

A MEANS TO ESTABLISH AND MAINTAIN SECURITY IN SHIPPING CONTAINERS

By Gerald A. Nadler, Chief Scientist - MachineTalker, Inc.

Defining the problem

The United States has 361 ports along the 95,000 miles of open shoreline in a 3.5-million square mile Exclusive Economic Zone. Ninety-five percent of cargo tonnage moving in and out of the country is by use of shipboard container (Figure 1). Each year, more than 7,500 commercial vessels make approximately 51,000 port calls, unloading over 7 million marine containers, less than two percent of which are subjected to any official inspection at all. According to the U.S. Department of Commerce, container cargo will quadruple in the next 20 years to approximately 30 million containers per year. The vast majority of these vessels sail under flags of convenience, registered in Tonga, Panama, Liberia, Cyprus, or the Bahamas, which means that they are not subject to control by any international authority.



Figure 1 - ISO Cargo Container

In October 2001, only weeks after the Sept. 11 attacks, authorities in an Italian seaport discovered an Egyptian man suspected of Al Qaeda membership hiding in a shipping container bound for Halifax, Nova Scotia. Airport maps and security passes were also found in the container, which he had outfitted with a bed and bathroom.

These conditions are an open invitation to individuals and organizations hostile to the United States who are rapidly gaining access to fissile materials, biological agents and other dangerous weapons. The potential that one of these millions of shipping containers will carry into the United States a nuclear device or a chemical or biological weapon of mass destruction is highly possible. It only takes one container with its lethal cargo to do enormous damage.

How do we implement a security system that can reliably and economically scale to an annual throughput of 30 million shipping containers within the next 20 years? This MachineTalker™ white paper will outline a solution.

Manual Inspection at the Source

Inspections of containers at the point of origin are a question of manpower costs, appropriate personnel security measures and background checks. The ability of the US to monitor hiring practices of security officials in foreign ports is highly dubious. From a financial point of view the average time required to load a shipping container is about three hours. A security inspector should be able to supervise the loading of at least four containers simultaneously, meaning that a single full-time inspector could supervise the loading of approximately fifty containers a week.

At the current annual influx of 7.5 million shipping containers, this translates to a full-time work force of about three thousand inspectors stationed at ports around the world. At a generous average salary of \$50 thousand a year, such an inspection force would operate on an annual budget of approximately \$150 million, increasing to \$600 million as container cargo quadruples over the next 20 years. These numbers can be considered conservative because of administrative and bureaucratic overhead.

NOTE: MachineTalker, Talker, MiniTalker, MicroTalker, TagTalker and SMMP are all Trademarks of MachineTalker, Inc.

Manual inspection only insures that when the containers are closed (sealed) that the cargo does not include any harmful contraband, although if each box in the container is not opened individually, dangerous cargo can still get aboard. Very often containers can sit in the storage yard prior to loading on the ship and thus are subject to tampering by people who can cut a hole (with a cutting torch) in the container and place dangerous material inside after it has been sealed.

Solving the Problem

In 2002 the U.S. Department of Transportation (Research and Special Programs Administration (RSPA) section) issued a Broad Agency Announcement (BAA) regarding container security. The DOT BAA requested a response for the solution to the problem of marine container security. The BAA included the following list of topics which the proposed solution should consider with appropriate comments. The list of pertinent topics is included below and will serve as an introduction to the MachineTalker solution to marine container security:

DOT BAA Shipping Container Security - Published Topics For Consideration
<ul style="list-style-type: none">▪ Real time risk management systems that can be scaled to address vulnerabilities and different levels of security threats.▪ Comprehensive risk profiling systems for container traffic including assessment of patterns, trends and performance of security systems.▪ Advanced systems for tracking container shipments from the point of loading and unloading at ports, conveyance and transportation in inter-modal systems and delivery to a customer.▪ Approaches for interlinking data on container information and cargo status including manifest information into a centralized national or global database.▪ Systems for identifying critical gaps in flow of container cargo information, processing, analysis and fusion of information for tracking containers and cargo between foreign ports and U.S. ports.▪ Technologies for remote or non-intrusive and timely detection of contraband materials including high energy release materials, explosives and weapons of mass destruction (WMD), chemical and biological agents, radiological materials or other hazardous materials or destruction mechanisms present in and around containers in single mode and multiple mode methods of cargo shipments.▪ Automated tracking and communication systems to report the status of container movements in transportation with capabilities to detect intrusions, anomalies or any attempts that compromise container integrity and sealing.▪ Advanced and tamper resistant sealing technologies including electronic seals for loaded and empty containers that produce a high level of sustained sealing integrity and performance, regardless of the mode of shipment and handling of the cargo.▪ Automated methods and tests to rapidly validate container sealing, integrity and sealing performance.▪ Concepts for advanced and self-contained design of containers with built in capabilities for communication, intrusion detection and cargo status.▪ Low cost and disposable electronic seals with electronic ID's that record container designation and continuously record status and provide tampering alerts.▪ Long life battery technologies incorporated in containers to power electronic seals and self-contained communication capabilities.▪ Rapid and systematic inspection techniques for timely detection of potential anomalies in container sealing at any stage of the container handling process.

This white paper will address the above BAA requests using the MachineTalker sensor based wireless networks.

MachineTalker Wireless Sensor Networks

The operation of the MachineTalker wireless network is a key ingredient in the MachineTalker solution for marine container security. The MachineTalker network is classified as an ad hoc self-forming mesh network (Figure 2). This is in contrast to most of the wireless networks that people use on a daily basis. For example, the Wi-Fi (802.11) wireless networks used with laptop and desktop PCs require an access point for operation. This (Wi-Fi) type of network operates in a master-slave mode, and in order for one network node to contact another node it must go through the access point.

Alternatively, a MachineTalker ad hoc mesh network does not require a master because all network nodes are "peers" and equal in functional characteristics. The MachineTalker network is self-forming and during startup, when power is applied, each network node goes through a discovery phase to "find" other wireless nodes within direct radio range. Operating in this peer-to-peer arrangement all MachineTalkers within radio range exchange information directly and form a "community". If any community member is out of radio range relative to some of the others, then those members that can "see" it, act as intermediaries to keep the community together (See Figure).

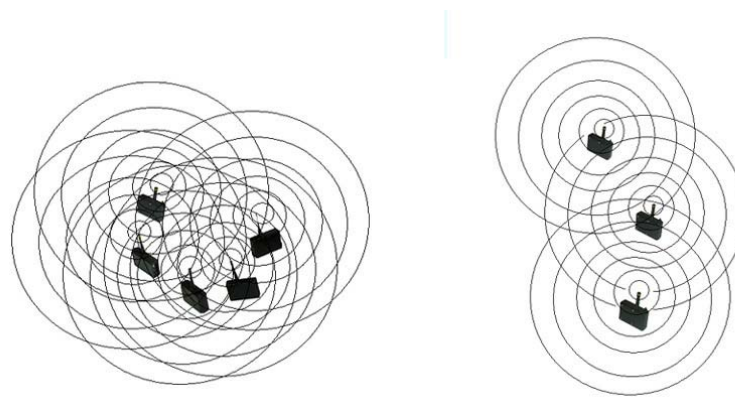


Figure 2 - MachineTalkers In Wireless Mesh Network Communities Of Differing Shapes

MachineTalker networks can also be organized into communities of small networks with the same functionality. These cooperating units can form redundant and self healing networks in case of failure. All MachineTalker wireless sensor nodes operate from battery power. Depending on the application, wireless sensor nodes can remain operational for 2-5 years on AA batteries.

All of these features can be utilized to build wireless sensor networks for marine container security.

MachineTalker Wireless Networks for Marine Container Security

At the present time the MachineTalker demonstration units are about the size of a business card. The size can be reduced to postage stamp size depending on the number and type of sensors (without battery). The MachineTalker wireless sensor node would be placed within the container

at any appropriate location. It can be affixed to the door, walls or ceiling, and Velcro or another more permanent form of attachment can hold it in place.

Because of community relationships, if the MachineTalker in one container detects an anomalous change it would communicate this to MachineTalkers in adjacent containers where the information can be checked against conditions in their own enclosures. The MachineTalker-based sensors inside a container could therefore be made to act in concert with other wireless sensor units in neighboring containers. The benefit of on-board MachineTalkers is that containers are made aware of themselves and carry with them the means to check themselves over, looking for unusual events.

Since one concern of container security is illegal entry the MachineTalker would manage a sensor connected to the door. If that intrusion sensor indicated that the door was opened the MachineTalker would issue an alarm to all other units within range. That alert could be sent to a human manned control station or to a MachineTalker that controls an audio/visual alarm or siren.

There are numerous types of sensors available for purposes of detection. In addition to illegal entry through the locked door, forced entry could be accomplished by cutting a hole in the container using a cutting torch. For this type of intrusion the MachineTalker would come equipped with a temperature sensor and a carbon dioxide sensor to detect an increase in carbon dioxide due to the presence of human beings (or other mammals) inside the container. Carbon monoxide sensors could be added to detect the presence of combustion products.

The recent concern with importation of weapons of mass destruction can dictate that small radiation sensors be installed in all containers to detect nuclear materials. Biohazard sensors are now coming on-stream and can be placed inside containers for constant monitoring of the air quality. The containers can be monitored for safety by detection of flammable or explosive gases that may form inside the container during transit. Finally, commercial value can be saved by examination of perishability parameters and incorrect environmental conditions that will endanger the cargo.

Another advantage of the MachineTalker network is that one does not have to wait for the container ship to enter the port to determine if there is a problem with the shipment. The container shipment status can be “read” at sea. A Coast Guard Cutter, helicopter or remotely piloted vehicle (RPV) can approach the ship and query the wireless network to send information regarding the condition and status of the cargo and the containers.

Each wireless network node has a powerful microprocessor that can contain a bill of lading for all the container contents. The non-volatile memory of each MachineTalker can contain literally thousands of lines of information concerning every aspect of the cargo including contents, port of embarkation, dates, times and an audit trail of sensor measurements throughout the entire trip.

All of this information can be “read out” and transferred to a back end database for data mining and inclusion in commercial databases. While in transit, a given container can inform handlers of its destination and can therefore be re-routed for efficiency or cost savings to different ships or loading facilities without becoming lost.

Position - Location (Figure 3)

MachineTalkers using advanced radio techniques can also determine relative position location to an accuracy of about one-half (1/2) meter. The containers when transferred from a ship can be tracked anywhere in a storage yard. If one MachineTalker is connected to a GPS unit giving absolute location (latitude and longitude) then the network can calculate the absolute position of each container, both stationary and moving, using triangulation techniques. This would help to recover “lost” and/or “missing” containers. As a container leaves the yard it may also leave its community of MachineTalkers, and this departure would be reported to an operator if necessary.



Figure 3 - Container Yard

Complete Solution to Marine Container Security

Using appropriate sensors the MachineTalker network can provide the basic raw data regarding the condition and location of marine containers. The knowledge to be gleaned from a MachineTalker network, or community, is only limited by the choice and variety of sensors.

Accumulation of data and immediate notification of any anomaly found within a container only targets part of the complete security system. The final step is the storage, analysis and post-processing of recorded information to look for trends or other vital details stored in the accumulated data from millions of containers being shipped.

Partnerships for Security Solutions

MachineTalker is teamed with two (2) other companies to achieve the complete solution and to implement a true security system for marine containers.

In the area of system integration the MachineTalker group consists of CACI (New York Stock Exchange, Symbol CACI) located in Chantilly, Virginia. CACI is a major prime contractor with system integration experience in government, military and commercial enterprises. CACI, with its global resources will provide the coordination to develop a complete and coherent solution to the worldwide marine security problem.

In order to provide for "data mining" and statistical analysis of the enormous database that will be created with the monitoring of millions of containers, MachineTalker has teamed with SAS (Cary, North Carolina). This large privately held software company is expert at all facets of gathering and processing statistical information like that from millions of sensors being serviced by MachineTalkers. The gathered data will be examined using algorithms to examine and correlate data and perform statistical analysis to look for possible trends that may indicate dangerous conditions. Such analysis may expose possibilities that are not immediately obvious by examining only small samples of data. Risk management can be accomplished by careful examination of all the security data that is gathered on a daily basis.

MachineTalker Has the Answers

The issues posed by the DOT BAA can now be examined in the light of the previous discussion, regarding a complete solution to marine container security as presented by MachineTalker, Inc. and its partners.

Real-time risk management and comprehensive risk profiling can be achieved by high level analysis using comprehensive data mining software components that look for a variety of patterns, trends and overall performance of security systems. The entire movement chain in an intermodal system can be tracked and examined from the moment the container is loaded to its final destination. At all stages there is a continuous stream of real-time data that can be examined and reported. Using appropriate security techniques all of the information can be reviewed from a host computer on the Internet. An individual located in Washington can determine the status of a shipment being loaded in Hamburg, Singapore or Hong Kong.

All manifest information including cargo status and container information is immediately reported and continuously monitored. This information is transferred using wireless networking. No human intervention or hand-held readers are required, like those used for bar codes or RFID tags. The MachineTalker radio node inside a container has all the pertinent information defining the container and its contents.

Since the flow of the cargo containers is being monitored, any critical gap in information delivery can be detected and one can determine the viability of the system at any moment in time. If any member of a MachineTalker community fails to report in a certain time period this condition is relayed or stored by the community for later access through remote connection. As a container ship approaches United States waters, Coast Guard Cutters, helicopters or remotely piloted vehicles can approach the ship and “read out” information about an entire ship in a matter of minutes using the wireless network (Figure 4). If required, the container ship can be equipped with a satellite link and the MachineTalker network can periodically report its enroute status via the satellite link to any location on the planet.



Figure 4 - Interrogation From Aircraft

Modern sensor technologies can be used for the detection of contraband materials including high-energy release materials, explosives and weapons of mass destruction, chemical and biological agents, radiological materials or other hazardous materials. MachineTalker is working with numerous commercial, government and university laboratories to determine the appropriate sensors to meet the challenge of increased security. These sensors can be integrated into the MachineTalker wireless network and will report any anomalies as required.

Once a container is sealed, multiple sensor arrays including those that detect temperature, carbon dioxide, carbon monoxide, motion detection, and other parameters, will insure that any attempt to breach the integrity of the container is discovered and reported. Since the interior of the

container is being monitored there is a real-time status that can be updated periodically indicating the present condition of the security system. If anything fails the entire MachineTalker community will record this information.

MachineTalker has performed radio propagation experiments with communications from inside standard marine ISO containers, yielding positive results. The MachineTalker demonstration units with sensors are about the size of a business card. They can be made considerably smaller and can be placed anywhere inside a container. If desired, they can be placed inside the container during the manufacture of the unit. For example a MachineTalker can be installed inside the plastic covering of the container air vent.

All MachineTalkers utilize battery power and depending on sensor type and duty cycle of the communications, a MachineTalker battery pack can last 2-5 years (The units notify the community if battery power is low).

Conclusion

The intelligent sensor-based wireless products of MachineTalker, Inc. when used inside shipping containers to provide on-board detection of events plus analysis of those events during long-term global movement of containers and contents will provide both immediate protection and determination of trends to promote both security and efficiency.

The team that can implement a working global system will include CACI to conduct the overall program, SAS to garner statistics to guide the future, and MachineTalker, Inc. to facilitate the technology for sensors and communications. Together, they can provide a viable and efficient solution to the problem of gaining and maintaining marine shipping container security.

Gerald A Nadler has been developing and applying wireless means for more than 25 years. Prior to his recent participation in the IEEE.802.15.4 standards committee, he has contributed to the advancement of early spread spectrum techniques and their use for military and industrial applications. Please email comments on this article to his attention to: info@machinetalker.com

MachineTalker, Inc. • 513 De La Vina Street, Santa Barbara, California 93101
West Coast: (805) 957-1680 • Fax: (805) 957-1740 • East Coast: (978) 897-2865
email: info@machinetalker.com • web site: www.machinetalker.com