THE SECURITY CONUNDRUM IN MOBILE AD HOC NETWORKS

Carla J. Miller Montroy, JD, 9600 Sandy Pointe Circle, Apt. 102, Fredericksburg, Virginia 22408, Cjmontroy.esq@gmail.com, (813) 293-5502

Jian Hua, University of the District of Columbia, 4200 Connecticut Avenue, NW, Washington, DC 20008, jhua@udc.edu, (202) 274-7138

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are wireless networks of various devices. MANETs face challenges and unique security needs that are not adequately addressed in most situations. This paper describes MANETS in today’s computing environment, and enumerates the unique security constraints and needs. This paper also provides overall suggestions for securing MANETs.

Keywords: Information Management and Technology, End-User Computing, Network Security, Intrusion Detection, Wireless Networks, Mobile Computing

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are multi-faceted aspects of everyday functioning in the professional/personal lives of users. Teleworking, global positioning systems enumerating directions, and military combat systems communicating from remote countries are only a few examples of numerous types of MANETs. One could drive down the road and connect his/her smart phone via cellular service to streaming music services, yet another example of using MANETS. A MANET is a wireless, short-lived and rapidly deployed network consisting of mobile nodes that communicate with one another by wireless radio links without the use of a pre-established, fixed network infrastructure or topology (Sahadevaiah & Reddy, 2011). Therefore, a MANET enables users to connect to the network anytime and anywhere.

Most users are accustomed to a wired network infrastructure at employment and /or perhaps having a personal Wi-Fi network at home. The usage of a Wi-Fi network at home and/or in a small office environment is an example of the simplest use of MANETs. However, regardless of the power of a MANET, the inherent security vulnerabilities must be acknowledged and mitigated. Challenges of connectivity and security management possess a much larger, global scale for an enterprise. It is a big headache for an IT department to ensure the confidentiality, integrity or availability of the information exchanged on a MANET while maintaining all the best practices tenets of security.

It is difficult as an IT professional in a large enterprise to anticipate the timing of entry to a MANET for each of the individual nodes while insuring adequate bandwidth and necessary resources for same. Since there is no established physical infrastructure (i.e. cabling, main server, backbone, client/server centralized topology) for a MANET, the IT professional faces a critical operational conundrum—how to secure the dynamic MANET to promote intellectual property, confidential data, asset security and availability of the network to authorized users.
BACKGROUND

Characteristics and applicable uses for the MANETs

There are universal attributes of MANETs collectively, regardless of the size of originating enterprise or usage. Some common attributes include but are not limited to: dynamic node movement, fluidity of the “infrastructure”, sporadic connectivity, dynamic physical topology, absence of centralized monitoring and management and lack of certificate authority (Sahadevaiah & Reddy, 2011). In other words, MANETs have no clear, established physical boundaries and lack client/server centralized network topology wherein security best practices can be deployed and maintained. MANETs are highly mobile, independent nodes that are resource allocation dependent and resource constrained. Resource allocation dependent and resource constrained pertains to limitations on the mobile nodes and MANETs such as memory allocation issues, energy consumption, and availability and bandwidth/throughput limitations. “Nodes” are various, stand-alone devices that connect via wireless radio signals to MANETs including, but not limited to, cell phones, smart phones, laptops, tablets and other devices of the like. Each individual node connects to and communicates through an access point and operates as the end node as well as a router for other nodes on a MANET (Hubaux, Buttyan, & Capkun, 2001). A MANET node utilizes Wi-Fi, cellular, Bluetooth or satellite transmission mediums to form the network.

The application of MANETs by an organization or enterprise is dependent upon the size of an organization, goals and resources of same. MANETs can be used for mission critical uses such as emergency situations, natural disasters and/or medical and military defense situations (Karthikeyan & Srivatsa, 2012). MANETs are suitably deployed for emergency, natural disaster and military situations due to minimal configuration, quick deployment and an absence of a central governing authority (Hubaux, Buttyan, & Capkun, 2001). For example, wireless sensor networks (a form of MANETs) are gaining popularity in the military and emergency services realms due to the low cost of the solution, coupled with the ability to deploy large sensor arrays in a variety of conditions (Deb, Chakraborty, & Chaki, 2011).

Another unique example of a MANET is deployment into autonomous vehicles, known as Vehicular Ad Hoc Networks (VANETS). VANETS, a growing area of MANET usage, enables traffic monitoring and direct communications between various vehicles without cell usage (Karthikeyan & Srivatsa, 2012). An example of VANET usage may be an emergency vehicle responder (mobile node) that communicates with devices/access points along interstates regarding emergency situations such as disabled vehicles, inclement weather, road construction and medical emergencies. The information from the vehicle mobile node is communicated to the stationary access points located roadside. Other MANET examples include but are not limited to the usage of diverse devices such as laptops, tablets and smart phones on a radio wireless frequency range that are enable other nodes to communicate despite the lack of existing infrastructure.
The Importance of MANETs Security

The highly related tenet for MANET security is known as non-repudiation. Non-repudiation ensures that the users/nodes provides the transmission or reception of some data and requires the use of public key cryptography to provide digital signatures (Gupta, 2011).

Defense-in-depth refers to a layered, onion like approach used to harden and protect a traditional, wired system. In turn, this practice bolsters the IT security position of a company and provides a framework to frustrate potential attackers and hackers. Defense-in-depth includes the initial physical security of an organization’s facility, however extends much further in a layered fashion to include other measures on networks such as firewalls, identification, authentication and authorization access controls, encryption, logical separation of servers, separation of user duties, deployment of routers and switches, system monitoring via an intrusion detection and/or intrusion prevent system, installation and maintenance of patch and upgrades and so forth.

Information security within an organization is of critical importance within any wired or wireless infrastructure of a private, public or governmental enterprise. Regardless of the type of company, proprietary information, trade secrets and personally identifiable information (PII) for clients and of the company must be safeguarded to protect a company from liability and irreparable harm. Due to the deliberate or inadvertent mishandling of PII or other sensitive and/or critical data, the organization could be subject to a lawsuit under any number of applicable federal laws and statutes including, but not limited to: Heath Insurance Portability and Accountability Act (hereinafter referred to as HIPAA), the Sarbanes-Oxley Act of 2002 and the Gramm-Leach-Bliley Act of 1999 (hereinafter “GLBA”). It is imperative that the organization practice IT security best practices (such as a layered defense-in-depth approach) to remain in legal compliance and to protect valuable assets-data, hardware, software or human capital regardless of the organizational infrastructure.

Provided for under HIPAA, a broad array of privacy and security rules were established to create safeguards against unauthorized use or disclosure of medical records and PII (O’Brien & Marakas, 2010). In particular, security rules pertain to Electronic Protected Health Information and incorporate three types of security tenets that are required for compliance: administrative, physical and technical. Any violations or misappropriation of private health information could result in serious sanctions and liability for corporations. This issue would be especially applicable to VANETS/MANETS of emergency and military personnel.

Under the Sarbanes-Oxley Act, the IT professional is charged with safeguarding the integrity of critical financial data of clients and the organization. Under GLBA, the company (financial institution) is required to develop and disseminate privacy notices that allow customers the option to prohibit institutions from sharing information with third parties. Therefore, any accidental or intentional disclosure of information is against the privacy notice that was disseminated to clients and could result in liability for each data spill/disclosure. Dependent on the type of organization and the nature of the data that was involved in a spillage (whether malicious or benign), the company could face civil and/or criminal liability and/or an unfavorable opinion held in the court of public opinion. Regardless of whether the company employs a traditional wired topology network or a MANET, the obligations remain unchanged.
Therefore, it is imperative that if a company chooses to allow proprietary and sensitive data to be accessed over a MANET by employees, that said company clearly understand the ramifications involved and exercise due diligence to protect the MANET. Understanding ramifications behind the use of a MANET requires the company to conduct a risk analysis and assessment in light of the security policy to ensure there are adequate safeguards in place.

**IDS Specifications and Implementation**

In IT security, the traditional IDS (known as Intrusion Detection) refers to another method employed by an organization to compliment the defense-in-depth approach. The choice of an ID is an educated decision made by IT staff in light of the physical network infrastructure, needs and goals of the organization, deployed defense-in-depth controls, IT overhead considerations, and criticality of data assets of said organization. The traditional IDS is software or hardware based, deployed on a wired network in “real time” to monitor and detect behavior anomalies in use by data collection, detection and response. As part of the IDS response, corrective action may be initiated, if necessary based upon set rules and policies (Madhavi & Kim, 2008). An IDS can be divided into two equally important segments: architecture that defines the operational structure of the IDS and the detection engine properties (Xenakis, Panos, & Stavrakakis, 2011). Traditionally, there are three different scanning variations of IDS signature, specification and anomaly based. Signature based IDS compares known attack signatures with ongoing system activities to detect any abnormal behavior; however this scan variation cannot detect new or undisclosed attacks (Sen & Clark, 2009). Specification based IDS has a set of specifications on any given program and a protocol to detect violations of said specifications (Sen & Clark, 2009). Anomaly based IDS profiles the normal behavior symptoms of the network and compares same to current usage, statistics, etc (Sen & Clark, 2009). When an intrusion is detected on the wired network infrastructure, an active or passive response by the IDS is deployed according to the set policies. A passive attack raises alarms to the appropriate IT staff as opposed to an active attack response that attempts to mitigate the intrusion (Sen & Clark, 2009). The placement of an IDS on the physical infrastructure of the network is located behind the firewall (on the intranet side) to detect any activity that is not blocked by the firewall. It can also be strategically placed on a physical network to monitor a critical server or segment. An IDS usage example occurs when the IDS on the network quarantines a large amount of suspicious traffic, while allowing legitimate traffic to continue to its destination.

However, as previously mentioned, an IDS is not easily utilized on MANETS due to the absence of a fixed infrastructure and central monitoring points (gateways, routers). Other inherent challenges facing the usage of an IDS/IPS on a MANET include, but are not limited to: device diversity, mobility freedom, limited energy and data resources, lack of clear defense and secure communications and lastly, cooperation between the various nodes (any node can pose as a neighboring node to participate in the MANET) (Sen & Clark, 2009).

**SECURITY PROBLEMS INHERENT TO MANETS**

The security requirements for an organization’s MANET depend upon the usage, goals and needs of an organization. Broadly speaking, there are numerous security vulnerabilities found in
MANETs, largely due to the lack of physical infrastructure and topology unique to MANETs. A noteworthy vulnerability in a MANET is the absence of a secure routing protocol and data forwarding weaknesses within same. This vulnerability is known as an attack on a basic mechanism (routing) of the MANET. Since the routing protocols are not specifically supported by an infrastructure or dedicated services, any individual node is subject to compromise of the routing protocol functionality simply by disrupting the route discovery mechanisms of the MANET. It is a critical vulnerability because each node discovers paths by which to communicate and send data. Accordingly, if a rogue or malicious node is repeatedly compromising one or more routes; the authorized, legitimate node must find a non-corrupted route to forward the data along on. As a result of this cycle (i.e. a node discovering and trying several different routing paths based on protocol such as Open Shortest Path First, etc.), delays and time-outs of transmission could occur. On a larger scale (from one malicious node to numerous malicious nodes and several compromised routing paths), the numerous, overwhelming attempts of the authorized nodes to find non-corrupted paths to transmit on would effectively cause a denial of service attack (active attack) on the MANET. A denial of service attack (DoS Attack) renders the MANET non-responsive and yields session time-outs to all authorized users.

In the realm of the previously aforementioned routing vulnerability, a MANET operates a peer-to-peer (one to one) connection (data transmission) wherein individual node serves as a self-configuring wireless access point and forwards packets to the next in a non-trusted way. Due to the very mobile and dynamic nature of the MANET, individual nodes are free to form associations with neighboring nodes, leave without notice, join the MANET at another time and location, etc. As such, this ability makes it difficult for the IT staff of an organization to have a clear picture of the MANET membership wherein no trust memberships among various nodes can be assumed. Each individual node serves as the single point of security failure wherein data could be sniffed, stolen, tampered with or some other data spillage could occur (against all three tenets of the CIA triangle). There is no method to ensure that paths to the various nodes are free of malicious activities, rogue nodes, etc. that would attempt to harm the MANET (by not complying with existing protocols) and/or organizational network as a whole.

Another critical security vulnerability inherent to MANETs is theft of information via eavesdropping. Eavesdropping, sniffing and theft of wirelessly transmitted data on the MANET are broken into different categories based upon the type of attack and status of the node. Typical eavesdropping of an unauthorized user that is solely used to gain valuable information off of the traffic channel (but does not disrupt normal functioning of the MANET) is known as a passive attack as opposed to an active eavesdropping attack that is performed to change the system and disrupt the normal functioning of the MANET. Active attacks on the MANET can be either internal or external in nature. Internal active attacks occur when an attack is carried out from cooperative nodes (the nodes cooperate with each other to establish the network) that are part of the network (such as hijacked nodes, node impersonation, modification, dissemination of false routing information for the packets, etc.) (Sahadevaiah & Reddy, 2011). Insider threats and attacks are very common and must be accounted for as part of security on wired networks. An external active attack is carried out by nodes that are not authorized to connect to the network (such as DOS, Modification, Jamming, Fabrication, etc.). Unfortunately, internal active attacks are the most difficult attacks to detect because hackers know the difference between the
organization’s private information on a compromised node and possess privileged access rights to the network resources from the hijacked node (Sahadevaiah & Reddy, 2011). There are several kinds of active MANET attacks with unique identifiers that are able to operate across every level of the OSI Networking model.

Attacks on existing security mechanisms can also occur, such as an attack on the key management mechanism of the MANET. A critical element in network security infrastructure is the use of cryptographic keys, such as Public Key Infrastructure (hereinafter referred to as “PKI”) to authenticate a user. Unfortunately, in MANETS, public keys can be maliciously compromised and/or the trusted key server may fall prey to malicious attackers. A trusted authority is necessary for the establishment of private keys of users. As such, given the lack of physical infrastructure in MANETS, it is generally not possible to have a trusted authority for the implementation of network security keys of symmetric key cryptography (Gupta, 2011). The alternative, asymmetric key cryptography is not without fundamental security flaws when employed in a MANET. Asymmetric key cryptography does not require trusted authority for key implementation; instead each node has a private and public key pair (Hubaux, Buttyan, & Capkun, 2001). Public keys are exchanged and shared with nodes; however private keys are kept confidential to the applicable node. However, security vulnerability exists with asymmetric key cryptography wherein one node has no way to verify that it received the actual authentic public key node of the other node.

Additionally, MANETS fundamentally lack sufficient, traditional physical, software and/or application security devices such as firewalls, intrusion detection and encryption that prevents the application of defense in depth mechanisms. The inability to initiate, deploy and maintain the use of traditional devices is largely due in part to the lack of centralized infrastructure and a client/server network topology or a hybrid, mesh topology. With a wired network that has known physical boundaries, a hacker must actually acquire physical access to a network element or pass through several layers of defense in depth to compromise the network (as defense-in-depth layering). With a MANET, the malicious node simply needs to enter the radio range of other nodes and it can communicate with the nodes in said range and join a MANET automatically thus enabling the malicious node to attack any node at any time (Li & Joshi). First and foremost, physical access to the network is secured by physical controls such as building locks, cameras, guards, man traps, CAC, smart cards, etc. Additionally, firewalls are the first layer of security that controls who and what has access to the network and can be nested inside and outside of the network (Poffenberger). Identification, authentication and authorization access controls work in conjunction with each other as part of confidentiality and integrity in which each user must have a password or some other authentication token to be authorized to use the system. This practice is referred to as two-tier authorization.

Additionally, all data crossing the wired network to one or more databases or to the internet should be encrypted to aid in the security practices of the organization. Routers and switches in traditional networking infrastructure also add security because the devices scan and monitor traffic for malicious IP traffic, etc. compiled from an access control list of known hacking addresses. Coupled with the firewall, an intrusion detection system and/or intrusion prevention system must be deployed to catch any remaining malicious activity that makes it past the.
firewall. On a wired network, IT staff monitors the network to aid in detecting traffic patterns and manages Windows and other updates system-wide which is not possible on a MANET.

MANETS are also vulnerable to physical security threats such as theft and other resource considerations, such as intentional and unintentional resource deprivation. It would be irresponsible of the corporate management to assume that nodes of the MANET are kept in a secured, locked environment free from the risk of theft and compromise. Mobile nodes, such as smart phones, laptops and tablets, are frequently stolen or could be misplaced; therefore granting access to the company’s confidential data by unauthorized parties.

Intentional and unintentional resource deprivation of mobile nodes refers to the shortage of essential elements that are unique to MANETs vs. wired infrastructures. In a MANET, nodes are assumed to be cooperative with one another. Nodes are expected to follow predefined rules in order to recover from collisions, share bandwidth, etc. A security vulnerability that could be exploited by a node is selfishness with the bandwidth thus causing data loss to the other nodes, or not relaying the packets to the other nodes in order to conserve battery resources (Hubaux, Buttyan, & Capkun, 2001). If the node is not cooperative with resources and/or communication channel rules, the resulting effect is unfair resource allocations to other nodes and an impact upon the network which effects availability or causing a DoS.

PROPOSALS AND ANALYSIS OF SOLUTION EFFECTIVENESS

Despite the dynamic nature of MANETS and the nodes therein; mobile users require security sustenance for individual nodes as they enter and move about the MANET to circumvent malicious nodes from freely moving throughout the infrastructure as well. However, two additional requirements must be met by any proposed IDS solution to be successful on the MANET which are low energy consumption and cooperation among the individual nodes on the MANET. A variation of IDS known as a mIDS (Mobile Intrusion Detection System) is tailored to mitigate weaknesses with a MANET in order to detect misbehavior among the nodes which includes packet forwarding anomalies and delays. Currently, there are three variations of MANET IDS architectures, and they are stand-alone, cooperative and hierarchical structures. Stand-alone IDS architecture consists of an IDS engine being installed on each node individually and only accesses the local data of said node. As such, this method is limited to locally available data to detect and resolve attacks (Xenakis, Panos, & Stavrakakis, 2011). Collaborative and hierarchical architectures process each host audit information locally, but use collaborative techniques to detect other attacks. An IDS engine is on every node to monitor local audit data and exchange information to detect and mitigate attacks (Xenakis, Panos, & Stavrakakis, 2011). The hierarchical architecture is multilayered; it segments the network into clusters based upon specific nodes and “cluster head nodes” for various IDS responsibilities (Xenakis, Panos, & Stavrakakis, 2011). Just as traditional, wired network IDS/IPS, the mIDS classifies attacks based upon signature, anomaly or specification based engines (with a pre-determined set of constraints to operate within each variation).

In addition, mIDS have two fundamental flavors of behavior of IDS systems based upon the aforementioned architecture schemes which are reputation and incentive based. Reputation based behavior detects misbehaving nodes and notifies all other nodes of same. Incentive based
behavior promotes positive behavior and cooperation among nodes (Madhavi & Kim, 2008). Accordingly, it relies upon a “monitor” node (there can be more than one monitor node on the MANET) that carries the identification process, overhears a certain communication channel and detects misbehavior (Madhavi & Kim, 2008). The mIDS must monitor the communication channel to ensure nodes are not ignoring the transmission protocol, jamming the channel or ignoring bandwidth requirements of other nodes. Further, the mIDS must incorporate the ability to detect anomalies and attacks in the packet forwarding mechanism of a MANET. Attacks on packet forwarding are numerous and include, but are not limited to the following, black hole, wormhole, routing loop, denial of service, cache poisoning, spoofing, dropped packets, false routing, etc. (Madhavi & Kim, 2008).

One of proposed kinds of a reputation based mIDS that operates as a stand-alone packet forwarding monitor is known as “Watchdog.” Watchdog detects malicious nodes, but does not report to other nodes (Deb, Chakraborty, & Chaki, 2011). By having a single node serve as the MANET monitor, it would reduce the strain on the resources of the other nodes (battery life, etc.) since IDS can carry a significant burden on the battery and bandwidth resources of a MANET. Watchdog operates in conjunction and as a complement to another program called “Pathrater”. Pathrater operates on an individual node (aids in limited resource issue) to rate all of the known nodes in the MANET regarding their reliabilities (Li & Joshi). Individual nodes start with a neutral rating and then are scored in light of said node’s behavior. Weaknesses inherent to Watchdog and Pathraters include misbehaving nodes which manipulate channels and escape detection by dropping packets below the set threshold level (Deb, Chakraborty, & Chaki, 2011).

An additional proposed mIDS serving as a compliment to Watchdog is CONFIDANT. CONFIDANT, much like Watchdog, is based upon the anomaly and reputation “flavors” of IDS and rates nodes based upon their behavior. Additionally, it reports misbehaving nodes to neighboring nodes. CONFIDANT is successful in the delivery of packets to the intended destination; however a drawback is that CONFIDANT assumes that there are several redundant paths to the destination node (for avoidance of malicious nodes) (Deb, Chakraborty, & Chaki, 2011). This assumption is simply not true all of the time and this outcome is not guaranteed.

Another proposed approach to reputation based IDS is called HIDS (Honesty Intrusion Detection System). HIDS is an anomaly based IDS engine that assigns honesty and trust values to each node based upon its behavior against normal baseline behavior. However, there is also incentive based behavior built into this model. When anode behaves normally, its trust value is increased and is rewarded wherein misbehavior results in the opposite reaction (Deb, Chakraborty, & Chaki, 2011). HIDS provides some safeguards against false positive results with a lower use of bandwidth and storage overhead. One downside of HIDS is that tables for anomaly scanning must be kept up to date on each individual node, hence causing some IT staff overhead, route detection weaknesses and energy resource limitations.

A hybrid mIDS solution was proposed that takes elements of Watchdog and Pathrater and combines it with another model (SCAN) to form what is known as Umpire. Umpire is a stand-alone IDS for a single node; however it also operates as collaborative IDS for multiple nodes (Deb, Chakraborty, & Chaki, 2011). Umpire addresses routing misbehavior and packet
dropping; however it is not fluent in detection of DoS attacks. There are more drawbacks than positive attributes with this model because leader election of a node is required which consumes more energy, said leader node may become comprised and/or malicious, and the nodes are not rewarded for normal behavior on the MANET. By the selection of a compromised leader node, the mIDS would have a greater chance of false positive readings and/or of not detecting anomalies at all.

Alternatively, new routing protocols for MANETS have been proposed to reduce the likelihood of a malicious node jamming or hijacking communication channels. An example of such a proposed protocol is known as Secure Message Transmission Protocol (hereinafter referred to as “SMT”). SMT uses a topology view of a MANET and determines a set of paths for connection of the source and receiver nodes with the concurrent usage of limited transmission redundancy (Papadimitratos & Haas, 2002). Each piece of a message (packet) exchanged on the network would be equipped with a cryptographic header which provides protection as it is transmitted from the source to the destination node. Upon completion, the destination node acknowledges and puts the pieces together. Contributions of this proposed routing protocol include: redundancy, security association via symmetric-key encryption, low overhead and fault tolerance (Papadimitratos & Haas, 2002). Weaknesses of this proposed routing protocol are as follows: limited protection against the use of compromised topological information resulting in a failure and incorrect routing information (Papadimitratos & Haas, 2002). Incorrect routing information could direct data straight to the malicious party’s compromised node or drop the data transmission altogether.

Key Management, similar to routing protocol proposals, forms another promising area for future MANET solutions. One such proposed key management solution relies upon the usage of private-public key cryptography and digital signatures by ensuring that each node is not responsible for issuing public key certificates to other nodes (Sahadevaiah & Reddy, 2011). Instead, an intermediary node would verify the digital signature of its neighbor to prevent the public key certificate from being modified during transfer. The public key certificate arrives at each node via symmetric key encryption. This proposed key management system, aptly named Cryptographic Hybrid Key Management for Secure Routing in MANETS, strives to achieve a confidentiality tenet using message encryption with the sender’s AES symmetric key and the receiver’s RSA public key. Both of these keys are then used to encrypt the AES secret key (Sahadevaiah & Reddy, 2011). Lastly, it is encrypted with the sender’s RSA private key (Sahadevaiah & Reddy, 2011). The encryption and the key management used in this scenario is used to combat sniffing, war driving and eavesdropping, stealing of the data during transmission, vulnerabilities within MANETS generally.

In the same category of solutions as Public Key infrastructure and routing protocols, the use of a Virtual Private Network (VPN) should be employed for any remote access nodes that access organizational resources from a MANET. The remote access users should use two-factor authentication access control via RADIUS or TACACS+ implemented on the physical infrastructure side of servers with a properly configured firewall to allow or deny traffic on various ports. Additionally, the organization should have a Remote Access Server that utilizes the options of Caller Id and Callback.
CONCLUSION

As one observes, there are no straightforward and simple solutions for the security vulnerabilities that are inherent to MANETS. The conundrum herein presented demonstrates IT professionals and corporations do not have a “silver bullet” to harden and defend MANETS. Each proposed solution enumerated above has merit; however, not a single option is a comprehensive solution to security vulnerabilities of MANETS. Keeping in line with IT security best practices, defense in depth is necessary to safeguard organizations as well as the users utilizing MANETS. To restrict an organization from the use of MANETS (especially in the mission critical military realm) is a significant disservice, but necessary in light of a risk assessment until the shortcomings of MANETS can be mitigated. It is incumbent upon an organization to evaluate the uses, needs, goals and resources of same to determine whether to assume the risk of the use of a MANET in compliance with the organization’s existing IT security policies and practices.

REFERENCES


 http://www.sans.org/reading_room/whitepapers/bestprac/computer-security-law-protect_1430
