WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2008; **8**:369–384
Published online 17 December 2007 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/wcm.583

An application-driven approach to designing secure wireless sensor networks

Eric Sabbah, Kyoung-Don Kang, Nael Abu-Ghazaleh*,[†], Adnan Majeed and Ke Liu
Department of Computer Science, State University of New York at Binghamton, NY, U.S.A.

Summary

Wireless sensor networks (WSNs) have recently attracted a lot of interest due to the wide range of applications they enable. Unfortunately, WSNs are exposed to numerous security threats that can adversely affect the success of important applications. Securing WSNs is challenging due to their limited capabilities and the unique nature of the network and applications. In this paper, we argue that the WSN security research generally considers mechanisms that are modeled after and evaluated against abstract applications and WSN organizations. Instead, we propose that the solution for WSN security must be sensitive to the application and infrastructure. Specifically, we formulate a new notion of an application-specific security context as the combination of a potential attacker's motivation and the WSN vulnerability. The vulnerability is a function of factors such as the sensor field, WSN infrastructure, application, protocols, system software, accessibility, and the observability of the WSN. To reduce the vulnerability, we argue that WSN design must balance security with traditional objectives such as the cost, energy efficiency, and application level performance to a degree proportional to the attacker's motivation. We illustrate this argument *via* four example applications. Overall, our work can be considered a basis to derive more grounded and realistic assumptions for WSN security and develop cost-effective security solutions to handle application-specific vulnerabilities in WSNs. Copyright © 2007 John Wiley & Sons, Ltd.

KEY WORDS: security; sensor networks; application-driven perspective

1. Introduction

Wireless sensor networks (WSNs) is an area of great interest to both academia and industry. They open the door to a large number of military, industrial, scientific, civilian, and commercial applications. They allow cost-effective sensing in a number of applications especially where human observation or traditional sensors would be undesirable, inefficient, expensive, or dangerous.

Even from their earliest applications, sensor networks have been targeted for attack by adversaries with interest in intercepting the data being sent, or in reducing the ability of the network to carry out its mission. Wireless sensors have limited energy and computational capabilities, making many traditional security methodologies difficult or impossible to utilize. Also, they are often deployed in open areas, allowing physical attacks such as jamming or node capture and tampering. Significant research effort has been extended to address these problems, including (but are not limited to) References [1–14]. Although these contributions are invaluable, most existing work

*Correspondence to: Nael Abu-Ghazaleh, Department of Computer Science, State University of New York at Binghamton, NY, U.S.A.

[†] E-mail: nael@cs.binghamton.edu

does not provide any guidelines to help application designers (or developers) to choose appropriate security mechanisms for their applications or specify the required new security schemes for their applications.

The main premise of this paper is that the large variety of application types and conditions in which WSNs operate make it difficult to discuss security without considering the application-specific context. It is known that security is not only a technical problem. For example, the integral relationships between economics/social issues and security [15,16]/privacy [17] are well studied, and their implications on system design in traditional systems are accepted. It is also critical to consider the specific application of interest to design a security solution; many existing security solutions fail not because the used mechanisms are weak but because they were used inappropriately [18]. Given the wide range of WSN applications with different levels of importance, scale, and structure, keeping these relationships in mind is essential. We present this application-driven perspective in more detail in Section 2.

In this paper, we argue that *the design of secure WSNs should consider the application-specific security context. Further, the set of assumptions made by security research in WSNs must be closely tied to the target application.* Our contribution is to suggest a set of factors that can be used to formalize this security relevant context and show how they apply to different applications. These factors include the *environment in which the application runs, expected threats in the environment, criticality of sensor data, expected gain of an attack, and the scale of the WSN to be deployed.* Our hope is that this work will be a step toward defining reasonable WSN security scenarios and enabling WSN security research with more grounded and realistic assumptions.

Most existing WSN security work considers an abstract sensor network and select assumptions and organizations that are decoupled from application details. Thus, they consider one or more theoretical vulnerabilities of an abstract sensor network model, rarely considering application-specific security threats and requirements. A review of existing work on WSN security is given in Section 3.[‡] We argue that the existing work can serve as mechanisms in a security policy that is driven by the security context.

We illustrate the application-driven perspective on security argument by applying it to four traditional WSN applications: habitat monitoring, health care monitoring, natural disaster recovery, and battlefield monitoring. These applications have diverse security vulnerabilities and motivation for attack. Sections 4 through 7 discuss the security issues that arise in the applications selected in this paper, and suggest general approaches to addressing these concerns in an application-driven manner. Finally, Section 8 concludes the paper and discusses directions for future work.

2. Security Context and Implications on WSN Design

The threats present to a WSN and the organization of the WSN in response to these threats are directly influenced by the application. Therefore, WSN security design and analysis must be sensitive to this context. Otherwise, the assumptions made on the organization of the WSN and the corresponding threats may become inconsistent with the problem domain, leading to solutions that address unrealistic problems.

The security context is not a precise technical specification; rather, it is a set of security-related factors narrowing down the WSN design space to the region that is consistent with them. Clearly, conventional constraints on WSN design such as cost, form factor, and energy must also be taken into consideration. We describe the security context in terms of two related groups of factors related to the WSN and its application: (i) *attacker motivation* and (ii) *vulnerabilities, or attack opportunities.*

2.1. Attacker Motivation

Motivation refers to the benefit the attacker hopes to gain from the attack. This can be further broken down into one of two classes of gains:

- *Benefit from data*: One of the motivations for attacking a WSN deployed for some applications is to gain access to the sensitive data being monitored or relayed. Thus, the goal of the attacker is access to the data being carried or meta data about the users or their activities. The emphasis for these types of applications is on confidentiality and privacy preserving measures.

[‡] Note that we claim our work to be a neither complete nor comprehensive survey. There have been other surveys regarding sensor network security including References [19–21]. However, they tend to focus on outlining the insecurity of specific existing protocols that were not designed to be secure.

DOI: 10.1002/wcm

- *Mission interference*: Another motivation for attacking a WSN is to interfere with its mission. In this case, the data carried by the WSN is not necessarily interesting to the attacker. Instead, he desires to compromise the WSN's ability to function. In these types of applications, the adversary is often being monitored and desires to circumvent this monitoring by falsifying data or disrupting the network or a subset of it. Here, attacks on the infrastructure and services enabling the WSN or data tampering attacks can achieve the desired effect. Note that not all points in the WSN are of equal benefit for disruption; disrupting critical relay nodes, nodes with unique coverage, or even the base station can result in disproportionately more damage than some redundant sensors that do not play an important role. Further, we distinguish between attacks that are *detectable*, and those that are not. In the latter case, the attacker's benefit may be enhanced, because the observer may act based on bad or manipulated data. If the failure is detectable, the observer may employ backup monitoring mechanisms or stop considering the WSN as a valid source of data.

Note that these two types of benefits may exist concurrently in an application. Further, in sensor and actuator networks, the benefit may be in terms of the action taken (or not taken) by the actuators. Regardless of the mode of benefit, the relative degree of benefit is an indicator of potential attackers' *motivation* as well as their relative *preference* among the different attacks. Thus, it is also an indicator of how much the designer and operator of the WSN should protect against these attacks. Finally, we note that accurately quantifying benefit is difficult. For example, some attacks such as vandalism, which has no tangible benefit to attackers, may occur. Therefore, human estimates are often used for utility in similar contexts.

2.2. Vulnerabilities and Opportunities

From an attacker's perspective, the opportunity is essentially a measure of the vulnerability (or the difficulty of attacking it). Given several available attacks, an attacker can perform a cost-benefit analysis based on the opportunities and benefits of the possible attacks to find the most cost-effective attack. There are a number of factors that are unique to WSN infrastructure that present some vulnerabilities to attackers. Especially, the data-driven nature of WSNs introduces a number of unique aspects of operation and corresponding vulnerabilities including:

- *Physical access*: The *in situ* nature of WSNs requires sensors to be integrated with the environment they are monitoring. As a result, the network may be physically vulnerable depending on the nature and extent of the sensor field. In addition, depending on the application, the attacker's access to the vulnerability may be limited, for example, due to the presence of some sensors in inaccessible or busy areas. Access to the sensors can be used to physically destroy them, to capture and subvert them to collect confidential data, or to attempt an insider attack on the network.
- *Wireless communication*: In addition to physical vulnerability of sensors, an outsider attack in WSNs is generally easier than that in a wired network. Attackers may have access to anything transmitted over the wireless channel. Further, attackers can launch an outsider attack by sending their own packets to inject false data or interfere with legitimate transmissions.
- *Attacks on coordination and self-configuration*: The nature of WSNs requires coordination among sensor nodes and self-configuration of the network *via* distributed protocols with localized interactions [22]. In many applications, WSNs heavily rely on cooperative services such as routing, localization, time synchronization, and in-network data processing to self-configure and collaboratively process data. Unfortunately, these services represent unique vulnerabilities which, with the exception of routing vulnerabilities, are not often encountered in conventional networks. For example, compromised nodes can claim the false proximity to the sink to attract packets, considerably increase the clock skew to disrupt coordinated network operations such as sleep scheduling, and inject false data to reduce the accuracy of sensing. Thus, attacks on fundamental coordination and self-configuration functions can be detrimental.
- *Observability of the network*: Clearly, understanding the span and structure of the network opens up risks for more precise and effective attacks. The observability of the network depends on a number of factors including the expected mission lifetime,[§] the observability of deployment and communications, and the access of the attacker to the sensor field. Beyond mere detection of the presence of the

[§] The longer the network runs, the more likely it is to be detected.

DOI: 10.1002/wcm

network, discerning the structure of the network invites more efficient attacks, for example, targeted for the base station or critical relay nodes.

2.3. Implications on WSN Design

There are a number of design choices for WSNs in terms of sensor types and capabilities, sensor density and distribution, as well as great flexibility in the software used to run on the sensors. Typically, the design of these elements is driven by the cost, energy-efficiency, and application-level performance such as the coverage or accuracy.

In applications with a high attacker motivation, the WSN design may trade off the cost or performance to reduce vulnerabilities to acceptable levels. At the physical level, this can translate to purchasing more expensive and/or tamper resistant sensors, or purchasing more sensors to introduce redundancy to better tolerate attacks. For example, the network can be better protected by using multiple base stations when the attacker's motivation for attacking a single base station is expected to be high. These extra capabilities may be deployed or tasked non-uniformly depending on the application. For example, more expensive sensors may be tasked with critical roles in underlying services or may be used in less secure areas of the network.

In terms of protocols, services, and application software, the tradeoff between security and performance is more explicit. Vulnerabilities arise especially in the setup stage of critical services such as routing. Protocols such as geographic routing expose the location of the destination in each packet, which could in turn enable attacks on critical points of the infrastructure. The use of encryption can improve confidentiality at the price of energy and computational resources; the size of the encryption key makes this a tunable tradeoff. In addition, to protect the structure of the network, anomaly and intrusion detection as well as trust management approaches should be employed. They enable detection of attacks and tolerating them, if possible, by isolating misbehaving nodes. Using per-hop encryption facilitates in-network data processing but may leave the network vulnerable to a few nodes becoming compromised and extracting the data in flight. In critical applications, end-to-end encryption may be used, causing a drop in energy efficiency due to the lack of in-network aggregation.

We contend that the attacker motivation and vulnerabilities associated with specific applications and sensor fields should be considered when making effective and secure design decisions. These factors should set the integrated security policy that can be composed using the mechanisms proposed in literature. Alternatively, the integrated policy can indicate how existing mechanisms should be extended, if necessary, to support the security of a specific application.

3. Security Issues and Existing Solutions

In the previous section, we argued for an application-driven perspective for WSN security. In this section, we survey some of the the solutions developed to address WSN vulnerabilities. While many of these security concerns are shared with other wireless networks and even traditional networks, the limited resources and data-driven nature of WSNs introduce special considerations that often require different solutions. We emphasize that these solutions are often presented and evaluated in the abstract, decoupled from the issues discussed in Section 2. As such, we view them as useful mechanisms to be used in an integrated application driven policy for WSN security.

3.1. Supporting Confidentiality, Integrity, and Authenticity

Traditional approaches can be used to support confidentiality, integrity, and authenticity in WSNs. Data can be encrypted to support confidentiality. Unless an adversary has the cryptographic key used for encryption, (s)he cannot read the encrypted sensor data. To support data integrity and authenticity, the sender can compute the message authentication code (MAC) on the message to be transmitted using a keyed one-way hash function. Upon receiving the message, the receiver can verify the MAC by applying the publicly known one-way hash function to the received data using the key. If the verification is successful, the receiver knows that the message has not been altered during the transit and the message is actually sent by the sender. This is because only the sender and receiver share the key unless the key is exposed to a third party. Replay attacks, in which an adversary replays old messages, can also be avoided by including the counter value (or sequence number) when the sender computes the MAC.

SPINS [1] and TinySec [2] can support message confidentiality, integrity, and authenticity in WSNs. μTESLA [1] can support authenticated broadcast in which only the base station can securely broadcast legitimate messages. Notably, most existing work including References [1,2] are based on the secret key system in which the sender and receiver share a

DOI: 10.1002/wcm

secret key. Although a public key system simplifies the difficult task of key distribution, it is several orders of magnitude more expensive than a secret key system in terms of computational complexity. For example, ecTinyOS [3] takes several minutes to run in the worst case. Also, end-to-end encryption is often inefficient because it makes it impossible to carry out in-network data processing such as data aggregation, which can yield significant improvement in efficiency. The simplest approach for encryption, message authentication, and in-network data processing is using a network-wide global key. However, this approach could be dangerous, because an adversary can get access to the entire network by compromising a single node. Better solutions involve the use of pairwise shared keys between neighbors and/or cluster-based shared keys. To this end, many approaches for key distribution in WSNs are developed to support link-layer secret key solutions.

3.2. Key Distribution

Eschenauer and Gligor [12] did one of the first work considering the key distribution problem in sensor networks. Since sensors are often deployed randomly, it is impossible to predefine the key sharing relations between sensors. In their approach, a sensor randomly chooses m keys from the key pool with n keys before the deployment. After being deployed, it contacts with its neighbors to see if it shares any key with its neighbor. m can be tuned to support the high probability for two neighboring nodes share at least one key. Notably, their approach do not require the base station to be involved in key distribution.

Chen *et al.* [13] extends Reference [12] in three ways. (Their basic scheme is similar to Reference [12].) In the *q-composite random key predistribution scheme*, q common keys instead of just one are used to compute a shared key, *via* hashing, between two nodes. An advantage of this approach is that an adversary needs to capture and compromise more nodes to compromise the same fraction of communications as the basic scheme. However, the resilience becomes even worse than the basic scheme as more sensors are compromised. In the *multi-path key reinforcement scheme*, a message is partitioned into several fragments and each fragment is routed through a separate secure path. Thus, an adversary should compromise at least one node in each path to retrieve the original data. Unfortunately, its overhead is higher than the basic scheme's overhead by an order of the magnitude. They also propose the *random-pairwise scheme* which is resilient to node capture, while providing node-to-node authentication. In predeployment, it generates N unique node identities. This N maybe larger than the number of nodes in the network, allowing for more nodes to be added later. Each node identity is matched up with m other randomly selected distinct node identities, and a unique pairwise key is generated for each pair. The key and the paired IDs are stored in both key rings. After the deployment, each node broadcasts its identity to its neighbors and searches for received IDs in its key ring.

Zhu *et al.* [23] propose a novel key management protocol called localized encryption and authentication protocol (LEAP) to support in-network processing, while restricting the impact of a compromised node, if any. The key idea is based on the observation that there are different types of messages in sensor networks, for example, routing control messages, queries, sensor readings, with different security requirements. For example, the authenticity should be supported for every message. However, control messages for routing may not have to be kept confidential, while sensor readings can be secret. To this end, they propose to use four different types of keys, that is, individual keys shared with the base station, group key, cluster key, and pairwise shared key.

3.3. Secure Localization and Location Verification

Location information is critical in many WSN applications. Most sensor readings, for example, for environmental/structural monitoring, fire detection, or target tracking, can be meaningless without location information. Although the simplest way of providing accurate location information is to equip each sensor with a GPS, this is too expensive. Recently, a lot of work has been done for localization in WSNs [24–31]. However, these approaches are designed without considering security. Thus, a compromised or malicious node can claim virtually any location.

Lazos *et al.* [32] propose a novel approach for secure range-independent localization. Their protocol can enable a sensor node to securely derive its location using trusted anchors. This protocol considers attacks on the localization mechanism that intends to cause nodes to have erroneous location information. However, this approach does not prevent a misbehaving node from lying about its own location to its neighbors.

To prevent a sensor node from falsifying its location, Sastry *et al.* have proposed a location verification scheme [14] in which a sensor node needs to send its location claim to a verifier that subsequently sends back

DOI: 10.1002/wcm

a challenge to the node. When the node receives the challenge, it should immediately reply to the verifier, through an ultrasonic channel, with the random nonce that was included in the original challenge message. To verify the location, the verifier measures the delay between the challenge and response. It compares the measured delay to the delay estimated according to the claimed location and speed of sound. Unfortunately, this approach requires ultrasonic hardware. It verifies the claimed location relative to only one verifier. Moreover, an immediate response may not always be possible, for example, due to overloads or packet losses. As a result, honest nodes could be unnecessarily invalidated. We have developed a different approach [33] for location verification that does not require an ultrasonic channel, while providing more accurate full location verification, rather than relying on the distance to a single verifier [14]. The key idea is reversing the triangulation process in localization. A sensor node is required to send a localization request *via* a radio transmission. Surrounding anchors localize the requesting sensor and issue the certified location information to the sensor.

An additional security flaw exists in localization algorithms. Beacon nodes that are assumed to know their own locations may also be compromised or replaced with malicious ones. A method of fighting against such attacks is discussed in Reference [4]. Non-malicious beacon nodes test for malicious ones by sending them a location request, and estimating their distance based on the round trip time of this request. This estimated distance is compared to the distance calculated from the claimed location and the beacon's own, known location. If the distances are substantially different,[‖] the testing beacon considers the tested beacon to be malicious, and reports this finding to the base station. The base station makes revocation decisions based on a combination of given threshold parameters, statistics about how many beacons have signaled mistrust in a potential adversary, and information about how many such mistrust reports each node makes to prevent a denial of service (DoS) attack where attacker gets legitimate nodes revoked. Another option when dealing with localization in the presence of malicious beacon nodes is to attempt to tolerate their presence rather than weed them out [5]. This can reduce overheads by eliminating extra messages used in the previous approach for both testing and revocation.

3.4. Resilient Routing

Ideally, appropriate recovery actions can be taken if the correct error/attack information is given; however, Intrusion detection is difficult in WSNs that involve a lot of errors and potential attacks. Due to the noisy, dynamic environment, it is hard to detect errors/attacks and distinguish between errors and attacks [34]. Also, the WSN under attack should continue to work while the source of error/attack is determined. Hence, it is essential to develop routing protocols resilient to attacks such as References [10,33,35]

Intrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) [10] can minimize the affected region of the network under attack. It works in three phases: pre-deployment, route discovery, and data forwarding. The pre-deployment phase is similar to μTESLA. After deployment, and periodically thereafter, the base station initiates the route discovery phase, which itself is comprised of three rounds. In the first round, the base station initiates a limited flood of a request message to sensor nodes *via* authenticated broadcast. Each node, upon seeing the request message for the first time, appends its ID (and a MAC of the complete new path generated with its key) to the path in the request message, adds the one-hop sender to its neighbor list, and forwards the request. If it receives a duplicate request with the same sequence number, it still updates its neighbor list, but does not forward the message. In the second round of route discovery: a feedback message—containing the list of neighbors' IDs and a path from itself to the base station (with all the MACs generated in round 1)—is sent back from each node using the individual key shared between the node and the base station to generate MAC on the entire feedback message. In the third round, the base station authenticates this neighborhood information, infers the topology of the entire network from it, computes what each node's routing table should be, and securely sends these tables to their respective nodes using the individual shared keys. Even if a node is captured, it only reveals its individual secret key. Therefore, the adversary cannot spoof paths in its feedback message. During the route discovery, the adversary can replay sequence numbers and thus fool downstream nodes into believing a bogus topology; however, this replay attack can have no effect on upstream nodes. A drawback of this approach is the high overhead due to secure route discovery. Also, it increases the burdens on the base station, decreasing the scalability of WSN applications.

ARRIVE [35] is a robust routing protocol applicable to WSNs with a tree topology. In this approach,

[‖] The degree of being 'substantial' is defined based on a calibration parameter of the algorithm.

DOI: 10.1002/wcm

a node overhears the behavior of the neighboring nodes to make probabilistic packet forwarding decisions. To overcome the unreliability of wireless communications, a node forwards a packet to not only a parent but also its neighbors with the reputation higher than the threshold.

Abu-Ghazaleh *et al.* [33] propose a resilient, multipath geographic routing protocol that can tolerate packet dropping DoS attacks by exploiting the observed trust (or reputation) of one-hop neighbors. If neighboring nodes are found to misbehave, new paths to the sink can be found from the trust information and verified location information. Geographic routing is highly scalable, since a node only has to keep the geographic locations of its one-hop neighbors. Trust information can be accordingly stored without incurring significant overhead. As a result, the scalability is not affected. In addition, mutually trusting nodes can exchange the trust information with each other to build the trust information beyond their one-hop neighbors. Boukerche and Li [36] propose a trust and reputation management scheme in WSNs with minimal delay and energy/bandwidth consumption. Trust-based routing has also been studied in ad hoc networks. Watchdog and Pathrater [37] monitor neighbors to detect misbehaviors in promiscuous mode. In AODV-S [38], a node monitors its neighbors to determine their trustworthiness and broadcasts intrusion detection messages to exclude misbehaving nodes from future routing. IS-AODV [39] also detects misbehaviors, similar to Reference [37,38]. However, it adopts lightweight cryptography. Further, different from AODV-S, it does not broadcast intrusion detection messages to avoid the possibility that attackers take advantage of the intrusion detection information. Instead, a node does not cooperate with a misbehaving node upon detection. In this way, trusted nodes can eventually get clustered. These protocols can be adapted for trust-based routing in WSNs considering the WSN security context.

3.5. Resilient Data Aggregation and False Data Filtering

Since transmission is most energy consuming, in-network data aggregation is a must in WSNs. The need for aggregation makes end-to-end cryptography infeasible as discussed before. In addition, an adversary can seriously hamper sensing applications by manipulating data even without having to disrupt other fundamental components such as routing or localization. An attack on an aggregation point allows an adversary to corrupt not only all the data from the downstream nodes but also the overall data aggregation result observed at the base station. Thus, in an extreme case, the adversary could damage the WSN as much as if (s)he had captured many individual sensor nodes by attacking a single node.

To address this issue, Pryzatek *et al.* [7] propose a secure data aggregation scheme. By random sampling and interactive proofs, in their approach, users can verify that the answers given by the aggregators are a reasonable approximation of the true value even when the aggregator or a subset of the sensors are compromised. Especially, they focus on the approaches to securely compute the median and average.

Wagner [11] has shown that the popular query operators such as minimum, maximum, sum, and mean are all insecure aggregation functions, because they can be affected to any desired degree by a single malicious value. He has defined the notion of *approximate integrity* and suggested to apply statistical approaches based on robust statistics to limit the impact of the data modified or injected by an adversary on the aggregation.

Baslie *et al.* [34] propose an on-the-fly approach to detect attacks on sensor data values and distinguish them from errors by applying statistical approaches based on Hidden Markov Models. One of the key observations is that calibration errors are nearly constant, while attacks are dynamic in that they dynamically adjust fabricated sensor readings to affect the overall sensing operation.

Generally, a good solution should provide accuracy at the base station. Also, it should eliminate the injected data as soon as possible to avoid unnecessary forwarding, which reduces the battery life. Zhu *et al.* [8] have recently proposed an approach that can filter out an injected false data if at most t nodes are compromised. In this approach, the WSN becomes more secure as t increases for the increasing cost. (As t increases, the total number of MACs increases and MACs should be transmitted farther before being verified.)

3.6. Anti-Traffic Analysis

As opposed to wired networks, or even ad hoc networks, the traffic flow in sensor networks tends to be limited to a few patterns [20]. Commands flow from the base station(s) to the nodes, data flows from the nodes to the base station(s), and there may be some local communication for a cluster head election or data aggregation [8]. This inevitably leads to the

DOI: 10.1002/wcm

problem of traffic analysis which can allow an attacker to figure out where the base station is located, and concentrate on attacking it, or the nodes closest to it for maximal impacts. Most protocols tend to assume that the base station is not compromised. On the other hand, most data flows are directed to the base station. Thus, successful attacks on it or the nodes near it could be catastrophic.

One approach to dealing with this issue is to make it difficult for the adversary to analyze the traffic patterns and thus discern which of the nodes are in this category. Deng *et al.* [9] discuss an approach for anti-traffic analysis. The simplest step that must be taken is to encrypt all information in a packet to hide the routing information. However, this is insufficient because monitoring the volume and path of data flow can yield the required information. There are two main vulnerabilities an adversary can exploit, namely rate monitoring and time correlation. Exploiting rate monitoring involves an adversary tracking the packet-sending rate of nearby nodes and moving toward those with higher rates, until it reaches the base station. An attacker can also examine the correlation in sending time between a node and the next hop's forwarding operation, and figure out the path to the base station by following the packet propagation. Sensor nodes could wait random intervals before forwarding packets, but this may not be sufficient defense in applications which may have some high-priority, time-sensitive packets that an attacker can initiate (especially an insider). Boukerche *et al.* [40] propose an efficient anonymous routing protocol for wireless ad hoc networks. In their approach, only trustworthy intermediate nodes are allowed to take a part in the path construction. At the same time, the anonymity of the communicating nodes are supported to avoid a possible traffic analysis. Their approach could be adapted for WSNs.

To address the problem, Deng *et al.* outline four techniques to reduce the uniform directionality of traffic flow. The first technique is to allow nodes to forward packets to one of a set of parent nodes to make routing patterns less evident. In addition, a random walk can be incorporated into the path a packet travels to distribute data flow and diminish the harm that rate monitoring can accomplish. Thirdly, some randomized subset of forwarding nodes can create dummy packets and forward them along bogus paths to frustrate the potential attackers' attempts to track packets movements toward a base station. Finally, various, random areas of high traffic can be produced, which would trick adversaries into believing the base station is someplace other than its genuine position. Despite the importance, anti-traffic analysis has received relatively little research attention. Clearly, more work is needed. Also, it is critical to redesign the WSN architecture to make it less vulnerable. Otherwise, there could be a great difficulty in deploying and running WSNs especially in a hostile environment.

3.7. Secure Code Distribution

It can be useful to have the capability of reprogramming wireless sensor nodes *in situ*. Deployed sensor nodes may need bug fixes, extension of features, or additional new applications. However, taking the nodes offline to fulfill such needs is inefficient. It may not even be possible if they are deployed in hostile environments.

If an adversary can reprogram nodes easily, then they can bypass all other security precautions. This could result in bringing down the network, stealing sensitive data, injecting false information, severe privacy violations, and susceptibility to virtually any of the attacks mentioned in this paper (and more). Thus, it is crucial for nodes to have the ability to verify that new code has been transmitted unaltered from a trusted source.

Early reprogramming methodologies developed for WSNs, such as Deluge [41], Aqueduct [42], MNP [43], and MOAP [44] enable code distribution in a WSN; however, they are not designed to be secure. To address the security issue, a protocol using public key cryptography for signing a chain of cryptographic hashes is implemented in Deluge [45]. However, there is still a need for a mechanism to reduce the high traffic overhead, while remaining resilient in the presence of node compromise and DoS attacks.

The benefits of using public key algorithms are that they streamline key distribution. In addition, they ensure that stealing the public key through node capture does not allow an adversary to spoof the base station. However, they are slow and require large amounts of memory. To address the problem, Krontiris and Dimitriou [46] extend the hash to obtain random subset (HORS) r-times signature algorithm [47] that works as follows:

1. The signer calculates a secret key made up of a number, t, of random values of a given bit length each.
2. The public key is then derived through the application of a one-way hash function to each of the values of the secret key.
3. Finally, these hashed values are disseminated to their predetermined destination nodes in an authenticated manner.

Specifically, they compensate for the limited memory of sensor nodes by reducing the size of the public key using Merkle trees [48]. The values of the secret key, mentioned in the first bullet above, are split into a number of groups, T, each with t/T such values. Each group then forms a set of leaves of a tree, so that there are T trees. The parents in these trees consist of hash values taken on all their children. The hashing is recursively applied toward the roots that ultimately become the new public key of the enhanced scheme. As a result, a signature now consists of the appropriate secret values and their corresponding path in the tree.

Gennaro and Rohatgi [49] adapt [46] by treating secure code distribution as a problem of signing digital streams, reducing the overhead by breaking the stream into blocks and implanting in each a hash of the subsequent block. Thus, the sender needs to sign only the initial block, and the rest of the blocks will be verified through 'chaining.' Signed hash chains incur very little overhead, since they require only one public key operation per chain. However, they do not tolerate out of order arrivals, which often occur in wireless networks. Hash tree-based schemes allow sensor nodes to verify packets which arrive out of order. Unfortunately, these methodologies generally involve larger memory overhead and more public key operations than hash chains. Deng *et al.*'s approach [50] attempts to combine the utility of these schemes into a hybrid approach such that their algorithm uses hash chains for inter-page authentication and hash trees for internal page authentication. As a result, their approach achieves:

- Resilience to node capture attacks, since all packets are ultimately protected by the public key and hash chain/tree framework.
- Resilience to certain DoS attacks due to the fact that the hash tree portion of the system ensures quick authentication of packets.
- Efficiency of performing public key authentication only once per code dissemination, while more rapid hash-based authentication is done for all packets other than the initial one.
- Reduction in wasted retransmissions, which would significantly decrease the battery life, due to the ability to perform out of order processing.

From this review of the related work (and others not included due to space limitations), we observe that they consider these vulnerabilities using sample scenarios that are not tied to specific applications. While generalizing the analysis is valuable, we argue that there are classes of WSN applications that give rise to different threats and require different organizations to address their security concerns. In the following sections, we will discuss whether the existing security solutions described in this section are necessary and/or appropriate for four canonical WSN applications with widely varying security issues to discuss application-driven perspectives on secure WSN application design.

4. Habitat Monitoring

The main advantage of WSNs is that they can provide high resolution information about the surroundings they are placed in. Thus, their use for habitat monitoring is a natural application. Sensor nodes are better for this purpose compared to human observers as human presence can change the behavior of the environment being studied by causing the 'observer effect.' The sensor networks deployed to monitor the Great Duck Island and the James Reserve [51] are two examples of how useful WSNs can be in habitat monitoring.

One important aspect of any attack on a network is the benefit to the adversary that needs to be considered for the deployment of a security. In the case of a habitat monitoring WSN such as those deployed at the Great Duck Island or the James Reserve, the only reason for an attack would be vandalism as one would hardly gain any benefit from attacking such a network. This would mean that the motivation of mounting an attack would be limited, and therefore, such a network may operate properly with moderate security mechanisms. Especially, there is not much concern about eavesdropping, physical compromise, or a traffic-analysis and subsequent attack.

Specifically, the requirements of a WSN for habitat monitoring is that it should relay correct information about the environment it is placed in. This requirement can be broken down into (i) guaranteeing integrity and authenticity of data; (ii) correctly routing the data to the base station or observers; and (iii) append correct context, for example, time stamps and the location where the data was gathered, to the information gathered.

Although it may not always be true, habitat monitoring applications such as Reference [51] would not generally be too concerned about the confidentiality of data, for example, data collected in the Great Duck Island. If a WSN is deployed for habitat monitoring expecting no observer effect, it can be assumed that there should be minimal human presence in the area and physical attacks on the sensor nodes incur little

DOI: 10.1002/wcm

concern. Additionally, the data being gathered would often be for later scientific studies and not time critical. Therefore, energy conservation for a long-term observation will be more important than real-time delivery or excessively expensive security measures. The related threats to such a WSN and recommended countermeasures are discussed as follows.

- *Attacks on integrity and authenticity*: Since the key objective is data collection, a main threat would be for an adversary to pollute the data. The integrity and authenticity of messages from the sensing nodes need to be supported *via* a cost-effective approach such as References [1,2]. Otherwise, without being detected, an adversarial node can modify data, transmit a false data claiming it is originated from a legitimate node, or replay old data. A key predistribution schemes similar to the ones discussed in Subsection 3.2 can be used to distribute cryptographic keys such that nodes can directly communicate in a secure manner to improve the scalability. In addition, secure localization or location verification is necessary when sensor nodes are initially deployed or newly added to provide the correct context information discussed above. This way, the location information, medium access control address, and cryptographic key can be used to verify, for example, *via* challenge/response, the identity of a node.
- *Attacks on routing and DoS attacks*: A prerequisite for authentic data reporting is for the network to correctly route packets to the desired nodes. Even very simple DoS attacks such as packet dropping or misrouting can severely disrupt habitat monitoring. Resilient routing protocols that can deliver a large fraction of data even under attack will be useful to handle this problem as discussed in Section 3. An adversary may consider more disruptive attacks such as jamming too expensive for relatively little monetary or tactical gains. From an attacker's perspective, traffic-analysis enabling a subsequent DoS attack on the base station or the nearby sensors, can also be considered cost ineffective. Thus, in general, anti-traffic analysis may not be necessary.
- *Injecting false packets*: An adversary can inject false data into the network. Injection will be especially straightforward if there is no integrity/authenticity support, because the adversary does not have to compromise any node in this case. Adversarial nodes can use correct cryptographic keys and follow the routing protocol as required. Statistical approaches can be cost effective to deal with this kind of attacks. Especially, it is important to maintain the correctness of those queries such as min or max that are more vulnerable to false data injection [11]. Domain specific knowledge, for example, observer effects, can also be exploited to further improve the statistical defense.

To summarize, a cost-effective security solution for habitat monitoring can consist of lightweight authenticity/integrity support (e.g., [1,2]), intrusion detection of application-specific observer effects whose model can be provided by domain experts, and efficient resilient routing protocols such as the ones described in Subsection 3.4.

5. Medical Applications

There is abundant potential for medical applications involving WNSs [52–56]. One of particular importance is the remote monitoring of patients, especially in the context of elder care. Wireless sensors can play several key roles in these applications: wearable devices can track predefined symptoms and vital signs to be transmitted to health care professionals at regular intervals or upon reaching emergency thresholds [57]. Smart appliances can assist in wellness through reminders of proper meal and medication times. Accidents such as falls can be detected and appropriate actions can ensue [58,59]. Also, when emergency care is needed, the caregivers can quickly access key information such as the patient history, current medications, and any allergy to certain medications from the home sensor network [60]. As a result, a faster facilitation of needed medical services is possible. It can also increase the quality of life due to enhanced mobility, the possibility of living at home instead of a treatment facility, and a more efficient allocation of medical professionals' time. They will not have to spend nearly as much time checking on patients (in person or at a stationary console), if they can rely on alert systems being transmitted to their personal digital assistants (PDAs) [61–63].

In addition to general security concerns, privacy concerns are prevalent in medical applications because of the private individual data being monitored. Most people want as few people as possible to know about their health-related statistics. They know that doctors, emergency medical technicians (EMTs), nurses, and insurance company workers will need access to portions of this data, but few want their employers or complete strangers (adversary) to gain

DOI: 10.1002/wcm

such access. There is ample motivation for acquiring the medical data for different adversaries. For example, pharmaceutical companies could use such statistics for scientific and business reasons, employers could use it to make prejudicial decisions about hiring and promotion, and others could use it for advertising or blackmail.

On the other hand, unlike other WSN applications, there can be relatively less concerns about routing and power management as a sensor device may be only a few hops away from the house's base station. Power replenishment can be relatively easy in a smarthome environment. Further, reasonable physical security is possible in a home environment, which limits an adversary's potential access to sensor devices.

Medical application could lead to dire consequences if faced with challenges to confidentiality, integrity, authenticity, DoS, and false data injection types of attacks. A more detailed discussion of these challenges and required solutions is given in the following.

- *Confidentiality, integrity, and authenticity*: These requirements are critical in medical applications as inadvertently exposed or corrupted medical data can incur a number of serious problems as discussed before. For these applications, the application designer needs to consider to apply security protocols stronger than usual sensor network protocols such as the ones discussed in Subsection 3.1 that are mainly focused on minimizing resource requirements. This is reasonable because an adversary, *via* a successful attack, can get monetary/societal gains or even risk patients' health. At the same time, security protocols can take advantage of relatively abundant computational resources and flat network topology.
- *Privacy*: Supporting the message confidentiality, integrity, and authenticity is a basis to secure home medical applications. In addition, privacy should be considered. The issues include not only secrecy and authentication, but also authorization [62–64]. Authorization goes beyond user authentication, for example, *via* passwords, to determine not only who (or what device) is granted access to the system, but what level of access is granted to different users. These issues involve not only patient preference, but also legislative design such as the Health Information Privacy and Portability Act (HIPAA) rules developed by US Department of Health and Human Services (HHS). For example, the information that someone's doctor needs to (and is allowed to) access is certainly different from that needed by a hospital administrator, the patient's employer, or the random Internet peruser. Due to the needs for stronger privacy and confidentiality, fine-grained data access control such as role-based access control [65] is required. Other fundamental mechanisms should also be reconsidered to support privacy. More fine-grained location tracking and motion sensing is necessary, for example, to detect a tripped elder person, in a privacy-aware manner. (A detailed discussion of privacy issues is beyond the scope of this paper.)
- *DoS attacks*: In medical monitoring applications, the performance of the sensor network can literally be life-or-death. Reliable, persistent, and timely transfer of information can be critical especially for emergency situations. On the other hand, it may not be as important to have as stringent demands on, for example, mealtime reminders. It can be relatively hard for an adversary to launch a DoS attacks due to the physical security available in a home environment. However, an adversary can attack the base station or access point connected to the wide area network. Thus, it is important to protect the base station/access point to avoid many possible attacks. In addition, resilient routing including the ones discussed in Subsection 3.4 is necessary to ensure a high data delivery rate even under attack. They can be further extended to support differentiated service considering the type of data, for example, normal vital readings and alerts, to be forwarded.
- *False data injection*: These attacks can cause a catastrophe. Imagine if a cognitively impaired person is tricked into taking their medication half as often (ineffective) or twice as often (overdose) as prescribed. Or, an EMT coming to a home can be led to believe that an unconscious woman is not allergic to a drug that proves to be fatal. Proper protection of the base station and inherent physical security available in a home environment can alleviate the risk of data injection. To further improve security, false data filtering and resilient data aggregation techniques described in Subsection 3.5 can be applied. However, care should be taken, because not all data are allowed to be filtered or aggregated due to related regulations and medical reasons. More research is required to consider allowed data aggregation rules to extend resilient data aggregation.

WSNs for medical applications have unique, complex security requirements with many open research issues. Although it is impossible to suggest a single perfect security solution, general guidelines

DOI: 10.1002/wcm

can be formed by considering the application-specific context as follows: (i) strong confidentiality and privacy must be supported at the cost for relatively high energy consumptions. For example, an application designer and security officer can select the strongest possible cryptographic algorithms that do not exhaust the battery before the care-taker's next periodic visit considering the energy consumptions of different cryptographic algorithms [2,66]. Or, special hardware for ambient energy collection can be used to automatically recharge batteries; (ii) careful selection between link-layer or end-to-end encryption is required. When aggregation is disallowed for some data, end-to-end encryption protocols can avoid potential confidentiality/privacy problems and energy consumptions due to the unnecessary packet decryption and re-encryption at intermediate nodes. Also, sensitive data should be encrypted in an end-to-end manner, while redundant data can be aggregated (if allowed) when link-layer encryption is applied. Thus, a hybrid approach can be more efficient than pure end-to-end or link-layer approaches; (iii) resilient routing is required to ensure the availability of data even in the presence of packet losses or collisions due to an error or malice; (iv) false data filtering needs to be combined with trust-based routing to filter out false data as early as possible while reducing the trust level of a node injecting false data. In this way, trusted nodes can avoid using non-trustworthy nodes to forward their data toward the sink. However, interactions between false data filtering and trust-based routing are unknown in the current state of art; (v) to improve the timeliness of critical data and energy efficiency, service differentiation based on data types, for example, normal vital signs *versus* alerts, is necessary. For service differentiation, an appropriate false data filtering and policing mechanism is also required to prevent an adversary from flooding the network *via* fake alert messages; and (vi) fine-grained distributed access control needs to be integrated with basic network services, for example, routing and localization, to block illegal attempts for data access or network manipulation as much as possible.

6. Natural Disaster Recovery

WSNs can be used in disaster recovery operations including forest fires, earthquakes, epidemics, and chemical spills. In such scenarios, WSNs can provide an ad hoc mechanism for quickly detecting areas that require rescuers' attention. More specifically, disaster recovery application can work by deploying sensors in the recovery zone. After the deployment, sensors can organize themselves into an ad hoc network and perform basic operations such as localization, clock synchronization, and calibration to ensure a common reference point for observations. After these initial phases, sensor nodes can start to take readings of concern to the specific type of disaster, for example, temperature and light for fires, seismic activity for earthquakes, and levels of toxins in the air for chemical spills, and exchange the readings among them. At the same time, sensor data can be accessed by emergency personnel carrying PDAs. In this way, sensor data can be utilized to ensure that recovery resources including emergency personnel, vehicles, and supplies are sent where they are most needed [67,68].

In general, the motivation for attack and access to the network depends on the specific disaster. However, the attacker could be a terrorist trying to disrupt the rescue mission or exacerbate the disaster. Energy conservation may not be the most important issue in a number of disaster recovery applications. For example, earthquake survivors may have to be rescued within a few weeks. Also, in such hostile conditions as intense heat, vibration, or physical shock, many nodes may die out independently of the battery life. Hence, sensors may need to operate at high duty cycles while supporting strong security measures and real-time constraints. Based on this discussion, we identify several security threats and desirable security solutions as follows:

- *Confidentiality, integrity, and authenticity*: Confidentiality may not be critical when dealing with *natural* disasters. For example, when attempting to contain and then extinguish a fire, it may not really matter if outsiders know the temperature or light levels being observed by nodes. However, if the disaster was caused by a terrorist attack or terrorists are suspected to plan to aggravate a naturally caused disaster, strong confidentiality is required. On the other hand, support for message integrity and authenticity is required to prevent any outsider from attacking the WSN by modifying/fabricating messages. Given that the WSN is expected to be relatively short lived, it is worthwhile to consume more energy to ensure resilience to attack.
- *DoS attacks*: In disaster recovery, the capability of quick, reliable data transmission is required. Resilient routing schemes including the approaches described in Subsection 3.4 are required to support the high data delivery rate under routing disruption attacks, for example, blackhole or

DOI: 10.1002/wcm

selective forwarding attacks. Note that resilient routing protocols should not severely affect the performance when there is no attack, because timely and prudent utilization of the limited response capabilities is required to avoid the loss of life or property/environmental damage.

- *Attacks on localization*: Unlike health care applications, disaster zones can be huge, encompassing large portions of a forest or entire cities, as in the Katrina hurricane. Narrowing down the specific hot spots where immediate attention is needed can be crucial. To this end, secure localization and location verification discussed in Subsection 3.3 are critical to correctly identify the location of, for example, seismic activities or survivors. Further, resilient data aggregation discussed in Subsection 3.5 needs to be extended to locate survivors in the presence of error or malice.
- *False data injection attacks*: In the worst case, these attacks can result in DoS against the overall rescue system, for example, by injecting false fire/seismic activity data or survivor data to the WSN. These attacks can disrupt, for example, building the fire dispersion map or survivor information in the affected area. Injected false data can also degrade the real-time performance incurring the loss of life or other damages. Thus, false data filtering and resilient data aggregation discussed in Subsection 3.5 are required.

The security requirements of large-scale disaster recovery applications significantly vary depending on the presence or absence of a terror as discussed above. If no terror is involved, it is more appropriate to maximize the timeliness and availability of data to expedite rescue operations. Cost-effective approaches such as lightweight message authentication and resilient routing can be appropriate. On the other hand, if a terror is involved or expected, a WSN should support strong security features including the ones discussed before. However, it is often difficult to precisely determine whether or not terrorism is involved. Hence, for example, it is possible for a terrorist to successfully attack a WSN that has originally employed lightweight security mechanisms only. An overdesign can avoid this problem by always applying a comprehensive set of strong security measures; however, the cost can be tremendous, adversely affecting the rescue operation due to the decreased data timeliness and unnecessarily high energy consumptions. Therefore, it is essential to allow a WSN to *dynamically (re)configure its own security policy and corresponding mechanisms* possibly using the approaches discussed in Subsection 3.7 to adapt the security protocols based on the presence or possibility of a terror. Moreover, it is critical to support *multi-resolution, resilient data aggregation, and routing* to deal with vast amount of data with timing and security constraints. For example, distant rescuers can only be allowed to see the overall dispersion of survivors in a large area, while the fine-grained location information of the survivors can be found as rescuers approach the area in which the survivors are. This approach can greatly reduce network traffic and corresponding energy consumptions. Also, it could contain possible attacks in a relatively small area by disallowing the propagation of suspicious data, while delivering valid data even under attack.

7. Battlefield Monitoring

Due to the critical nature, the security requirement of WSNs for battlefield monitoring is stringent. Further, the benefit of attacking the network is very high from the adversary's perspective. In an extreme case, a successful defense can result in winning the battle. In such networks, there is very high attacker motivation in detecting the network, accessing the data being measured, and/or disrupting its function. The security requirements of such a WSN would include to (i) support confidentiality, integrity, and authenticity; (ii) correctly route data to the base stations or friendly observers; (iii) append the correct context information; (iv) deliver information within the time constraints (real-time requirement); and (v) avoid a traffic analysis. On the other hand, attacks that can be mounted on such a network are all over the spectrum. These include (but are not limited to) the following.

- *Confidentiality, integrity, authenticity, and injection of false data*: By compromising a few key nodes, an adversary may be able to extract the transmitted data and accordingly make tactical decisions. Such an attack would be well hidden as the compromised nodes could relay all the received data to avoid the detection. Also, an adversary can modify the forwarded information or inject false data, for example, to falsify the enemy troops' location.
- *DoS attacks*: As discussed before, correct routing is an essential part for any network to function properly. Therefore, this is an obvious aspect of the network that can be attacked by an adversary to cripple the network completely or cause it to perform incorrectly.

DOI: 10.1002/wcm

- *Attacks on localization*: An adversary can make nodes interpret their location incorrectly. If a successful attack is mounted on localization, any data may become useless regardless of the correctness of the data itself as the geographic context information (e.g., location of the enemy troops) is compromised.
- *Attacks on real-time requirements*: If an adversary can increase the traffic in a particular area of the network by injecting false or dummy packets, the transmission of critical data to the sink(s) can be delayed. It can be an effective attack, since stale data may become useless in a battle. An adversary can also inject false high-priority messages at different locations in the network to mask authentic high- (and low-) priority messages coming from the location where the adversary's activities are actually being carried out.
- *Attacks on the network using topological information*: If an adversary can extract topological information of a particular area of the network, it can partition the network by simply jamming or physically compromising the nodes critical to the connection of that area with the other. As a result, important sensor data could not be delivered to the sink.

In battlefield monitoring, several optimizations are possible considering the application-specific context information. Based on the geographic location and tactical values, data can be treated in a differentiated manner in terms of security and routing. For example, higher security and timeliness is required if the data origin is closer to the current location of the enemy. On the other hand, security and timing constraints can be relaxed as the enemy move out of the area. Similarly, regular messages reporting no enemy troop movement can be transmitted using link-layer encryption to enable data aggregation. Important messages such as the movement of enemy troops toward the frontline can be routed with high priority using unique end-to-end encryption keys pre-established between individual nodes and the base station to maximize the secrecy of the data while minimizing the delay. Other approaches such as defense against jamming [69] can also be optimized considering the relevant battlefield situations such as the proximity of sensors to the enemy and the presence and pattern of jamming, if any, in the neighborhood. In summary, battlefield monitoring is most challenging among the applications considered in this paper due to its stringent security and timing constraints. It requires a holistic application-driven approach that seamlessly integrates security protocols and network services including defense against jamming, resilient routing, false data filtering, multi-resolution resilient data aggregation and routing, service differentiation based on data types and context information, policing, and WSN reconfiguration considering dynamic tactical situations.

8. Conclusions and Future Work

WSNs are exposed to numerous security threats that can endanger the success of applications. Security support in WSNs is challenging due to the limited energy, communication bandwidth, and computational power. Also, sensors are often deployed in an open environment where no physical security is available. Given the diversity of WSN applications and possibly different security requirements, we think application-driven approaches to securing WSN is necessary. Despite the importance, the related work is relatively scarce. To shed light on this problem, we analyze the security issues prevalent in several important applications and discuss their security requirements. Ultimately, we aim to aid WSN application designers in specifying security requirements for the application they are in charge of. Ideally, given the security requirements, a security officer can configure the desirable security solution from a standard library. Further, a WSN should be able to dynamically reconfigure itself as the situation changes in time. In the future, we will further extend our work by giving a more in-depth discussion of the applications and their security requirements discussed in this paper (and other ones). We plan to perform a case study in which we can apply application-driven approaches to securing a specific WSN application and compare the results to existing approaches that do not take application-centric approaches. Further, we will develop a dynamically reconfigurable WSN security middleware.

References

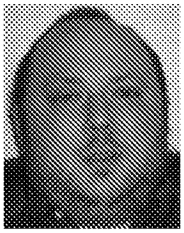
1. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: security protocols for sensor networks. In *MobiCom*, 2001.
2. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks. In *ACM SenSys*, 2004.
3. Malan DJ, Welsh M, Smith MD. A public-key infrastructure for key distribution in tinyOS based on elliptic curve cryptography. In *IEEE SECON*, 2004.
4. Liu D, Ning P, Du W. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *The 25th International Conference on Distributed Computing Systems*, June 2005.
5. Liu D, Ning P, Du WK. Attack-resistant location estimation in sensor networks. In *IPSN'05*, April 2005.
6. Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks: analysis and defenses. In *IPSN'04*, 2004.

7. Przydatek B, Song D, Perrig A. SIA: secure information aggregation in sensor networks. In *Proceedings of ACM SenSys*, 2003.
8. Zhu S, Setia S, Jajodia S, Ning P. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. In *IEEE Symposium on Security and Privacy*, 2004.
9. Deng J, Han R, Mishra S. Countermeasures against traffic analysis attacks in wireless sensor networks. Technical report, CU-CS-987-04, 2004.
10. Deng J, Han R, Mishra S. A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *2nd International Workshop on Information Processing in Sensor Networks (IPSN 03)*, April 2003.
11. Wagner D. Resilient aggregation in sensor networks. *SASN'04*, October 2004.
12. Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In *the 9th ACM conference on Computer and Communications Security*, 2002.
13. Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. *IEEE Symposium on Security and Privacy*, May 2003.
14. Sastry N, Shankar U, Wagner D. Secure verification of location claims. In *the ACM workshop on Wireless Security*, 2003.
15. Odlyzko AM. Economics, psychology, and sociology of security. In *Financial Cryptography: 7th International Conference, no. 2742 in Lecture Notes in Computer Science*, Springer, Guadeloupe, French West Indies, 2003; 182–189.
16. Anderson R. Why information security is hard—an economic perspective. In *17th Annual Computer Security Applications Conference*, 2001.
17. Odlyzko AM. Privacy, economics, and price discrimination on the internet. In *ACM ICEC2003: Fifth International Conference on Electronic Commerce* 2003; 355–366.
18. Anderson R. *Security Engineering*. John Wiley and Sons, Inc.: NY, NY, 2001.
19. Wood AD, Stankovic JA. Denial of service in sensor networks. *IEEE Computer* September 2002; 54–62.
20. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. *Elsevier's AdHoc Networks Journal* 2003; **1**(2–3): 293–315.
21. Perrig A, Stankovic JA, Wagner D. Security in wireless sensor networks. *Communications of the ACM* 2004; **47**(6): 53–57.
22. Estrin D, Govindan R, Heidemann JS, Kumar S. Next century challenges: scalable coordination in sensor networks. In *Mobile Computing and Networking*, 1999; 263–270.
23. Zhu S, Setia S, Jajodia S. LEAP: efficient security mechanisms for large-scale distributed sensor networks. In *the 10th ACM Conference on Computer and Communications Security (CCS '03)*, 2003.
24. He T, Huang C, Blum BM, Stankovic JA, Abdelzaher T. Range-free localization schemes for large scale sensor networks. In *MobiCom'03*, San Diego, CA, 2003.
25. Wellenhoff BH, Lichtenegger H, Collins J. *Global Positioning System: Theory and Practice* (4th edn). Springer Verlag: Austria, 1997.
26. Savvides A, Han CC, Srivastava MB. Dynamic fine-grained localization in ad-hoc networks of sensors. In *MOBICOM'01*, July 2001.
27. Bahl P, Padmanabhan VN. RADAR: an in-building RF-based user location and tracking system. In *Proceedings of the IEEE INFOCOM'00*, March 2000.
28. Niculescu D, Nath B. Ad hoc positioning system (APS) using AoA. In *INFOCOM'03*, 2003.
29. Bulusu N, Heidemann J, Estrin D. GPS-less low-cost outdoor localization for very small devices. *IEEE Personal Communication*, 2000.
30. Niculescu D, Nath B. DV based positioning in ad hoc networks. *Journal of Telecommunication Systems*, 2003; **22**: 267–280.
31. Nagpal R. Organizing a global coordinate system from local information on an amorphous computer. Technical Report A.I. Memo 1666, MIT A.I. Laboratory, August 1999.
32. Lazos l, Poovendran R. SeRLoc: secure range-independent localization for wireless sensor networks. In *the ACM Workshop on Wireless Security*, 2003.
33. Abu-Ghazaleh N, Kang KD, Liu K. Towards resilient geographic routing in wireless sensor networks. In *1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (Held in Conjunction with ACM/IEEE MSWiM 2005)*, October 2005.
34. Baslie C, Gupta M, Kalbarczyk Z, Iyer RK. An approach for detecting and distinguishing errors versus attacks in sensor networks. In *Performance and Dependability Symposium, International Conference on Dependable Systems and Networks*, 2006.
35. Karlof C, Li Y, Polastre J. ARRIVE: algorithm for robust routing in volatile environments. Technical Report UCB//CSD-03-1233, University of California at Berkeley, 2003.
36. Boukerche A, Xu L. An agent-based trust and reputation management scheme for wireless sensor networks. In *IEEE GLOBECOM*, Vol. 3, 2005.
37. Marti S, Giuli T, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In *ACM/IEEE International Conference on Mobile Computing and Networking*, 2000.
38. Yang H, Meng X. Self-organized network-layer security in mobile ad hoc networks. In *ACM Workshop on Wireless Security*, September 2002.
39. Bononi L, Tacconi C. Intrusion detection for secure clustering and routing in mobile multi-hop wireless networks. *International Journal of Information Security, Springer Berlin/Heidelberg*, July 2007.
40. Boukerche A, El-Khatib K, Xu L, Korba L. An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. *Computer Communications* 2005; **28**(10): 1193–1203.
41. Hui JW, Culler D. The dynamic behavior of a data dissemination protocol for network programming at scale. In *2nd International Conference on Embedded Networked Sensor Systems (SenSys'04)*, November 2004.
42. Phillips LA. Aqueduct: robust and efficient code propagation in heterogeneous wireless sensor networks. Master's Thesis, University of Colorado at Boulder, 2005.
43. Kulkarni SS, Wang L. Mnp: multihop network reprogramming service for sensor networks. In *25th International Conference on Distributed Computing Systems (ICDCS)*, June 2005.
44. Stathopoulos T, Heidemann J, Estrin D. A remote code update mechanism for wireless sensor networks. Technical Report CENS-TR-30, University of California, Los Angeles, Center for Embedded Networked Computing, 2003.
45. Dutta PK, Hui JW, Chu DC, Culler DE. Securing the deluge network programming system. In *5th International Conference on Information Processing in Sensor Networks (IPSN'06)*, April 2006.
46. Krontiris I, Dimitriou T. A practical authentication scheme for inNetwork programming in wireless sensor networks. In *REALWSN'06*, June 2006.
47. Reyzin L, Reyzin N. Better than BiBa: short one-time signatures with fast signing and verifying. In *ACISP '02: Proceedings of the 7th Australian Conference on Information Security and Privacy* 2002; 144–153.
48. Merkle RC. A certified digital signature. In *CRYPTO'89: Proceedings on Advances in Cryptology* 1989; 218–238.
49. Gennaro R, Rohatgi P. How to sign digital streams. *Information and Computation* 2001; **165**: 100–116.

DOI: 10.1002/wcm

50. Deng J, Han R, Mishra S. Secure code distribution in dynamically programmable wireless sensor networks. In *5th International Conference on Information Processing in Sensor Networks (IPSN'06)*, April 2006.
51. Mainwaring A, Polastre J, Szewczyk R, Culler D, Anderson J. Wireless sensor networks for habitat monitoring. In *WSNA*, 2002.
52. House_n: the Home of the Future. http://architecture.mit.edu/house_n/
53. Fulford-Jones T, Malan D, Welsh M, Moulton S. CodeBlue: an ad hoc sensor network infrastructure for emergency medical care. In *International Workshop on Wearable and Implantable Body Sensor Networks*, 2004.
54. Center for Future Health—Smart Medical Home. http://www.futurehealth. rochester.edu/
55. The aware home—georgia institute of technology. http://www.cc.gatech.edu/fce/ahri/projects/index.html
56. Intel. Digital home technologies for aging in place. http://www.intel.com/research/exploratory/digital_home
57. Nam YH, Halm Z, Chee YJ, Park KS. Development of remote diagnosis system integrating digital telemetry for medicine. In *International Conference IEEE-EMBS* 1998; 1170–1173.
58. Coyle G, Boydell L, Brown L. Home telecare for the elderly. *Journal of Telemedicine and Telecare* 1995; **1**: 183–184.
59. Celler BG, Hesketh T, Earnshaw W, Ilsar E. An instrumentation system for the remote monitoring of changes in functional health status of the elderly. In *International Conference IEEE-EMBS* 1994; 908–909.
60. Johnson P, Andrews DC. Remote continuous physiological monitoring in the home. *Journal of Telemed Telecare*, 1996.
61. Bauer P, Sichitiu M, Istepanian R, Premaratne K. The mobile patient: wireless distributed sensor networks for patient monitoring and care. In *IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, 2000; 17–21.
62. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer Networks* 2002; **38**: 393–422.
63. Puccinelli D, Haenggi M. Wireless sensor networks: applications and challenges of ubiquitous sensing. *IEEE CIRCUITS AND SYSTEMS*, 3rd Quarter 2005; 19–29.
64. Shnayder V, Chen BR, Lorincz K, Fulford-Jones T, Welsh M. Sensor networks for medical care. Technical Report TR-08-05, Harvard University, 2005.
65. Ferraiolo DF, Kuhn DR, Chandramouli R. *Role-Based Access Control*. Artech House: Norwood, MA, 2003.
66. Wander AS, Gura N, Eberle H, Gupta V, Chang Shantz S. Energy analysis of public-key cryptography for wireless sensor networks. In *IEEE International Conference on Pervasive Computing and Communication*, 2005.
67. Buschmann C, Fischer S, Koberstein J, Luttenberger N. Towards information centric application development for wireless sensor networks. In *System Support for Ubiquitous Computing Workshop (UbiSys) at the Sixth Annual Conference on Ubiquitous Computing (UbiComp 2004)*, September 2004.
68. Fok C-L, Roman G-C, Lu C. Rapid development and flexible deployment of adaptive wireless sensor network applications. In *24th International Conference on Distributed Computing Systems (ICDCS'05)*, June 2005; 653–662.
69. Wood AD, Stankovic JA, Son SH. JAM: a jammed-area mapping service for sensor networks. In *Real-Time Systems Symposium (RTSS)*, 2003.

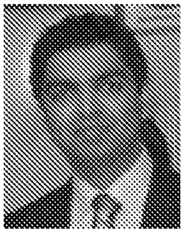
Authors' Biographies



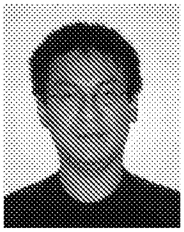
Eric Sabbah is a doctoral student in Computer Science at the State University of New York (SUNY) at Binghamton. He received his B.S. degree in Computational Mathematics from the City University of New York's (CUNY) Brooklyn College, and his M.S. degree from New York University (NYU). His research interests include wireless computing, sensor networks, and network security.

Kyoung-Don Kang is an Assistant Professor in the Department of Computer Science at the State University of New York at Binghamton. He received his Ph.D. from the University of Virginia in 2003. His research interest includes real-time data services including e-commerce and traffic/weather information service, wireless sensor networks, and wireless network security.

Nael Abu-Ghazaleh is an Associate Professor in the Computer Science Department at the State University of New York, Binghamton. He received his Ph.D. in Computer Engineering from the University of Cincinnati in 1997. His research interests are in wireless networks, sensor networks, and parallel/distributed systems.



Adnan Majeed is currently pursuing his Ph.D. in Computer Sciences from the State University of New York at Binghamton. He completed his Bachelors of Science in Computer System Engineering from GIK Institute in Pakistan. His research interests are in wireless mesh networks and sensor network security.



Ke Liu is a Ph.D. candidate in Computer Science at SUNY Binghamton. He received his B.S. degree from Fudan University, Shanghai, Chain, at 2000, and his M.S. from SUNY Binghamton, 2005, both in Computer Science. His research interests include the routing protocols and security for wireless sensor networks, WPAN MAC protocols such as UWB, Zigbee.

DOI: 10.1002/wcm