipulate information across many operating platforms via Web sites and remote sources, with the flexibility to incorporate a variety of software plug-ins, filters, codes, public and private access keys, and encryption algorithms.

Existing devices with two circuit secure read-write memory architectures are not only more expensive than devices with SOTOP™ memory; they are also inherently more vulnerable to compromise. In an existing type of device, data is written from volatile memory into read-write memory under the supervision of a control program that is not located in the read-write memory. This opens up at least three means for tampering with the data. Firstly, after data is written, it may be completely erased without trace. Secondly, forged data may be rewritten in place of correct data. Thirdly, the control program itself may be altered.



In a single circuit secure memory architecture system, whenever data is written, it is downloaded to and held in steady state in peripheral components. After a short time, a byte (or word) moves from the peripheral components and is written to the permanent storage memory. With a single circuit secure memory, memory is not re-writable, so data written to the memory permanently and uniquely identifies and authenticates all transactions. Transaction history is not volatile and is incapable of subsequent modification. Any subsequent erasure of data, if possible at all (depending on the implementation of the control program), is 100% tamper evident since *erased storage* is different from *unused storage*. These are security advantages unique to the Swapcard single circuit secure memory architecture. Thus, the Swapcard single circuit secure memory device *gains* security from what it *leaves out* of manufacturing cost In order to compensate for their inherent vulnerability, two circuit memory architecture devices need a lot of processing power: to provide for highly sophisticated, relatively high bandwidth software for data authentication, communication with storage memory and servers, and to erase verified data from both of its memories. The needed sophistication of general purpose two circuit memory architecture devices is a major disadvantage and arises from these high operational power requirements. The Swapcard single circuit secure memory architecture uses a simplified approach that requires much less operational power and gains much from what it leaves out.

Swapcard's proprietary, **(US patent #6772239)** "secret partner" system of authentication, based on the patented single circuit secure memory, can provide higher security and operational assurance when enable as a *micro-mesh network* or a single authenticate memory pad compared to other two circuit memory architecture devices. Secret Partner (SP) uses one-time portable memory pad storage key management, which is the strongest key management system available. A series of unique random credentials (keys) are programmed into the single circuit secure memory during the manufacturing process along with a unique device identifier. As the active OFID device processes transactions, each transaction can be encrypted and authenticated using a copy of a unique one-time pad credential stored on a centralized authentication support system. A journal containing transaction information may be stored in the single circuit secure memory and transactions can be validated against journal entries

produced by the authentication support system. If the credentials in the one-time pad become exhausted, the low cost active OFID can be economically discarded. The streamlined architecture and low operational requirements result in low production costs making mass deployment inexpensive.

In the typical handshake approach used in existing devices for authenticating transactions, encryption keys or encrypted data get transmitted once every session and are subject to eavesdropping (snooping). The secret partner security system uses two separate private keys, one to encrypt at one location and one to decrypt at another location. These keys are unique for each transaction making the method invulnerable to snooping. An advantage with Secret Partner combined with single circuit secure memory is that the authentication device is single purpose. The device is produced to authenticate a series of transactions such as “the lock with the unique identifier X was opened by operator A.” Typically other active RFIDs are very small multi-purpose computers. Specific architectural information about existing active RFIDs and associated “development environments” enter the public domain. This makes counterfeiting of the active RFID relatively easy with non-production line methods. Swapcard active OFIDs combine a unique device identifier, portable one-time pad key management and permanent transaction documentation that cannot be counterfeited easily because all the authentication credentials are written during production and *only* become accessible as the device is gradually consumed. Moreover, any compromising of a Swapcard active OFID would require, at a minimum, physically breaking into the sealed-for-life and tamper-evident device (in addition to expensive and unusual manufacturing equipment).

While all digital security schemes are ultimately hackable, the non-rewritability of the single circuit secure memory makes it less vulnerable than either two circuit memory architecture or read-write architecture devices based on general-purpose designs. The general-purpose nature of two circuit memory architecture devices makes them more vulnerable to hacking and they can be cloned and counterfeited. This has been a frequent occurrence, for instance, with satellite TV systems, cell phones, GPS devices, and existing Smartcards. This vulnerability has required increasingly complicated encryption schemes, and increasingly more expensive hardware to support those schemes. Sadly, it is a truism that software engineers invariably seek to rectify defects by adding complexity, the Swapcard active OFID avoids that trap.

Active devices using two circuit secure memory are limited in the scalability of deployed applications because the high costs make wide deployment prohibitive. These costs arise out of the fact that those devices require a larger processor to work with two memory spaces, have a large number of peripheral components to support at least two different memory spaces. Also, active RFID devices have a relatively large antenna to transmit data in 360 degrees. Single circuit secure memory active OFIDs have infrared emitters and detectors instead of antennas. They have smaller processors and operating system using only one memory space, with far fewer peripheral support components. Point to point data transmission via light requires far less power than 360 degree transmission over any distance. The docking station of the Swapcard single circuit secure memory active OFID also has a low cost in comparison with the existing devices’ smart card readers or magnetic stripe readers.