An Application-Driven Perspective on Wireless Sensor Network Security*

Eric Sabbah, Adnan Majeed, Kyoung-Don Kang, Ke Liu, and Nael Abu-Ghazaleh
Department of Computer Science
State University of New York at Bighamton
{esabbah,adnan,kang,kliu,nael}@cs.binghamton.edu

ABSTRACT

Wireless sensor networks (WSNs) have recently attracted a lot of interest due to the 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 unique nature as an application and a network, and due to their limited capabilities. 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 an effective solution for WSNs must be sensitive to the application and infrastructure. We propose 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, the WSN infrastructure, the application, protocols and system software, as well the accessibility and the observability of the WSN. To reduce the vulnerability, we argue that WSN design must balance traditional objectives such as energy efficiency, cost, and application level performance with security to a degree proportional to the attacker's motivation. We illustrate this argument via two example applications.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless Communication; C.2.0 [**General**]: Security and Protection

Keywords

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 especially in applications where human observation or traditional sensors would be undesirable, inefficient, expensive, or dangerous.

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. To address the problem, a lot of research work including (but are not limited to) [27, 13, 19, 17, 16, 21, 28, 35, 7, 6, 31, 8, 5, 29] have recently been done to make WSNs more secure. Although their contributions are invaluable, most existing work do not provide any guidelines to help application designers or developers to choose appropriate security mechanisms for their applications (or help them specify the required new security schemes for the 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 an application-specific context. It is known that security is not only a technical problem. For example, the integral relationships between economics and security [24]/privacy [25] and the implications on system design in traditional systems are accepted. 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 towards defining reasonable WSN security scenarios and enabling WSN security research with grounded and realistic assumptions.

Most existing WSN security work consider an abstract sensor network and select assumptions and organizations that are decoupled from application details. Much of the other work in WSN security tend to consider one or more theoretic 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.[1] We argue that this existing work can serve as mechanisms in a security policy that is driven by the security context. We illustrate this argument by applying it to two canonical WSN applications with diverse security vulnerabilities and motivations for attacks. (We can only present two due to space considerations.) Sections 4 through 5 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 6 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 influenced directly by the WSN application. As a result, 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: (1) Attacker Motivation; and (2) Opportunity and Infrastructure.

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 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 activity. The emphasis for these types of applications is on confidentiality and privacy preserving measures.

- **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 of interest to the attacker, who instead 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 attacks allowing tampering with the data 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 sensor that does 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 acts based on bad or manipulated data. If the failure is detectable, the observer may employ backup monitoring mechanisms or ignore 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 the *motivation* of an attacker to attack 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; often human estimates are used for utility in similar contexts. Finally, some attacks such as vandalism may occur that have no tangible benefit to attackers.

2.2 Vulnerabilities and Opportunities

There are a number of factors that are unique to WSN infrastructure that present some vulnerabilities to attackers. From an attacker's perspective, the opportunity is essentially a measure of the vulnerability (or the difficulty of attacking it). The opportunity, when combined with the benefit, can be used to define the cost-benefit ratio among the available attacks. 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 that sensors 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, or 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, 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 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 [10]. In many applications, WSNs heavily rely on coordinated 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

---

[1]Note that we claim our work to be neither a complete nor comprehensive survey. There have been other surveys regarding sensor network security including [33, 14, 26]. However, they tend to focus on outlining the insecurity of specific existing protocols that were not designed to be secure.

that are not present 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[2], the observability of deployment and communications, and the access of the attacker to the sensor field. Beyond mere detection of the presence of the network, detecting the structure of the network incurs more directed attacks, e.g., targeted for the base station or nearby nodes.

2.3 Implications on WSN Design

There are a number of design choices for WSNs in terms of the 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 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 cost or performance to reduce vulnerabilities to acceptable levels. At the physical level, this can translate to purchasing more expensive and secure sensors, or purchasing more sensors to introduce redundancy or tolerance against a possible attack. 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 and secure 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 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 because in-network processing cannot occur.

---

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

WSN security has received considerable attention and there exists a number of identified attacks and solutions to them; we review these in more detail in Section 3. We contend that the attacker motivation and the vulnerability which are both a function of the application and sensor field should be considered when making effective and secure design decisions.

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 operation and capabilities 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 approach to WSN security.

3.1 Supporting Confidentiality, Integrity, and Authenticity

Data can be encrypted to support the 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 MAC (Message Authentication Code) 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 [27] and TinySec [13] can support message confidentiality, integrity, and authenticity in WSNs. μTESLA [27] can support authenticated broadcast in which only the base station can securely broadcast legitimate messages. Notably, most existing work including [27, 13] are based on the secret key system in which the sender and receiver share a 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 [19] takes several minutes to run in the worst case. Also, end-to-end encryption is often ineffective due to a strong need for in-network data processing prevalent in WSNs. 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 pair-wise 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 [9] did one of the first work considering the key distribution problem in sensor networks. Since sensors are often deployed randomly, it is impossible to pre-define 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 [5] extends [9] in three ways. (Their basic scheme is similar to [9].) 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 [34] propose a novel key management protocol called LEAP (Localized Encryption and Authentication Protocol) 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, e.g. 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, i.e., 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, e.g. 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 have been done for localization in WSNs [11, 32, 30, 2, 22, 4, 23, 20]. However, these approaches are de-signed without considering security. Thus, a compromised or malicious node can claim virtually any location.

Lazos et al [15] 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 [29] in which a sensor node needs to send its location claim to a verifier that subsequently sends back 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, e.g., due to overloads or packet losses. As a result, honest nodes could be unnecessarily invalidated. We have developed a different approach [1] 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 [29]. 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 [17]. 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[3], 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 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 [16]. 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, Intru-

---

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

sion 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 [3]. 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 [6, 12, 1]

INSENS (Intrusion-tolerant routing protocol for wireless SEsor NetworkS) [6] 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 [12] is a robust routing protocol applicable to WSNs with a tree topology. In this approach, 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 [1] propose an resilient, multi-path 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 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.

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 [28] 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 [31] 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 [3] 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 [35] 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 [14]. 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 [35]. This inevitably leads to the 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 dif-

ficult for the adversary to analyze the traffic patterns and thus discern which of the nodes are in this category. Deng et al [7] 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).

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 towards 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.

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 two sample 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, their use for habitat monitoring is therefore 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, something called the "observer effect". The sensor networks deployed to monitor the Great Duck Island and the James reserve [18] 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 no one would 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 be 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 habitat monitoring WSN 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, e.g., 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 [18] would not generally be too concerned about the confidentiality of data, e.g., 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 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 [27, 13]. 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 section 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, MAC (Medium Access Control) address, and cryptographic key can be used to verify, e.g., 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 is important to maintain the correctness of those queries such as min or max that are more vulnerable to false data injection [31]. Domain specific knowledge, e.g., observer effects, can also be exploited to further improve the statistical defense.

5. 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 the win of 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) guarantee confidentiality, integrity and authenticity; (ii) correctly route the 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, the attacks that can be mounted on such a network are all over the spectrum. These include (but are not limited to) the following.

- **Loss of Confidentiality, Integrity or Authenticity and Injection of False Data:** An adversary may be able to extract the transmitted data and make tactical decisions accordingly by compromising a few key nodes. 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, e.g., to falsify the enemy troops' location.

- **Attacks on Routing and DoS Attack:** 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.

- **Attacks on Localization:** An adversary can devise mechanisms to 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.

Due to the large benefit of a successful attack as discussed above, an adversary can be willing to spend a lot of resources to render the WSN useless. Consequently, strong security mechanisms have to be built into such a system to withstand such attacks. Notably, a military surveillance operation can be either short-term or long-term depending on operational purposes and battlefield status. If a WSN is deployed for a short-term usage, the energy available per operation greatly increases. This additional energy can be used to provide the additional security required by such networks. However, for a long-term usage, energy becomes a major problem, because minimizing energy while providing the discussed security becomes a onerous task.

6. CONCLUSIONS AND FUTURE WORK

Wireless sensor networks 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. This work is an initial step to achieve the goal. 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 also 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.

7. REFERENCES

[1] N. Abu-Ghazaleh, K. D. Kang, and K. Liu. 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)*, Oct. 2005.

[2] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *Proceedings of the IEEE INFOCOM '00*, March 2000.

[3] C. Baslie, M. Gupta, Z. Kalbarczyk, and R. K. Iyer. 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.

[4] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less Low-Cost Outdoor Localization for Very Small Devices. *IEEE Personal Communication*, 2000.

[5] H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. *IEEE Symposium on Security and Privacy*, May 2003.

[6] J. Deng, R. Han, and S. Mishra. 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.

[7] J. Deng, R. Han, and S. Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. Technical report, CU-CS-987-04, 2004.

[8] L. Eschenauer and V. D. Gligor. A Key-Management Scheme for Distributed Sensor Networks. In *ACM Conference on Computer and Communications Security*, 2002.

[9] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *the 9th ACM conference on Computer and Communications Security*, 2002.

[10] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. Next century challenges: Scalable coordination in sensor networks. In *Mobile Computing and Networking*, pages 263–270, 1999.

[11] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher. Range-Free Localization Schemes for Large Scale Sensor Networks. In *MobiCom'03*, 2003.

[12] C. Karlof, Y. Li, and J. Polastre. ARRIVE: Algorithm for Robust Routing in Volatile Environments. Technical Report UCB//CSD-03-1233, University of California at Berkeley, 2003.

[13] C. Karlof, N. Sastry, and D. Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. In *ACM SenSys*, 2004.

[14] C. Karlof and D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Elsevier's AdHoc Networks Journal*, 1(2-3), 2003.

[15] L. Lazos and R. Poovendran. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In *the ACM Workshop on Wireless Security*, 2003.

[16] D. Liu, P. Ning, and W. Du. Attack-Resistant Location Estimation in Sensor Networks. In *IPSN '05*, April 2005.

[17] D. Liu, P. Ning, and W. Du. Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks. In *The 25th International Conference on Distributed Computing Systems*, June 2005.

[18] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson. Wireless Sensor Networks for Habitat Monitoring. In *WSNA*, 2002.

[19] D. J. Malan, M. Welsh, and M. Smith. A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography. In *IEEE SECON*, 2004.

[20] R. Nagpal. Organizing a Global Coordinate System from Local Information on an Amorphous Computer. Technical Report A.I. Memo 1666, MIT A.I. Laboratory, August 1999.

[21] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis and Defenses. In *IPSN '04*, 2004.

[22] D. Niculescu and B. Nath. Ad Hoc Positioning System (APS) Using AoA. In *INFOCOM '03*, 2003.

[23] D. Niculescu and B. Nath. DV Based Positioning in Ad hoc Networks. *Journal of Telecommunication Systems*, 2003.

[24] A. M. Odlyzko. Economics, psychology, and sociology of security, 2003.

[25] A. M. Odlyzko. Privacy, economics, and price discrimination on the internet. In *ACM ICEC2003: Fifth International Conference on Electronic Commerce*, pages 355–366, 2003.

[26] A. Perrig, J. Stankovic, and D. Wagner. Security in Wireless Sensor Networks. *Communications of the ACM*, 47(6), June 2004.

[27] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar. SPINS: Security Protocols for Sensor Networks. In *MobiCom*, 2001.

[28] B. Przydatek, D. Song, and A. Perrig. SIA: Secure Information Aggregation in Sensor Networks. In *Proceedings of ACM Sen-Sys*, 2003.

[29] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In *the ACM workshop on Wireless Security*, 2003.

[30] A. Savvides, C. C. Han, and M. B. Srivastava. Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors. In *MOBICOM '01*, July 2001.

[31] D. Wagner. Resilient Aggregation in Sensor Networks. *SASN'04*, Oct. 2004.

[32] B. H. Wellenhoff, H. Lichtenegger, and J. Collins. *GlobalPositions System: Theory and Practice, Fourth Edition*. Springer Verlag, 1997.

[33] A. Wood and J. Stankovic. Denial of Service in Sensor Networks. *IEEE Computer*, pages 54–62, Sept. 2002.

[34] S. Zhu, S. Setia, and S. Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In *the 10th ACM Conference on Computer and Communications Security (CCS '03)*, 2003.

[35] S. Zhu, S. Setia, S. Jajodia, and P. Ning. An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data In Sensor Networks. In *IEEE Symposium on Security and Privacy*, 2004.