Proceedings of the 2005 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY

Wireless Sensor Network Denial of Sleep Attack

Michael Brownfield, *Member, IEEE*, Yatharth Gupta, *Member, IEEE* and Nathaniel Davis IV, Senior Member, *IEEE*

Abstract* – *With the progression of computer networks extending boundaries and joining distant locations, wireless sensor networks (WSN) emerge as the new frontier in developing opportunities to collect and process data from remote locations. Like IEEE 802.3 wired and IEEE 802.11 wireless networks, remote wireless sensor networks are vulnerable to malicious attacks. While wired and infrastructure-based wireless networks have mature intrusion detection systems and sophisticated firewalls to block these attacks, wireless sensor networks have only primitive defenses. WSNs rely on hardware simplicity to make sensor field deployments both affordable and long-lasting without any maintenance support. Energy-constrained sensor networks periodically place nodes to sleep in order to extend the network lifetime. Denying sleep effectively attacks each sensor node's critical energy resources and rapidly drains the network's lifetime. This paper analyzes the energy resource vulnerabilities of wireless sensor networks, models the network lifetimes of leading WSN medium access control (MAC) protocols, and proposes a new MAC protocol which mitigates many of the effects of denial of sleep attacks.

Index terms –Wireless Security, Sensor Network, Energy Efficiency, Medium Access Control (MAC)

I. Introduction

The progressive nature of the Information Age creates increasing demands for processed data, and the consistent fulfillment of Moore's Law produces smaller hardware devices with improved capabilities to gather and process new data. As world business becomes more mobile and computational applications become widely distributed, wireless networks bridge the gap by making distance and movement seamless. Wireless networks require innovative medium access techniques to share the limited broadcast bandwidth in a fair and efficient manner as computing and communications devices continue to proliferate. Wireless sensor networks (WSN) offer the ability for applications to remotely monitor and react to events, but their remoteness also introduces challenges and vulnerabilities for network control and energy consumption. This paper analyzes the security vulnerabilities of a denial of sleep attack against three leading energy-efficient sensor medium access control (MAC) protocols and proposes a new WSN MAC protocol which dramatically mitigates its effects.

In an effort to make inexpensive sensor platforms ubiquitous, these platforms have limited processor capability, memory capacity, and battery life. Small system platforms which integrate sensors, processors, and transceivers are referred to as *motes*. Table 1 illustrates the power and memory limitations of four leading motes. The first mote, Smartdust, is the result of a UC Berkeley/DARPA research project which designed and built a $1mm^3$ WSN platform [1]. This device represents the extreme limit for WSN resource constraints. The 60kB and 128kB EEPROMs on the other three motes also significantly limit the code size available for sophisticated protocols. Developers implement sensor protocols in NesC, a structural, component-based programming language, and link it to the hardware through a open-source operating system called TinyOS. As technology advances, the wireless sensor trend will continue building physically smaller and more energy-efficient platforms.

Table 1. Mote Microcontroller/Transceiver Platform Specifications

Platform	Smartdust	Mica2 [2]	TelosA [3]
Micro-controller	8-bit	16-bit ATMega 128L	16-bitTI MSP430
MCU RAM	512B	4kB	2kB
EEPROM	512B	128kB	60kB
Radio	916MHz	868MHz CC1000 [4]	2.4GHz CC2420
Data Rate	10kbps	76.8kbs	250kbs

Besides the classical denial of service attacks that plague the IEEE 802.3 wired and IEEE 802.11 wireless networks, WSN networks have a unique vulnerability due to their fixed energy capacity upon deployment. The mote systems generally operate on two AA batteries (3.0 volts) with an approximate 3000mAh energy capacity. Malicious attackers can easily target the battery supplies and reduce network lifetimes from years to days. Achieving a secure system requires security integration into every component to prevent a vulnerable point of attack [5][6]. WSN designers must incorporate the protection of the critical energy resource into the system architectures.

Michael Brownfield is a Ph.D. candidate, Yatharth is senior undergraduate student, and Nat Davis is a Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University. Email: {brownfld, yatharth, ndavis}@vt.edu.

0-7803-9290-6/05/$20.00 ©2005 IEEE.

II. Related Work

Most security research focuses on protecting confidentiality, data integrity, and service availability. These protective measures are mature in wired and infrastructure-based wireless networks and continue to strengthen in response to increasingly smarter attacks. Confidentiality protects against the improper disclosure of information; data integrity protects the information against improper modifications; and service availability prevents denial of system services. The WSN denial of sleep attack is a subset of the denial of service class of network attacks. Stajano and Anderson [7] first mention denial of sleep attacks in 1999 as "sleep deprivation torture." Energy-limited system designers often incorporate power management mechanisms to monitor active processes and power down non-essential subsystems when feasible. A denial of sleep attack penetrates a device's power management system to reduce the opportunities to transition into lower power states. Stajano and Anderson proposed either charging for service access or requiring users to perform a resource intensive function, such as solving a puzzle, in order to gain access. Since then, many researchers have studied the effects of battery intrusion for a variety of mobile devices, laptops, personal data assistants (PDA), and wireless sensor networks.

In analyzing battery attacks against PDAs, Martin et al. [8] divide sleep deprivation into three categories: service request power attacks, benign power attacks, and malignant power attacks. A *service request power* attack repeats valid service requests with the deliberate intention of draining power; a *benign service attack* initiates a power intensive operation on the device under attack (DUA) to quickly drain power resources; and a *malignant power attack* penetrates the DUA and alters existing programs to consume more power than required. To counter these attacks, Martin et al. propose a system architecture which provides multi-layer authentication and energy signature monitoring. The multi-layer authentication technique requires authentication for service requests accessing crippling energy level processes, ones that cause the DUA's lifetime to fall short of a target. An energy signature monitor polls energy monitoring units throughout the device and reports energy patterns. Upon detecting a suspected intrusion, the energy signature monitor compares the energy signatures in a database using either statistical- or rules-based anomaly algorithms [9][10]. These comparisons are feasible for a PDA platform which has the resources to store and analyze signatures. However, WSNs require simpler solutions to the same security challenges due to limited processing capability, memory storage, and energy capacity. Additionally, many attacks against PDAs may be caught by monitoring power variables and expected bounds of consumption, but in heterogeneous WSN networks, some sensors report routinely, while others trigger only upon the occurrence of environmental events.

The exposed wireless medium provides attackers with the ability to access a network without physically tapping into the system. Friendly traffic flows beyond intended boundaries allowing malicious attackers to obtain information from the packets and reuse it against the network. Additionally, the wireless nature allows them to penetrate the boundaries to launch denial of service attacks or attempt to access confidential information. Placed in remote areas, sensor networks are even more vulnerable to attack than the wireless infrastructure networks due to the inability to provide any physical security in protecting the network.

WSN defenses against denial of sleep attacks involve protecting the power management mechanisms at the architectural level. Since the transceiver on the WSN platform consumes the most energy and is the primary source for power management savings, defensive strategies implemented at the network link or MAC layer are the most effective in protecting radio usage [6][11][12].

Two direct link layer attacks which impact a WSN node's energy supply are link layer collision and link layer exhaustion [6]. A *collision attack* against the link layer, like jamming in the physical layer, occurs when an attacker sends a signal at the same time and frequency as a legitimate message for as little as one octet (or byte) in a transmission to corrupt the entire packet [11]. Physical layer jamming countermeasures include frequency-hopping or code division multiple access spread spectrum techniques [13][14]. Once the attacker determines the hopping/chipping frequency or increases the jamming power level to achieve a sufficient signal-to-noise ratio, the transmissions begin to collide with the network traffic. If a link layer frame fails a cyclic redundancy code (CRC) check, the link layer automatically discards the entire packet. In addition to wasted bandwidth and sleep opportunities, this attack consumes critical energy for both the sender and receiver in subsequent retransmissions. One approach to counter the collision effects is to use forward error-correcting codes (FEC) to recover lost information [6]. Again, the attacker can counter this defense by extending the duration of the jamming signal to corrupt more bits to overcome the coding gain of the FEC. A link layer *exhaustion attack* occurs when an attacker manipulates protocol efficiency measures and causes nodes to expend additional energy. For example, an attacking node in an IEEE 802.11-based network could repeatedly send request-to-send messages (RTS) and force the node listed in the RTS destination field to respond with a clear-to-send (CTS) message and remain awake waiting for the follow-on message [11]. A suggested defense against this type of exhaustion is to

0-7803-9290-6/05/$20.00 ©2005 IEEE.

encrypt the control messages [14] or provide *rate limiting* by allowing nodes to ignore excessive network requests from a node. Rate limiting can easily be overcome by a distributed denial of service attack (DDoS) or an attacker who can iterate through many source identities in the anonymous wireless environment.

III. WSN Security Components

Authentication and encryption solutions for the resource-constrained WSN cannot achieve the same protection levels as wired and wireless infrastructure-based networks. Securing communications in WSNs entails a secure group approach in order to support nodes communicating with one another while performing in-network processing and aggregation necessitated by wireless bandwidth limitations [5]. Additionally, individual node's limited key storage capacity prevents the use of per-link encryption strategies. This section introduces three leading software and hardware tools to maintain group security and performance for WSNs.

TinySec is a software-based link layer security architecture which provides the basic necessities in network security, authentication, and encryption [15]. The network link layer is the logical choice for implementing these security components in sensor networks since the sensor traffic tends to involve either source-to-sink or broadcast traffic (one-to-many), not end-to-end (one-to-one) traffic like traditional networks. TinySec is a module which works with the TinyOS operating system. The design goals are to provide link layer security measures to protect access control, message integrity, and message confidentiality without significantly impacting the energy and throughput of the network. TinySec pairs a two-byte counter and source field with the traditional TinyOS packet header fields (destination, active mode, length) to develop an initialization vector (IV). Since the IV uses integral header fields, the encryption mechanism minimizes control overhead. TinySec then combines the 8-byte IV with a cyclic block code (CBC), Skipjack, to attain reasonable security without a computationally complex algorithm. Experiments using Advanced Encryption Standard (AES) proved to be too slow without hardware acceleration. Additionally, TinySec replaces the medium access control frame's CRC field with the message authentication code to maintain the 8-byte security control overhead. To allow the sensor application the ability to tradeoff security to reduce computation and communication overhead, TinySec provides the ability to operate in three modes: open, authentication (TinySec-Auth), and authentication-encryption (TinySec-AE).

Offering a hardware alternative to TinySec's software components, IEEE 802.15.4 compliant radios have the ability to perform 128-bit AES hardware encryption on the radio platform [17]. AES is a Federal Information Processing Standard (FIPS) which uses a cryptographic algorithm to protect electronic data by implementing a symmetric block cipher to encrypt and decrypt information [16]. The Chipcon CC2420 [4] radio with integrated AES offers four security modes:

1. Disabled
2. Cipher block chaining (CBC-MAC) authentication
3. Counter (CTR) encryption / decryption
4. Counter with Cipher Block Chaining-Message Authentication Code (CCM) authentication and encryption / decryption.

As with TinySec, the integrated 802.15.4 security mechanism provides message integrity and confidentiality. Incorporating these algorithms using hardware and software routines located directly on the radio releases the processor's limited memory and processing capacity to handle other operations.

Security Protocols for Sensor Networks (SPINS) is a software security protocol suite developed by Perrig et al. at UC Berkeley for use in extremely resource- limited networks like the Smartdust $1mm^3$ device [18]. With only 8-bytes of packet overhead, the secure network encryption protocol (SNEP) provides data confidentiality, two-party data authentication, and evidence of data freshness. Another SPINS suite component, μTESLA, authenticates broadcast messages for resource-constrained networks. Although true authenticated broadcasts require asymmetric cryptographic mechanisms, μTESLA uses a resource-friendly symmetric mechanism, but interjects asymmetry through a delayed disclosure of symmetric keys. Security issues that SPINS does not address include denial of service attacks and compromised nodes. A significant limitation to this security system for dynamic WSNs is the requirement to have a base station with additional memory and energy resources and a static network topology.

The security offered by the current software and hardware implementations is insufficient to protect a WSN from a denial of sleep attack. The three basics options are to encrypt the data and the header, encrypt the data, or provide no encryption. Denial of sleep attacks force a sensor platform to stay awake and receive a transmitted packet. If the complete packet is encrypted, the sensor node must receive the entire packet, decrypt the header, and then determine if it is the intended receiver. The data-only encryption mode allows the node to view the header as it arrives, but the node will not be able to authenticate the sender until the packet data is decrypted. In this case, if the attacker is able to provide a legitimate source and destination, the receiver will stay awake to accept the entire packet. The link layer will then discard

any packets which fail the message authentication code check. The unencrypted mode expends the same amount of energy receiving the packet, and it will pass the incoming message up to the network layer.

IV. Link Layer / MAC Sources Of Energy Loss

Current methods in securing wireless sensor networks address the confidentiality and integrity of the data in the network. Due to their limited energy resources, WSNs remain extremely vulnerable to denial of service attacks by the draining of their most critical resource – their energy supply. Understanding both normal and malicious sources of energy loss is essential in designing a power control system. Typical sources of energy loss, and thus vulnerabilities, in WSNs include: frame collisions, message overhearing, and idle listening.

Frame Collisions: A frame collision occurs when a wireless sensor node sends a MAC protocol frame, or message, which collides or overlaps in time with another message. If the interfering signal strength is high enough, the data is corrupted at the receiving end. In most single-channel radios, the radio cannot simultaneously receive while in transmit mode. Therefore, the message sender's only indication of a collision is the failure of the receiver to return an acknowledgement (ACK) for the message. Frame collisions occur naturally in wireless networks due to the extensions of space and time in distributed radio networks. Finite radio receive-to-transmit transition times (the capture effect) ranging from 250μs to 500μs after sensing a clear channel, propagation delays between distant stations, and hidden nodes which are out of range of the sender, but within range of the receiver, are the leading causes for wireless frame collisions. Resending messages causes both the sending and receiving node to expend additional energy. Protocol designers reduce frame collisions by employing contention-free scheduling protocols or contention-based backoff algorithms to minimize the probability of collisions. Typically, link layer parameter settings permit a limited number of retransmissions before discarding a message. Building on the collision discussion in Section II, attackers may take advantage of this vulnerability by successively jamming small portions of a message transmission. This attack not only denies message exchanges, but also drains network energy from the additional transmissions.

Message Overhearing: Receiving and discarding messages intended for other nodes, or *message overhearing*, is commonly employed in non-energy constrained networks to increase throughput and decrease latency. Message overhearing is costly in WSNs since it causes all of the nodes to expend energy receiving a message intended for just one node. Two energy-efficient methods exist to reduce message overhearing: early

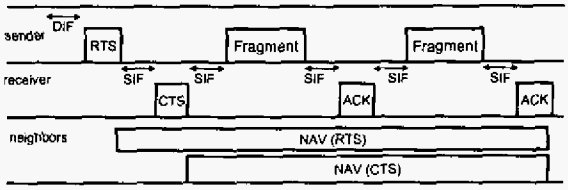

Fig. 1. Message Passing Overhearing Avoidance Strategy

rejection and message passing. Early rejection allows a sensor node to turn off its radio once it has read the destination field for an incoming unicast message or the group id for a broadcast message [15]. Message passing, shown in Fig. 1, allows nodes to schedule a sleep period during the overheard RTS-CTS handshake sequence by noting the message duration field and scheduling a network allocation vector (NAV) table interrupt [20][21]. An attacker could exploit message passing by broadcasting multiple RTS requests or CTS responses to keep nodes from transmitting and receiving network data. This attack denies network access and can increase network lifetime by continuously sending nodes to sleep.

Idle Listening: Non-energy constrained wireless network interface devices continuously monitor the medium for incoming transmissions. Idle listening occurs when a device listens to an inactive medium. Since many wireless sensor radios consume more energy during idle listening than during transmissions, energy-efficient WSN MAC protocols attempt to synchronize network traffic so that transmissions begin only in predetermined time slots. Once all network transmissions are complete for a particular cycle or time *frame*, the protocols allow nodes to return to sleep until the next transmission period. To launch a denial of sleep attack, attackers can determine the transmission and sleep rhythm, and then concentrate the attack at the end of the active period to force nodes to remain awake beyond the normal traffic requirements.

V. Contention-Based Sensor MAC Protocols

WSN designers strive to extend network lifetimes while meeting application-specific throughput and latency requirements. They achieve these savings by minimizing the opportunities of frame collisions, message overhearing, and idle listening. The most significant method to extend network lifetime is synchronizing nodes to actively pass data and then sleep as much as possible. Fig. 2 shows that the CC2420 radio consumes up to 19.7mA in the receive mode, but only 1uA in power off mode. With two 3000mAh AA batteries, the difference in lifetime of a fully active platform (20.1mA) and a sleeping platform (2.4μA) is 6.2 days vs. 143 years (or battery shelf life). Measurements on the CC2420 radio in the Telos A platform indicate a 0.470ms power off sleep transition and a 6.5ms recovery time. Effective power

management places nodes into the various power- saving modes based upon the duration of the sleep period and can extend the lifetime of a network by two to three orders of magnitude. Even with power management tools in place, unless a MAC protocol can create opportunities to sleep for long durations, the platform cannot achieve extended network lifetimes. This section presents an overview of the energy-efficiency strategies for three leading WSN contention-based MAC protocols and introduces a new energy-efficient protocol.

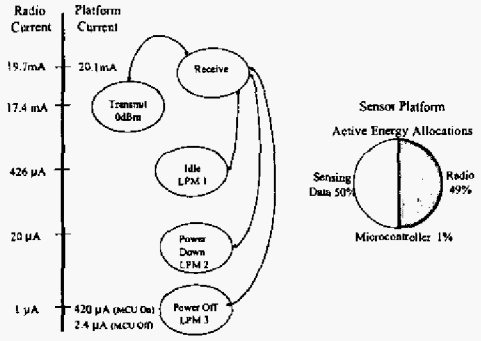

Fig. 2. Radio Energy Modes and Platform Energy Allocations [3][4]

A. Sensor MAC (S-MAC)

S-MAC [21] represents the baseline energy-efficient sensor MAC protocol designed to extend WSN network lifetime. S-MAC divides a time frame into listening and sleeping periods. Fig. 3 shows that the listen period is further divided into a synchronization period and data transfer period. The synchronization period allows nodes to periodically announce their sleep schedules to correct network time drift and synchronize their sleep times to form virtual clusters of nodes with the same active listen and sleep periods. By creating a 10% active duty cycle (D), node lifetimes can be significantly extended with bounded throughput and latency tradeoffs. Sensors that border two synchronized clusters have the option of choosing one or the union of both sleep schedules. The two nodes at the bottom of Fig. 3 illustrate the effect of having nodes whose sleep schedules do not completely overlap. If node 1 attempts to transmit to node 2 late in node 1's listening period, node 2 is already in sleep mode and will not be able to receive the message. Creating a slotted starting time for all network traffic and concentrating the traffic into a smaller time frame reduces idle listening, trading off latency and throughput. To minimize collisions, nodes use the IEEE 802.11 standard contention backoff for all channel access attempts. Furthermore, S-MAC also reduces energy consumption using the message passing techniques discussed in Section IV for overhearing avoidance.

S-MAC's sleep cycle is fixed at the time of network deployment. This limitation causes the protocol to be inflexible in responding to network traffic fluctuations or network scaling. On the other hand, the fixed sleep cycle

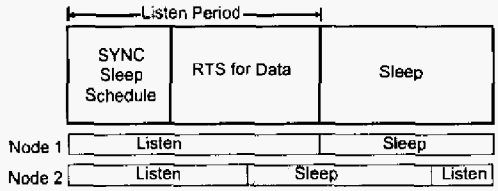

Fig. 3. S-MAC Frame architecture

protects the network lifetime from the denial of sleep attacks by ensuring that nodes are only vulnerable during a fixed listening period. S-MAC is most vulnerable to a broadcast attack in which an attacker sends multiple broadcast messages to keep all nodes active and receiving throughout the entire listening period. Let $T_{frame} = T_{listen} + T_{sleep}$ and $D = T_{listen}/T_{frame}$ (duty cycle $D \approx 10\%$) Since an attacker can broadcast a message to the entire network simultaneously, S-MAC's maximum network lifetime from a broadcast attack is:

$$T_{network\,lifetime} = T_{sensor\,lifetime} = \frac{C_{battery(mAhr)}}{(D)(I_{active(mA)}) + (1-D)(I_{sleep(mA)})} \quad (1)$$

S-MAC is also vulnerable to unicast attacks with back-to-back RTS messages, but the attack effects are limited to draining energy from one node at a time, while denying all other node's network access.

B. Timeout MAC (T-MAC)

Timeout MAC (T-MAC) [22] is also an energy-efficient MAC protocol designed to maximize sleep opportunities and builds on the successes of S-MAC. T-MAC obtains additional sleep time at the expense of increased throughput and latency. T-MAC adopts all of S-MAC's sleep methods (virtual clustering and message passing) and improves on the idle listening overhead by dynamically adapting the active listening period in response to network traffic. T-MAC permits nodes to sleep as soon as all network traffic has completed. As shown in Fig. 4, the end of traffic is signaled by nodes monitoring an idle channel for an adaptive timeout *(TA)* period which represents the longest period in which a hidden node would have to wait before hearing the first bit of a CTS message.

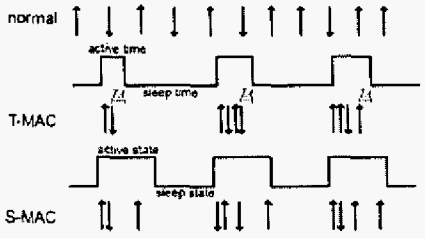

Fig. 4. T-MAC adaptive timeout [22]

The waiting timeout period is determined by the largest contention window (t_{CW_Max}), the time to send an RTS message (t_{RTS}), and the protocol small interframe spacing (SIFS) delay before the receiving CTS node can process a response to the RTS:

$$TA = 1.5 * (t_{CW\_Max} + t_{RTS} + t_{SIFS}) \quad (2)$$

Simulations showed the requirement for a 1.5 scaling factor to produce a stable network. Once a node has waited a timeout period without sensing any traffic, the node transitions to sleep until the next scheduled listen period. The arrows in Fig. 4 indicate message traffic and illustrate how T-MAC effectively condenses the traffic into a smaller time frame to reduce idle listening at the expense of increased message delay. In an event-based and periodic reporting scenario, T-MAC achieved five times the energy savings as S-MAC.

T-MAC is more vulnerable to a broadcast attack than S-MAC. If an attacker can get T-MAC network nodes to repeatedly receive broadcast messages, the attacker can force all nodes to remain awake throughout the sleep period, creating almost a 100% duty cycle. Eqn. 3 shows how one attacker can simultaneously drain the life of an entire network.

$$T_{network\,lifetime} = T_{sensor\,lifetime} = \frac{C_{battery(mAhr)}}{I_{active(mA)}} \quad (3)$$

C. Berkeley MAC (B-MAC)

Berkeley MAC (B-MAC) [23] takes a decentralized sleep schedule approach by allowing nodes to adopt any sleep schedule, but the sleep cycle frequency is fixed. At the end of a node's sleep period, a node wakes up and samples the channel using a process called low power listening (LPL). As illustrated in Fig. 5, if the node senses activity, it wakes up, synchronizes with the packet preamble, and receives the packet. A sender must transmit a preamble length greater than the sleeping nodes sampling cycle to ensure that the node is awake for synchronization. Since many of the sensor platform transceivers expend more energy receiving than transmitting, experiments have shown that the penalty for idle listening in the entire network far exceeds the penalty for transmitting a longer preamble if the system is tuned correctly.

Since an attacker can extend a broadcast message preamble across an entire sleep period and wake up every

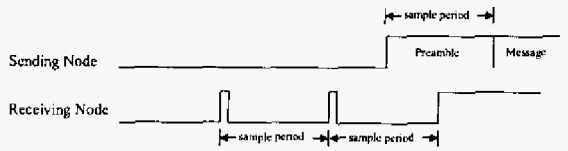

Fig. 5. BMAC low power listening [19]

node, B-MAC is equally as susceptible to a denial of sleep attack as T-MAC.

VI. Proposed Gateway MAC (G-MAC)

Gateway MAC (G-MAC) is a proposed energy-efficient sensor MAC protocol designed to coordinate transmissions within a cluster. Like the WSN MAC protocols previously discussed, all nodes have equally limited resources and have traffic intended to pass to neighboring nodes for in-network processing and out of the network to designated applications (network sink) for further processing. G-MAC has several energy-saving features which not only show promise in extending the network lifetime, but the centralized architecture makes the network more resistant to denial of sleep attacks.

G-MAC divides a frame into a collection period and a distribution period as shown in Fig. 6. During the collection period, the cluster coordinator, called the gateway sensor (GS) node, collects two types of network traffic: intra-network (local) and inter-network (non-local) traffic. Intra-network traffic represents messages exchanged among nodes in the same cluster. The sender transmits a future-RTS (FRTS) message to reserve a delivery slot in the non-contention distribution period. Inter-network traffic represents messages which originate in the cluster and will be forwarded by the gateway to the outside network. The sender and gateway exchange an RTS-CTS-data-ACK message sequence for immediate collection. After all transactions are complete, the gateway attempts to forward all traffic out of the cluster, gathers any incoming data for the cluster, and then transitions to sleep (I&S inter-network and sleep period in

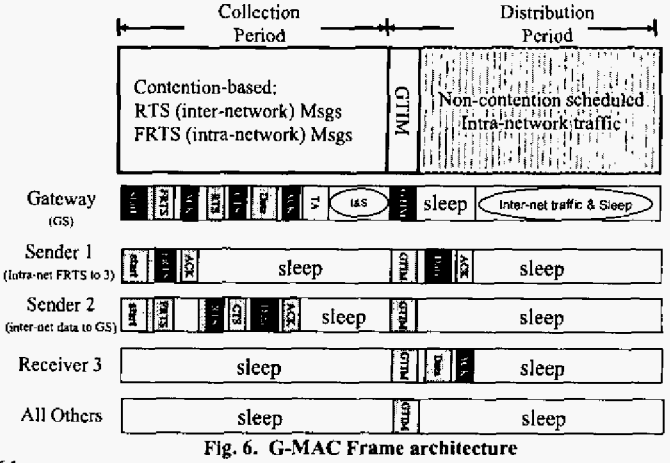

Fig. 6. G-MAC Frame architecture

Fig. 6). The distribution period begins with all nodes waking up and receiving the gateway's traffic indication message (GTIM). In this message, the gateway declares the next collection period, the next distribution period, and the schedule of message transactions between cluster nodes. The GTIM describes the traffic exchange time slots by source, destination, and time offset. Based upon the GTIM synchronization time, the offset field indicates the time duration before a node must wake up for its message transaction. The receiving node returns the next offset value in the ACK response to synchronize the next transmission.

G-MAC periodically elects a new gateway node to equally distribute the energy requirements among all of the sensors. Although the network has a default changeover frequency for self-recovery, every GTIM contains an election bit that is set to indicate whether the next distribution period will changeover the gateway. To reduce the overhead of exchanging available resource updates, G-MAC uses a passive method of determining the next gateway by calculating an election contention backoff period based upon a node's available resources. Nodes with fewer resources will have larger backoff times based upon a multi-tiered critical resource algorithm. The group of nodes with the most available resources will produce the next gateway. The new gateway is the *volunteer* node which first gains contention of the medium after the start of the GTIM period. A gateway will signal for a new election whenever it transitions to a lower energy state, reaches critical memory levels, or approaches a default changeover.

Since cluster nodes only respond to the gateway node, network attackers cannot penetrate the link layer of the G-MAC protocol. Unicast or broadcast messages sent to the gateway must be authenticated prior to being distributed to the individual nodes. The best success that a broadcast attacker can achieve is to send broadcast messages to the gateway and force the gateway to receive the entire message before discarding it due to authentication failure. Once the gateway's energy level reduces to a lower level, a fresh gateway takes its place. Shown in Eqn. 4, the attacker must effectively erode the network's energy one node at a time.

$$T_{networklifetime} = T_{sensorlifetime} = \frac{n_{nodes} * C_{battery(mAhr)}}{(D)(I_{active(mA)}) + (1-D)(I_{sleep(mA)})} \quad (4)$$

VII. Analysis Of Protocols

Modeling each network with no traffic, regular unicast traffic, regular broadcast, and broadcast attack traffic conditions yields the results shown in Table 2.

Each WSN protocol is modeled in MATLAB using similar configurations to provide a fair comparison. The IEEE 802.11 standard MAC protocol [24] establishes a baseline for a network lifetime without any power-saving mechanisms. The S-MAC model has a 500ms frame time with a fixed sleep period of 450ms, translating to a 10% duty cycle. The S-MAC implementation includes RTS-

Table 2. MAC Protocol Performance Results

MAC Protocol	Network Lifetime (days)			
	Empty Network (no traffic)	Regular Unicast Traffic	Regular Broadcast Traffic	Denial of Sleep Broadcast Attack
802.11	6	6	6	6
S-MAC	63	88	63	63
B-MAC	244	87	87	87
T-MAC	295	130	108	108
G-MAC	480	455	203	478

CTS exchanges for message overhearing avoidance. The T-MAC model also has a frame time of 500ms with the adaptive sleep timeout set to 10.2ms and a fixed contention period of 5ms for every packet. The B-MAC model senses the channel for 0.35ms during every 14ms check interval. In fairness, the low power listening mechanism for B-MAC consumes the same power as the receive mode in all other models. The G-MAC protocol also uses a 500ms frame time containing a collection period, a GTIM broadcast, and a distribution period. The size of the GTIM is 35 bytes + (6 bytes * number of packets/frame). The system models forty nodes in a single-hop neighborhood and operates at 62.6kbps. The network lifetime is based solely on the CC2420 radio energy to receive (19.7mA), transmit (17.4mA), and power down sleep (0.02mA).

The results indicate that G-MAC performs significantly better than the other protocols in every traffic situation. The empty network case shows the protocol overhead and idle listening effects determined by the effective duty cycle. IEEE 802.11 performs poorly with a 100% duty cycle. B-MAC establishes a 2.5% effective duty cycle, and S-MAC uses a 10% fixed duty cycle. With adaptive listening, all T-MAC nodes must monitor the network for a complete timeout period of 10.2ms at the beginning of every 500ms slot for a 2.1% duty cycle. G-MAC's equivalent 0.95% duty cycle is the weighted average of the duty cycle of the gateway node and the other nodes. The gateway node monitors the network for a complete timeout and sends the empty GTIM. All other nodes wake up only to receive the GTIM and return to sleep.

Regular unicast and broadcast traffic is modeled as four 32-byte messages per second. By only having the transmitting nodes awake during the contention period, G-MAC outperforms all of the other protocols in terms of network lifetime. T-MAC performs better than S-MAC due to its ability to curtail the active period after

completing all transmissions. Interestingly, S-MAC uses less network energy with traffic than in the empty traffic scenario. The ability for the passive nodes to transition to sleep after receiving the RTS or CTS messages allows them to save message overhearing energy costs. The performance of B-MAC significantly decreases because each passive node has to wake up and receive every message. Additional tests show that B-MAC works well in ultra-low traffic networks.

Any shared medium can be attacked with physical layer jamming. A denial of sleep attack is most effective if the attacking node uses knowledge of the MAC protocol to drain network energy without expending much of its own. For fairness, the model makes the unbiased assumption that each protocol can authenticate a message after it is completely received. The denial of sleep broadcast attack is modeled as an attacker sending four 32-byte broadcast messages per second. All nodes in S-MAC, T-MAC, and B-MAC protocols simultaneously receive a broadcast message, but discard the message if it fails authentication. The attacking node is able to deny sleep to all of the network nodes at the same time. S-MAC performs better than T-MAC since it automatically transitions to sleep after receiving the last packet initiated prior to the sleep period. T-MAC nodes must wait the additional adaptive timeout period. With G-MAC, the attacker must gain access to the network through the gateway node which relays all inter-network traffic and reserves timing slots for intra-network traffic. If the gateway does not properly authenticate the packet, it will not forward it to the other network nodes. The broadcast message does not directly affect the sleeping nodes. Furthermore, if the attacker cannot properly encrypt a GTIM message, the other nodes will not accept an attacker's traffic schedule if it tries to masquerade as the gateway node. Therefore, a link layer denial of sleep attacker can only affect one node at a time, because nodes alternate the gateway responsibilities based upon incremental decreases in battery levels. Since n-1 nodes will always be sleeping during the broadcast, the network lifetime for an attack increases linearly with the number of nodes. For these reasons, G-MAC significantly outperforms the other MAC protocols in the broadcast denial of sleep attack category.

VIII. Future Work and Conclusions

This paper describes the denial of sleep vulnerabilities for leading wireless sensor network MAC protocols and models the catastrophic effects these attacks can have on a deployed network. The link layer denial of sleep attack exposes the necessity to consider all primary threats to every system component during the design phase to properly integrate security with functionality. The WSN link layer MAC protocol introduced in this paper, Gateway MAC, established an effective denial of sleep defense by centralizing cluster management. Future work in WSN protocol research includes analyzing other security vulnerabilities such as physical layer jamming, node/key capture containment, and network layer misrouting. Providing solutions for these resource-constrained networks requires delicate tradeoffs in security, performance, and usability.

IX. References

[1] J. Kahn, R. Katz, and K. Pister, "Next century challenges: mobile networking for 'Smart Dust'," In *ACM MobiCom*, Aug. 1999.

[2] CrossBow Corporation, MICA2 and MICAZ Series Data Sheet [Online], http://www.xbow.com.

[3] MoteIV Corporation, TelosA Data Sheet [Online], http://www.moteiv.com/products-reva.php.

[4] Chipcon Corporation, CC1000 and CC2420 Data Sheet [Online], http://www.chipcon.com/.

[5] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," In *ACM Comm.*, 2004.

[6] A. Wood and J. Stankovic, "Denial of service in sensor networks, "In *IEEE Computer*, Oct. 2002.

[7] Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," In *ICISC*, Springer-Verlag, 2000.

[8] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," *In PERCOM*, Mar. 2004.

[9] G. Jacoby and N. Davis, "Battery-based intrusion detection," *IEEE Globecom*, Dec. 2004.

[10] J. Cannady and J. Harrell, "A comparative analysis of current intrusion detection technologies," In *TISC*, 1996.

[11] Y. Law, et al. "Link-layer Jamming Attacks on S-MAC," Technical Paper, Univ. of Twente, NL, 2005.

[12] E. Shi and A. Perrig, "Designing secure sensor networks," In *IEEE Wireless Comm*, Dec. 2004.

[13] R. Negi and A. Perrig, "Jamming analysis of MAC protocols," Carnegie Mellon Technical Memo, 2003.

[14] M. Stahlberg, "Radio Jamming attacks against two popular mobile networks," In *Helsinki University of Tech. Seminar on Network Security*, Fall 2000.

[15] C. Karloff an, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks, In *ACM Sensys*, Nov. 2004.

[16] National Inst.of Std. and Tech., "Federal Information Processing Standards Publication 197: Advanced Encryption System Standard (AES)," Nov. 2001.

[17] Wireless MAN medium access control and physical layer specification for low-rate WPANs, IEEE Std. 802.15.4 – 2003 edition.

[18] A. Perrig, et al. "SPINS: Security Protocols for Sensor Networks," In *Wireless Networks*, 2002.

[19] K. Langendoen and G. Halkes, "Energy Efficient Medium Access Control," unpublished, 2004.

[20] V. Bharghavan, et al., "MACAW: a media access protocol for wireless LANs," In ACM *SIGCOMM*, Aug. 1994.

[21] Y. Wei, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *INFOCOMM*, Jun. 2002.

[22] T. van Dam and K. Langendoan, "Energy-efficient MAC: An adaptive energy-efficient MAC protocol for wireless sensor networks," in *ACM SENSYS,* Nov. 2003.

[23] J. Polstre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in *ACM SENSYS* 2004.

[24] Wireless LAN medium access control and physical layer specification, IEEE Std. 802.11-1997 edition.

0-7803-9290-6/05/$20.00 ©2005 IEEE.