Towards a New Paradigm for Securing Wireless Sensor Networks

K. Jones, A.Wadaa, S. Olariu, L. Wilson
Department of Computer Science
Old Dominion University
Norfolk, VA, 23529-0162
olariu@cs.odu.edu

M. Eltoweissy
Department of Computer Science
James Madison University
Harrisonburg, VA 22807
eltowemy@jmu.edu

ABSTRACT
The network model assumed in this paper consists of tiny, energy-constrained, commodity sensors massively deployed alongside with one or more sink nodes that provide the interface to the outside world. The sensors in the network are initially anonymous and unaware of their location. Our main contribution is to propose a new robust and energy-efficient solution for secure operation of wireless sensor networks. The paper motivates a new paradigm where security is based upon using parameterized frequency hopping and cryptographic keys in a unified framework to provide differential security services for wireless sensor networks.

Keywords
Wireless sensor networks, energy-efficient protocols, security, frequency hopping.

1. INTRODUCTION
Recent advances in nano-technology make it technologically feasible and economically viable to develop low-power, battery-operated devices that integrate general-purpose computing with multiple sensing and wireless communications capabilities. It is expected that these small devices, referred to as sensor nodes, will be mass-produced making production costs negligible. Individual sensor nodes have a non-renewable power supply and, once deployed, must work unattended. For most applications, we envision a massive random deployment of sensor nodes, numbering in the thousands or tens of thousands. Aggregating sensor nodes into sophisticated computation and communication infrastructures, called sensor networks, will have a significant impact on a wide array of applications including military, scientific, industrial, health, and domestic. The fundamental goal of a wireless sensor network is to produce, over an extended period of time, global information from local data obtained by individual sensor nodes [1,2,4,6,15].

The vast majority of military, medical, scientific and industrial applications require that sensor networks offer a high degree of security. If an adversary can thwart the work of the network by perturbing the information produced, stopping production, or pilfering information, then the perceived usefulness of sensor networks will be drastically curtailed. Thus, security is a major issue that must be resolved in order for the potential of wireless sensor networks to be fully exploited. The task of securing wireless sensor networks is complicated by the fact that the sensors are mass-produced anonymous devices with a severely limited energy budget and initially unaware of their location.

Recently, the problem of securing ad-hoc networks has received a great deal of well-deserved attention in the literature [2,5,7,9,17,18]. Unfortunately, wireless sensor networks are sufficiently different in their characteristics from ad-hoc networks that security solutions designed specifically for the former do not apply to the latter. Quite recently, a number of solutions for securing wireless sensor networks have been proposed [11,13,16]. Somewhat surprisingly, none of these solutions addresses the problem of jamming. Furthermore, all assume sensors with unique identities. In Section 3, we examine some of these solutions in more detail.

The main contribution of this work is a novel solution to the problem of securing wireless sensor networks. Specifically, we show that by a suitable enhancement, the classic frequency hopping strategy [3,19] can provide a lightweight and robust mechanism for securing wireless sensor networks. A significant advantage of our solution is that it is readily applicable to networks having anonymous nodes that are unaware of location. It is worth noting that our solution supports a differential security service that can be dynamically configured to accommodate changing application and network state. We view our work as an initial contribution towards developing a paradigm for securing sensor networks based on a holistic approach to securing multiple layers in the protocol stack. An important aspect of this paradigm, as envisioned, is the exploitation of the interplay between security measures in different layers to provide a security service for the whole network.

The remainder of this paper is organized as follows. Section 2 introduces the wireless sensor network model assumed in the paper, along with basic protocol for organizing the network into clusters. Section 3 provides the parameters of the security service that we propose as well as the motivation, background and state of the art in securing wireless sensor networks. Section 4 presents the details of our proposed security solution. Section 5 evaluates our solution in terms of well-known security goals. Finally, Section 6 offers concluding remarks and maps out directions for future work

2. THE SENSOR NETWORK MODEL
We consider a class of wireless sensor networks consisting of a sink node and a large number of sensor nodes randomly deployed within the transmission range of the sink. We

New Security Paradigms Workshop 2003 Ascona Switzerland

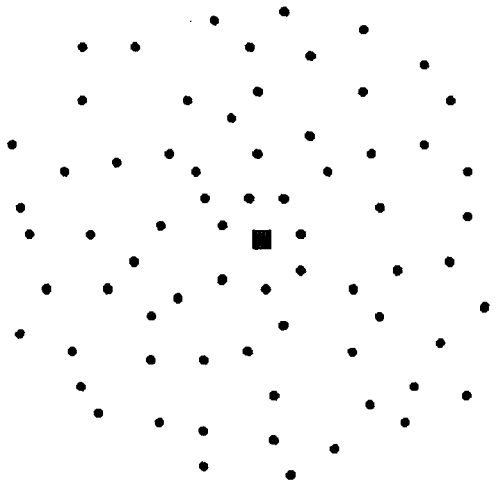
assume that individual sensor nodes operate subject to three fundamental constraints. First, each sensor has a non-renewable power budget. Second, each sensor is in sleep mode most of the time, waking up at random points in time for short intervals under the control of an internal timer. Third, each sensor has a modest transmission range, perhaps a few meters with the ability to send and receive a wide range of frequencies. The range constraint implies that outbound messages sent by a sensor can reach only the sensors in its proximity, typically a small fraction of the sensors in the entire network. As a consequence, the sensor network must be multi-hop and only a limited number of the sensor nodes count the sink among their one-hop neighbors. For reasons of scalability, it is assumed that no sensor node knows the topology of the network.

2.1 The sensor and sink models

We assume a sensor to be a device that possesses three basic capabilities: sensing, computing, and communicating. We assume that a sleeping sensor consumes essentially no energy. We assume that the sensor network is connected to the outside world through a sink node having a full range of computational and communication capabilities and a renewable power supply. Note that the sink could be mobile or even a committee.

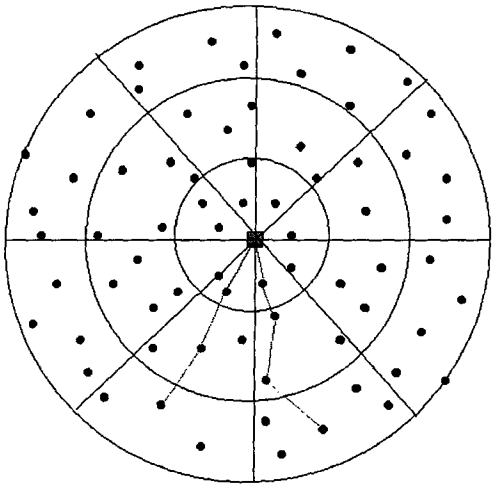
2.2 Training the sensor network

Briefly stated, the goal of training is to provide location awareness, to establish clusters and to organize the infrastructure needed by node-to-sink multi-hop communications. Figure 1(a) features an un-trained sensor network with the sink shown at the center for simplicity. Training imposes a coordinate system onto the sensor network in such a way that each sensor belongs to exactly one sector. Further each sensor will be aware of its sector. Referring to 1(b), the coordinate system divides the sensor network area into equiangular wedges. In turn, these wedges are divided



(a)

into sectors by means of concentric circles or coronas centered at the sink and whose radii are determined to optimize the transmission efficiency of sensors-to-sink transmission. [14]. Note that post training one may consider the sectors as clusters and may also easily define multi-hop paths connecting the nodes in each wedge to the sink. For details of our training protocol, the establishment of node-to-sink paths we refer the interested reader to [14].



(b)

Figure 1: (a) An untrained sensor network with a central sink node (b) A trained sensor network with some multi-hop paths illustrated.

3. Motivation and background

In this section we define the parameters of the security service supported by our proposed solution to securing wireless sensor networks. We begin our discussion of these parameters by briefly reviewing some fundamentals of network security. We then go on to describe the principles underlying our application of these fundamentals.

3.1 Network security fundamentals

Encryption, steganography and securing access to the physical layer are well known techniques for securing computer networks.

Encryption: In sensor networks, power is extremely constrained and transmission is the major consumer of power. Therefore, increasing the ratio of the total number of bits transmitted to the effective data bits (often a result of encryption), increases the total number of bits transmitted and, thus, the power consumed. Key management is also a problem for use of encryption in sensor networks. How are keys generated and disseminated? How can keys be changed in a reasonable time? Humans are not available at each sensor, distribution and modification of keys are difficult, and the sensor (and thus, embedded keys) is physically at risk. Perrig *et al.* [11] describes techniques for reducing the resource requirements. While their reduction techniques are creative and substantial, they still consume nearly 50% of sensor mote memory, computation, and transmission resources for security.

Steganography: Recent works in steganography [8,10] describe ways to embed messages into digital images that can be publicly distributed while allowing secure extraction of the embedded messages. Unlike cryptography, which hides the content of a message, steganography hides the existence of the message. This is accomplished by replacing the least significant bit(s) of bytes representing a digital image by bits

forming the hidden message. This does not apply directly to securing wireless sensor networks as we do not anticipate having publicly distributed images suitable for carrying embedded messages. However, we do hope to hide our messages in the frequency domain such that eavesdroppers will not know that a communication has occurred as will be described in section 4.

Securing access to the physical layer: Frequency hopping can provide this service to sensor networks. Given that techniques are known to discover a hopping sequence by monitoring transmissions, security can only be provided if the design modifies the hopping sequence in less time than is required to discover the sequence. Parameters in the specification of frequency hopping determine the time required to discover the sequence:

- **Hopping Set**; The set of frequencies available for hopping,
- **Dwell Time**; The time interval per hop, and
- **Hopping Pattern**; The sequence in which frequencies in the hopping set are traversed.

A dynamic combination of these parameters can improve security at little expense of memory, computation and power. As frequency hopping requires events to happen simultaneously for both senders and receivers, all must maintain a synchronized clock.

3.2 Guiding principles of holistic security in wireless sensor networks

We view this paper, in part, as an initial contribution towards developing a paradigm for securing sensor networks based on a holistic approach to securing multiple layers in the protocol stack. An important aspect of this paradigm, as envisioned, is the exploitation of the interplay among security measures in different layers to provide a security service for the whole network.

We now propose a set of principles for addressing the problem of securing wireless sensor networks. A solution in the context of these principles supports a *differential security service* that can be dynamically configured to cope with changing network state, for example, a detected state change in security risks or energy content in the network. Reconfiguration of dynamic security service can potentially minimize the energy cost of security over the network lifetime.

The four guiding principles for securing wireless sensor networks are:

i. Security of a network is determined by the security over all layers. For example, provisioning confidentiality, two-party authentication, and data freshness typically addresses security of the link layer. Referring to Figure 2, we note that securing the link layer confers the layers above some security; however, it does not address security problems in the physical layer below, most notably jamming. In general, an insecure physical layer may practically render the entire network insecure, even if the layers above are secure. This is especially true in the sensor network environment since basic wireless communication is inherently not secure.

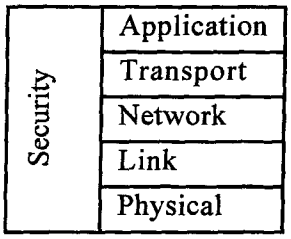


Figure 2: A holistic view of security

ii. **In a massively distributed network, security measures should be amenable to dynamic reconfiguration and decentralized management.** Given the nature of sensor networks, a security solution must work without prior knowledge of the network configuration after deployment. Also, the security solution should work with minimal or no involvement of a central node to communicate globally (or regionally) shared information.

iii. In a given network, at any given time, the cost incurred due to the security measures should not exceed the cost assessed due to the security risks at that time. The sensor network is expected to experience different magnitudes of risk at different times, especially considering the, typically, long lived nature of a network. In principle, security services should adapt to changes in assessed security risk. This entails that a cost model for both security provisioning and risk be an integral part of the security model.

iv. **If physical security of nodes in a network is not guaranteed, the security measures must be resilient to physical tampering with nodes in the field of operation.** For example, a sensor network deployed in a battlefield should exhibit graceful degradation if some network nodes are captured.

3.3 Related work

Recently, the problem of securing ad-hoc networks has received a great deal of well-deserved attention in the literature [5,7,9,17,18]. However, since wireless sensor networks are different in their characteristics from ad-hoc networks security solutions designed specifically for the former do not apply to the latter. Quite recently, a number of solutions for securing wireless sensor networks have been proposed in the literature [11,13,16]. We now examine some of these solutions from the viewpoint of the guiding principles proposed above.

Perrig *et al.* proposed *SPINS* [11], a general security infrastructure for sensor networks. The infrastructure consists of an encryption primitive, *SNEP*, and an authenticated streaming broadcast primitive, *micro TESLA*. These primitives constitute building blocks that can be used to construct higher-level security services. SPINS, however, does not address security in the physical layer, and thus departs from the holistic security approach implied by the first principle. In addition, SPINS supports a *binary* security model, either *no security* or *maximum security*.

Besides, the key management model in SPINS does not scale in a massively deployed network, since it prescribes a unique key per node (called master key) to be loaded into the node prior to deployment.

TinySec [13] proposes a link layer security mechanism for sensor networks, based on an efficient symmetric key encryption protocol. Similar to SPINS, TinySec does not

address security in the physical layer, and is based on a binary security model. TinySec presents an assessment of the tradeoffs between security on one hand, and energy consumption and RAM utilization on the other hand. However, this cost model is not integrated into their security model, and is not a factor in configuring the security service supported. In fact, the security service supported by TinySec is not dynamically reconfigurable. Another limitation of TinySec is that it is tightly coupled with the Berkeley TinyOS radio stack [15], and is, therefore, not applicable to a general sensor network model

4. OUR SECURITY SOLUTION

We propose a solution for securing wireless sensor networks that fundamentally adheres to a large extent to the guiding principles described earlier. The proposed solution uses parameterized frequency hopping and cryptographic keys in a unified framework to provide differential security services for the network. Using frequency hopping in radio communications is not a new idea and was explored before [3,19]. Conventional frequency hopping mechanisms have been used as means of implementing frequency diversity and interference averaging in a non-hostile context; by design, these mechanisms offer no cryptographic value. In contrast, our use of frequency hopping is novel in that it does.

The proposed solution constitutes, in effect, a reconfigurable network security service A multitude of parameters, as explained in detail later, define a *configuration space* for the security service. In general, different configurations of the security service are characterized by the energy cost assessed, and the amount of security afforded. Reconfiguration of the security service is dynamic.

4.1 The basic problems

In the context of our proposed solution, secure communications between a given sender and receiver, can be defined in terms of three basic problems, as follows.

I. *How do a sender and receiver without unique node identifiers establish a trusted path (i.e. acquire a shared path secret)?*

In our solution communication uses a frequency hopping mechanism, as we explain shortly. The *cryptographic measure* we employ is a *randomization process* defined on the frequency hopping mechanism and driven by a secret shared by the path from sender to receiver. Within our paradigm, we propose a solution to the trust establishment problem that scales in the number of nodes, and addresses security of an entire *path*, as opposed to *hop or link* security.

II. *How do a sender and receiver synchronize?*

For communication to occur, both the sender and receiver must be in sync. We propose a lightweight synchronization solution that enables a sender and a receiver sharing a common secret to synchronize.

III. *How do a synchronized sender and receiver communicate securely?* We propose an integrated cryptographic key and parameterized frequency-hopping security solution.

In Subsection 4.2 we exploit frequency hopping to provide significant security for wireless sensor networks. In Subsection 4.3 we extend our solution to further enhance this security for wireless sensor network that has been trained as described in Section 2.

4.2 Frequency hopping in a wireless sensor network

How do a synchronized sender and receiver communicate?

(Precondition: Sender, s, and receiver, r are mutually trusting, and are in sync)

Our solution for this problem works as follows. We assume that time is ruled into epochs. For a given sender, s, and receiver, r, at time epoch, t, s transmits (and r receives) following a hopping pattern across a set of frequencies, called the hopping set for t. We assume that, for each epoch, the hopping set is drawn from a designated frequency space (band) that provides the set of all possible frequencies that can be used, e.g. ISM band.

The key idea is that the shared secret between *s*, and *r*, is used to drive a randomization of the frequency-hopping process. Specifically, the shared secret enables the *epoch length*, the hopping pattern, and the size and membership of the hopping set for each epoch to be changed according to random number sequences. Let both *s*, and *r* be in sync at epoch t_i. Seeded by the shared secret, a random number generation scheme is used, in both *s* and *r* to generate the successive epoch lengths, hopping sets, and hopping patterns, for the epochs $t_i, t_{i+1}, t_{i+2}, \ldots$. To an observer, however, successive epoch lengths, hopping sets, and hopping patterns appear as the product of an unknown random process. It should be noted that our solution makes it feasible to graft an encryption scheme on top of the frequency-hoping scheme described above. During each hop in each epoch, the messages may be transmitted in either encryption or a no encryption mode.

In our solution, the cost incurred by the network is a function of the configuration of the security service. Each of the epoch length, frequency set, frequency pattern, and encryption mode during a hop can be dynamically configured. This gives rise to a differential security service that potentially incurs differential cost. On one hand, a constant epoch length, hopping pattern, hopping set, and a non encrypted transmission during a hop correspond to minimal security and minimal cost incurred. On the other hand, a randomized epoch length, hopping pattern, and hopping set, in addition to encrypted transmission during a hop corresponds to maximum security and possibly maximum cost incurred. A multitude of configurations can be defined between these two extremes, each having an associated cost incurred.

Synchronization is an important concern in any frequency-hopping scheme. In our solution we propose a lightweight synchronization scheme, to enable arbitrary pairs of sender and receiver nodes that can exchange messages directly to synchronize. This scheme is detailed next.

How do a sender and receiver synchronize?

The main goal of this subsection is to spell out the details of a lightweight synchronization protocol that underlies our new security paradigm for wireless sensor networks. Our protocol achieves synchronization with high probability. The natural way for nodes to synchronize is by following the master clock running at the sink node. Thus, the sink node here is the sender, and the node that wants to synchronize is the receiver.

We assume that the sink dwells τ micro-seconds on each frequency in the hopping sequence. It is clear that determining the epoch and the position of the sink in the hopping

sequence corresponding to the epoch is sufficient for synchronization.

For the purpose of showing how synchronization is effected, assume that time is ruled into epochs $t_1, t_2, \ldots, t_n$. For every $i, (1 \le i \le n)$, we let l_i stand for $\left\lceil \frac{t_i}{\tau} \right\rceil$; thus, epoch t_i involves a hopping sequence of length l_i. Further, with epoch t_i $(1 \le i \le n)$, we associate a set of n_i frequencies and a corresponding hopping sequence $\lambda_1, \lambda_2, \ldots, \lambda_{l_i}$. We can think of the epoch t_i $(1 \le i \le n)$, as being partitioned into l_i slots $s_1, s_2, \ldots, s_{l_i}$ such that in slot $j, (1 \le j \le l_i)$, the sink is visiting frequency λ_j.

We assume that, just prior to deployment, the sensor nodes are synchronized. However, due to natural clock drift re-synchronization is necessary. Our synchronization protocol is predicated on the assumption that clock drift is bounded, as we are about to explain. Specifically, assume that whenever a sensor node wakes up during its *local* time epoch t_i the master clock is in one of the time epochs t_{i-1}, t_i, or t_{i+1}. The sensor node knows the *last* frequencies $\lambda_{l_{i-1}}, \lambda_{l_i}, \lambda_{l_{i+1}}$ on which the sink will dwell in the time epochs t_{i-1}, t_i, and t_{i+1}. Its strategy, therefore, is to tune in, cyclically, to these frequencies, spending $\frac{\tau}{3}$ time units on each of them. It is clear that, eventually, the sensor node meets the sink node on one of theses frequencies. Assume, without loss of generality, that the node meets the sink on frequency λ_{i+1} in some (unknown) slot s of one of the epochs t_{i-1}, t_i, or t_{i+1}. To verify the synchronization, the node will attempt to meet the sink in slots $s+1$, $s+2$ and $s+3$ according to its own frequency hopping for epoch t_{i+1}. If a match is found, the node declares itself synchronized. Otherwise, the node will return to scanning frequencies $\lambda_{l_{i-1}}, \lambda_{l_i}, \lambda_{l_{i+1}}$ as discussed above.

We note that even if the sensor node declares itself synchronized with the sink, there is a slight chance that, in fact, it is not. The fact that the node has not synchronized will be discovered fast and the node will attempt to synchronize again. There are ways in which we can make the above synchronization protocol deterministic. For example, the hopping sequence can be designed in such a way that the last frequency in each epoch is unique and it is not used elsewhere in the epoch. However, this entails less flexibility in the design of the hopping sequence and constitutes, in fact, an instance of a differential security service where the level of security is tailored to suit the application or the power budget available.

1.3 Trusted paths in a trained sensor network

How do a sender and receiver establish a trusted path (i.e. acquire a shared path secret)?

(Precondition: at pre-deployment the entire network shares a secret for an initial post-deployment frequency-hopping phase, (this is a condition for the proper operation of the network even if secret paths are not used.) A network without node identifiers receives training, for example as described in Section 2. On the average, nodes are distributed equally among wedges.)

We present a solution based on symmetric keys to establish secure paths between a sender and a receiver as follows. Pre-deployment, sensors are loaded with a set of m keys that are selected at random from a set of k keys. The number of keys |k| is chosen such that two random subsets of size |m| overlap in at least one key with probability p. Post-deployment, a link may be established between neighboring sensors on the path to the sink if a key of their selected sets of m keys overlap. It is to be noted that the number of overlapping keys may be a parameter in the security solution. On the one hand, increasing the number of overlapping keys needed to establish a link will reduce the number of paths between nodes, which will make it more difficult to eavesdrop, on the other hand, it may limit the existence of paths that may otherwise be selected due to other criteria, for example, energy budget. Path determination is outlined next.

1. Using the shared frequency-hopping secret, FHS, the sink endows each wedge, Wi, with a unique wedge key, WKi, and (possibly) a new wedge FHS, WFHSi, for 1<= i <= NW, where NW is the number of wedges. This in effect creates a firewall at wedge boundaries. This process can initially take place during the training phase. Note that the time to start using the new WFHSi should also be broadcast to the wedge.

2. Using encryption with WKi or a hopping set with seed WFHSi or both, depending on the level of security required, a source sensor broadcasts indexes (or puzzles) to its set of m keys. If an overlap is detected with a neighbor, a link may be established.

3. All neighbors in the direction of the sink with established links (i.e., with overlapping keys), in turn, broadcast indexes (or puzzles) to their sets of m keys. Again a link may be established between neighbors with overlapping sets in the direction of the sink.

4. The process continues all the way to the sink.

5. The source node generates a path key, PKj, and sends it along each of the established j paths within the same wedge. If either the frequency hopping set based on FHSi is used or PKj is encrypted with WKi, then only nodes on the established paths that are within the same wedge will know the path key.

6. The path key is used to send: (1) new path FHS, PFHSj, that are generated by either the source (or the sink) for each path j and, (2) the time to start running the FH algorithm with the new seed PFHSj.

Remarks:

- After the initial frequency-hopping phase, the secure operation of the network will not depend on the entire network sharing a common secret.
- To limit the probability of compromising the wedge key and the wedge frequency-hopping secret, the sink can randomly update their values one at a time. Also, once a path key is established, nodes can purge their stored wedge key and wedge frequency-hopping secret.
- If a node is compromised, its impact will be limited to the paths that it can participate in. If anomalous behavior along

a path is detected, either the source or the sink may purge that path.

- Our solution allows for graceful degradation; it is possible to start by purging paths within a wedge, then purging wedges and so on.

5. EVALUATION OF OUR PROPOSED SOLUTION

It is widely recognized that the task of securing a network involves achieving the following important goals [18].

- Availability: ensures the survivability of network services despite denial-of-service attacks.
- Confidentiality: ensures that certain information is not disclosed to unauthorized entities.
- Integrity: guarantees that a message being transferred is never corrupted by an attack.
- Authentication: enables a node to ensure the identity of the peer node with which it communicates.
- Non-repudiation: ensures that the origin of a message cannot deny having sent the message.

The main goal of this section is to evaluate our proposed solution to securing wireless sensor networks in terms of achieving the goals we just listed. As already mentioned, just prior to deployment, the individual sensor nodes are synchronized and are injected with genetic material consisting, essentially, of a program capable of generating the random sequences defined in this paper. Individual sensor nodes are assumed to be tamper-resistant and are programmed to self-destruct (perhaps by erasing their ROM) if physical tampering is attempted. It is encouraging that present-day technology affords various solutions to designing tamper-resistant nodes [5,12].

AVAILABILITY: we note that in our solution the adversary cannot infiltrate the system other than by physically tampering with the individual sensor nodes. In particular, the only denial of service (DoS) attack on the system is by jamming, contrary to what can happen in other security schemes as discussed in [11,13]. Thus, in our solution, preventing DoS attacks is tantamount to preventing jamming. In turn, jamming is made extremely expensive by our frequency-hopping scheme.

CONFIDENTIALITY and INTEGRITY: Our solution provides both confidentiality and message integrity since the adversary does not have the time to learn our hopping sequence in any given epoch. Indeed our assumption that individual sensor nodes are tamper-proof, combined with the process of securely migrating between various sets of frequencies and between various frequency hopping sequences from one time epoch to the next, makes the task of breaking into the system extremely difficult.

AUTHENTICATION and NON-REPUDIATION: Due to the fact that sensor nodes are anonymous, the classic definition of authentication and non-repudiation do not apply to wireless sensor networks presented in this paper. These two goals are extremely important and there is on-going work trying to address these issues.

6. CONCLUSION AND DIRECTIONS FOR FUTURE WORK

It is anticipated that in the near future wireless sensor networks will be employed in a wide variety of applications ranging from military, to industrial, to social, to domestic, establishing ubiquitous networks that will pervade society, redefining the way in which we live and work. It is widely recognized that sensor network research is in its infancy [1,2,4-6,11,13-16]. In particular, there is precious little known about how to get sensor networks to self-organize in a way that maximizes the operational longevity of the network and that guarantees a high level of availability in the face of potential security attacks. Unfortunately, the characteristics of sensor networks are such that security protocols developed for wired, cellular, or ad-hoc networks do not apply here [2,11,16].

We proposed a new solution to the problem of securing wireless sensor networks. Specifically, we showed that by a suitable enhancement the classic frequency hopping strategy can provide a light-weight and robust mechanism for securing wireless sensor networks. Our solution supports a differential security service that can be dynamically configured to accommodate changing application and network system state.

A large number of security-related problems are still open. One of the key open problems is authentication. Clearly, the classic definition of authentication does not apply to an environment populated by anonymous sensor nodes. We are contemplating the concept of result-based authentication as well as that of collective authentication, whereby a group of sensors is uniquely authenticated by combining individual keys. Yet another unsolved problem has to do with non-repudiation. Just like authentication, the non-repudiation goal is complicated by node anonymity. One partial solution is to endow the sensor nodes with temporary IDs.

7. ACKNOWLEDGMENTS

The authors wish to thank the workshop participants for their helpful comments. This work was supported in part by a grant from the Commonwealth Technology Research Fund (SE 2001-01) through the Commonwealth Information Security Center.

8. REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, Wireless sensor networks: A survey, *Computer Networks*, Elsevier Science, vol. 38, no. 4, 2002, 393-422.

[2] P. Bahl, W. Russell, Y.-M. Wang, A. Balachandran, G. M. Voelker, and A. Miu, PAWNs: satisfying the need for ubiquitous secure connectivity and location services, *IEEE Wireless Communications*, vol 9, no. 1, February 2002, 40-48.

[3] A. Ephremides, J. Wieselthier and D. Baker, A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling, *Proceedings of the IEEE*, 1987.

[4] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, System architecture directions for networked sensors, *Proceedings of the ninth international conference on Architectural support for programming languages and operating systems*, Cambridge, Massachusetts, November 2000.

[5] J.-P. Hubaux, L. Buttyan, and S. Capkun, The quest for security in mobile ad-hoc networks, *Proc. MOBIHOC*, Long Beach, CA, 2001.

[6] J. M. Kahn, R. H. Katz and K. S. J. Pister, Mobile networking for Smart Dust, *Proc. MOBICOM'99*, Seattle, WA, August 17-19, 1999.

[7] J. Kong et al., Providing robust and ubiquitous security support for mobile ad-hoc networks, *Proc. 9th International Conference on Network Protocols, IEEE* CS Press, Los Alamitos, California, 2001, 251-260.

[8] C. Kurak and J. McHugh, A Cautionary Note on Image Downgrading in Computer Security Applications, San Antonio, pp. 153-159, Dec. 1992.

[9] S. Marti et al., Mitigating routing misbehavior in mobile ad-hoc networks, *Proc. MOBICOM'2000*, Boston, August 6-11, 2000.

[10] I. S. Mokowitz, G. E. Longdon, and L. Chang, A New Paradigm Hidden in Steganography, *Proc. NSPW*, Ballycotton, County Cork, Ireland, pp 12 ACM, Sept 2000.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, SPINS: Security protocols for sensor networks, *Proc. MOBICOM'2001*, Rome, Italy, August 2001.

[12] A. Pfitzmann, B. Pfitzmann and M. Waidner, Trusting mobile user devices and security modules, *IEEE Computer*, February 1997.

[13] TinySec http://www.cs.berkeley.edu/~nks/tinysec/

[14] A. Wadaa, S. Olariu, L. Wilson, K. Jones, and Q. Xu, On training wireless sensor networks, *Proc. 3-rd International Workshop on Wireless, Mobile and Ad Hoc Networks*, Nice, France, April 2003.

[15] B. Warneke, M. Last, B. Leibowitz, and K. Pister, SmartDust: communicating with a cubic-millimeter computer, *IEEE Computer*, vol. 34, no. 1, January 2001, 44-51.

[16] A. D. Wood and J. A. Stankovic, Denial of service in sensor networks, *IEEE Computer*, October 2002, 54-62.

[17] Y. Zhang and W. Lee, Intrusion detection in ad-hoc networks, *Proc of MOBICOM'2000*, Boston, August 6-11, 2000.

[18] L. Zhou and Z.J. Haas, Securing ad-hoc networks, *IEEE Network*, vol. 13, no. 6, 1999, 24-30.

[19] J. Zyren, T. Godfrey and D. Eaton, Does frequency hopping enhance security? http://www.packetnexus.com/docs/20010419_frequency Hopping.pdf