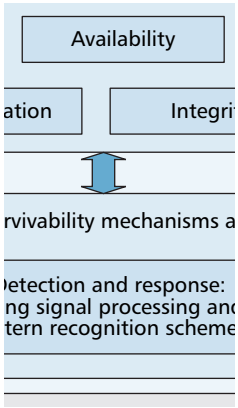
A DESIGN FOR SECURE AND SURVIVABLE WIRELESS SENSOR NETWORKS

YI QIAN AND KEJIE LU, UNIVERSITY OF PUERTO RICO AT MAYAGÜEZ
DAVID TIPPER, UNIVERSITY OF PITTSBURGH



The authors present a study of the design of secure and survivable wireless sensor networks (WSN) that has yet to be addressed in the literature. Their goal is to develop a framework that provides the security and survivability features that are crucial to applications in a WSN

ABSTRACT

In this article, we present a study of the design of secure and survivable wireless sensor networks (WSN) that has yet to be addressed in the literature. Our goal is to develop a framework that provides the security and survivability features that are crucial to applications in a WSN, because WSNs are vulnerable to physical and network-based security attacks, accidents, and failures. To achieve such a goal, we first examine the security and survivability requirements. We then propose a security and survivability architecture in a WSN with heterogeneous sensor nodes. To understand the interactions between survivability and security, we also design and analyze a key management scheme. The results of the experiment show that a good design can improve both security and survivability of a WSN; however, in some situations, there is a trade off between security and survivability.

INTRODUCTION

A wireless sensor network (WSN) consists of battery-operated sensor devices with computing, data processing, and communicating components. In a WSN, the sensor nodes can be deployed in controlled environments, such as factories, homes, or hospitals. They also can be deployed in uncontrolled environments, such as disaster or hostile areas or in a particular battlefield, where monitoring and surveillance is crucial. Clearly, *security* in a WSN is extremely important for both controlled environments (e.g., health-care, automation in transportation, etc.) and uncontrolled and hostile environments (e.g., environmental monitoring, military command and control, battlefield monitoring, etc.). Moreover, the majority of the WSN applications should be run continuously and reliably without interruption. Hence, *survivability* also should be taken into account in developing a WSN.

In the design of secure and survivable WSNs, survivability implies that networks should have the capability to operate under node failures and attacks. On the other hand, security encompasses the aspects of confidentiality, authentication, and integrity of the application information. Obviously, security and survivability in a WSN face many common challenges — ranging from the wireless nature of communications, resource limitations on sensor nodes, very large and dense networks, and unknown network topology prior to deployment — to the high risk of physical attacks on unattended sensors. More importantly, these two factors may couple with each other. With the popularity of the WSN as an emerging wireless technology, there is a need to study the coupling between survivability and security and a need to create design strategies consistent with both sets of requirements for a WSN.

In this article, we present a comprehensive study of security and survivability for WSN. Our goal is to develop a framework for a WSN that provides security and survivability measures that are available for critical services in spite of physical and network-based security attacks, accidents, or failures. To achieve this goal, we first study the requirements of both security and survivability. We then present a general architecture for a WSN with heterogeneous sensor nodes. With the architecture, we identify metrics that quantify the performance of a WSN. We also address the issues of the interaction between security and survivability for a WSN. For instance, node failures or coordinated physical/cyber attacks on sensor nodes result in security breaches and impact the WSN performance simultaneously. Similarly, a security attack compromising network components (e.g., sensor node or cluster head) could affect the network survivability techniques. On the other hand, a survivability strategy for restoring the performance very likely could be inconsistent with the security requirements. As a case study, we investigate a distributed key management scheme for a WSN with heterogeneous sensor nodes.

The remainder of this article is organized as follows. We first discuss the requirements of

1536-1284/07/$20.00 © 2007 IEEE

security and survivability for a WSN. We then present a detailed architecture for WSN survivability and security design. After that we present the study to understand the interaction between survivability and security for a WSN. In the last section, we give a summary of this study and future work.

Security and Survivability Requirements in WSNs

Security Requirements for WSNs

In this section, we analyze the security requirements that constitute the fundamental objectives on which every sensor application is based and to which every application should adhere to guarantee an appropriate level of security [1].

Confidentiality: This requirement is to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in the environment of the sensors to protect information from disclosure when traveling between the sensor nodes of the network or between the sensors and the base station, because an adversary having the appropriate equipment can eavesdrop on the communication. If we consider eavesdropping to be a network-level threat, then a local-level threat could be a compromised node that an adversary has in his possession. Compromised nodes are a big threat to the confidentiality objective, because the adversary could steal critical data stored on nodes such as cryptographic keys that are used to encrypt the communication.

Authentication: As in conventional systems, authentication techniques verify the identity of the participants in a communication, distinguishing in this way legitimate users from intruders. In the case of sensor networks, it is essential for each sensor node and base station to have the capability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a situation occurs and false data are supplied to the network, then the behavior of the network cannot be predicted, and most of the time, the outcome will be unexpected.

Integrity: This refers to the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems, because the consequences of using inaccurate information can be disastrous. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications, such as environmental and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Therefore, there is an urgent need to ensure that information is traveling from one end to the other without being intercepted and modified in the process.

Secure management: Management is required in every system that is constituted from multiple components and handles sensitive information. In the case of a WSN, we require secure management on the base station level. Because sensor node communication ends at the base station, issues such as key distribution to sensor nodes to establish encryption and routing information require secure management. Furthermore, clustering requires secure management as well, because each group of nodes may include a large number of nodes that must be authenticated with each other and exchange data in a secure manner.

The security requirements that should be met to better protect a WSN from adversaries: confidentiality, authentication, integrity, and secure management are discussed. The same security objectives that exist in conventional systems are required for sensor networks as well. The difference is that the security objectives here are addressed in the context of sensor node characteristics such as their architecture and limitations. Although many of these security problems have been studied in distributed systems, as well as ad hoc networking, in general, the solutions proposed are too computationally demanding to work for sensors. Security aspects of a WSN have received little attention compared to its other aspects.

Survivability Requirements for WSNs

Reliability: In addition to the security concerns, the *reliability* of the network is also of special interest because many applications require the WSN to operate in uncontrolled environments. In such cases, some wireless sensor nodes may fail, thus affecting the operation of the whole network. Reliability is the capability to keep the functionality of the WSN even if some sensor nodes fail.

Availability: *Availability* ensures that services and information can be accessed at the time that they are required. In a WSN, there are many risks that could result in loss of availability, such as sensor node capturing and denial of service attacks. Lack of availability may affect the operation of many critical real-time applications. Therefore, it is critical to ensure resilience to attacks that target the availability of the system and to find ways to fill the gap created by the capturing or disablement of a specific node by assigning its duties to other nodes in the network. The protocols employed by the WSN must be robust enough to mitigate the effects of outages by providing alternate routes.

Energy efficiency: A WSN consists of battery-operated sensor devices with computing, data processing, and communicating components. Energy conservation is a critical issue in a WSN, because batteries are the only limited-life energy source available to power the sensor nodes. Apparently, the battery life affects the reliability and availability of the WSN. Protocols, including security mechanisms designed for the WSN, should be energy aware and efficient.

Evidently, there is a coupling between security, reliability, availability, and energy efficiency of a WSN. This motivates us to study the interactions of security and survivability of WSNs, so that we can effectively analyze and design secure and survivable WSNs.

Although many of these security problems have been studied in distributed systems, as well as ad hoc networking, in general, the solutions proposed are too computationally demanding to work for sensors. Security aspects of a WSN have received little attention compared to its other aspects.

The reliability of the network is also of special interest because many applications require the WSN to be operating in un controlled environments. In such cases, some wireless sensor nodes may fail, thus affecting the operation of the whole network.

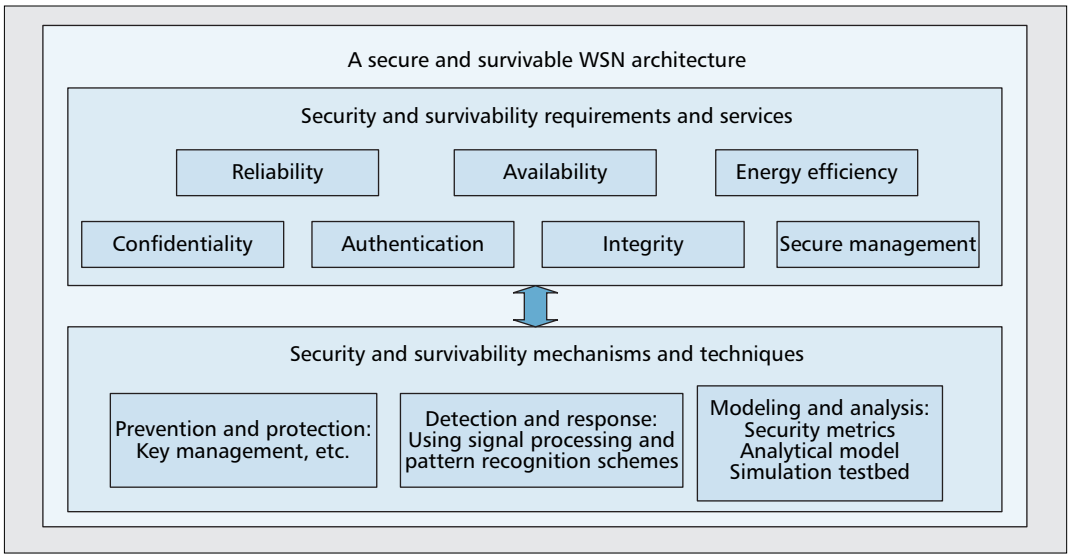


Figure 1. *A secure and survivable WSN architecture.*

A Secure and Survivable WSN Architecture

The Architecture

As the first step of a secure and survivable WSN design, we present a WSN security architecture with heterogeneous sensor nodes. In a WSN, ensuring the physical security of wireless links is virtually impossible because of the broadcast nature of and resource limitation on sensor nodes and the uncontrolled environments where they are left unattended. Consequently, security attacks on information flow can be widespread, for example, passive interception of data transmission, active injection of traffic, and overloading the network with garbage packets. Modification of information is possible because of the nature of the wireless channel and the uncontrolled node environments. An opponent can make use of these natural impairments to modify information and also render the information unavailable. Security requirements in a WSN are similar to those of wireless ad hoc networks due to the similarities of the two types of networks [2]. Thus, WSNs also have the general security requirements of confidentiality, authentication, integrity, and security management.

The reliability of the network is also of special interest because many applications require the WSN to be operating in uncontrolled environments. In such cases, some wireless sensor nodes may fail, thus affecting the operation of the whole network. A WSN consists of battery-operated sensor devices with computing, data processing, and communicating components. Many early studies assume that these sensor nodes are homogeneous, which means that the sensor nodes have the same capabilities. Recently, however, heterogeneous sensor networks are gaining more attention [3–5]. The heterogeneity in terms of transmission range for wireless sensor nodes becomes a practical solution. Recent studies also show that such heterogeneity can increase the network performance and network lifetime without significantly increasing the cost [3–5].

To enhance security and survivability, we propose a general framework for a WSN with heterogeneous sensor nodes. The individual security mechanism in a WSN has been dealt with to a certain extent, but research and development of security and survivability architectures has been less extensive. To provide secure and survivable communications for a WSN, all the aspects of security requirements and services must be met and provided. Up till now, most of the existing security schemes for distributed WSNs assume that the sensor nodes are homogeneous with the same capabilities for each sensor network. Therefore, it is of significance to investigate how to design a suitable secure architecture for heterogeneous WSNs. Consequently, it is also important to address the reliability issue in the design of secure and survivable architectures for heterogeneous WSNs using the modeling and analysis techniques.

Figure 1 illustrates the proposed architecture for a WSN. In Fig. 1, the prevention and protection schemes must be designed to achieve the WSN security and survivability requirements and provide the secure and survivable services; the detection and response schemes must be designed to passively protect the WSN; the modeling and analysis schemes must be developed to design the secure and survivable WSN more effectively. Key management is one of the most important aspects to design a prevention and protection mechanism for a WSN. Advanced signal processing and pattern recognition schemes can be used to design detection and response mechanisms for WSNs. Modeling and analysis techniques include identifying security and survivability metrics and building an analytical model, simulation, or testbed. The security and survivability requirements and services, combined with the security and survivability mechanisms and techniques, form a general secure and survivable WSN architecture.

In the proposed framework for distributed peer-to-peer based WSNs, we consider that there are I classes of sensor nodes in the network, with Class 1 the least powerful nodes, and

Class I the most powerful nodes, in terms of communication range, node processing capability, and energy level. Particularly, in terms of communication range, we assume a bidirectional link between any two nodes. Let r_i denote the communication range of Class i nodes; we always have $r_m < r_n$ if $m < n$. Therefore, if a Class m node is within the range of a direct communication link of a Class n node, the Class m node might require multiple links to reach the Class n node if $m < n$. The heterogeneity of the sensor nodes are distributed in the WSN, with p_i the percentage of the Class i nodes, and $p_1 + p_2 + \ldots \ldots + p_I = 1$. Here it is important to notice the fundamental difference between the heterogeneous WSN assumed in this article and the hierarchical WSN in [6, 7]. In the hierarchical WSN, the base stations (or cluster supervisors) are centralized nodes, and more importantly, they are acting like key distribution centers. By contrast, in the heterogeneous WSN, except that the higher class nodes are more powerful in terms communication range, node capability, and energy level, the communications between all different classes of nodes are still peer-to-peer and distributed.

The Security and Survivability Metrics

The security requirements and services can be described by the following metrics: scalability, efficiency, resilience, and reliability. *Scalability* is the ability to support a large number of wireless sensor nodes in the network. The security mechanisms must support a large network and must be flexible against a substantial increase in the size of the network even after deployment. *Efficiency* is the consideration of storage, processing, and communication limitations on sensor nodes. *Resilience* is about the resistance against node capture. Compromise of security credentials, which are stored on a sensor node or exchanged over radio links, should not reveal information about security of any other links in the WSN. Higher resilience means a lower number of compromised links. *Reliability* is the capability to keep the functionality of the WSN even if some of the sensor nodes fail. The survivability concerns can be provided with the design goals of scalability, efficiency, key connectivity, resilience, and reliability. *Key connectivity* is the probability that two or more sensor nodes store the same key or keying material. Sufficient key connectivity must be provided for a WSN to perform its intended functionality.

Toward Secure and Survivable WSN

To understand the interaction between survivability and security of our WSN architecture with heterogeneous sensor nodes, we conduct a case study for the key management scheme. Our study shows that the WSN can achieve higher key connectivity and higher resilience with our proposed key management scheme, with a small percentage of heterogeneous nodes that have reasonable storage, processing, and communication capabilities. We also can show the trade off between the reliability and the security in some examples.

A Key Management Study

Key management is one of the most important prevention and protection schemes for security mechanisms of a WSN. To provide secure communications for the WSN, all the messages should be encrypted and authenticated. Consequently, security solutions for such applications depend on the existence of strong and efficient key distribution mechanisms for uncontrolled environments of the WSN. We illustrate how to design an effective key management framework under the general heterogeneous WSN architecture. It also is important to address the reliability issue in the design of a key management scheme. Energy conservation is a critical issue in a WSN because batteries are the only limited-life energy source to power the sensor nodes. The key management schemes designed for WSNs should be energy aware and efficient.

Obviously, using a single shared key in the whole WSN is not a good idea because an adversary can easily obtain the key. Therefore, as a fundamental security service, pairwise key establishment is used, which can enable the sensor nodes to communicate securely with each other using cryptographic techniques. However, due to resource constraints on sensor nodes, it is not feasible for sensors to use traditional pairwise, key establishment techniques, such as public key cryptography and key distribution centers [3, 8]. Instead, sensor nodes can use pre-distributed keys directly or use keying materials to dynamically generate pairwise keys. In such a case, the main challenge is to find an efficient way of distributing keys and keying materials to sensor nodes prior to deployment.

The key generation in heterogeneous distributed WSNs here is based on our previous work [3, 4]. It is similar to the key-pool based random key distribution [9] and the polynomial-based key pre-distribution protocol [10] and is inspired by the approaches of [11]. We consider that there are three steps in the framework to establish pairwise keys between the sensor nodes: initialization, direct key set up, and path key set up. The initialization step is performed to initialize the sensors by distributing polynomial shares to them, with the consideration of the heterogeneity of the sensor nodes. The direct key set-up step is for any two nodes trying to establish a pairwise key, in which they always first attempt to do so through direct key establishment. If the second step is successful, there is no need to start the third step. Otherwise, these sensor nodes may start the path key set-up step, trying to establish a pairwise key with the help of other sensors. During the key distribution procedure, a number of factors must be considered, including the probability that adjacent nodes can share a common key, the resilience of the network when it is under attack, and importantly, the nature of the heterogeneity.

Understanding the Interaction between Survivability and Security

Based on the discussion in the previous section, we can see that our new key generation scheme is essentially different from most existing

During the key distribution procedure, a number of factors must be considered, including the probability that adjacent nodes can share a common key, the resilience of the network when it is under attack, and importantly, the nature of the heterogeneity.

According to the definition, key connectivity is the probability that two or more sensor nodes store the same key. Obviously, enough key connectivity must be provided for a WSN to perform its intended functionality.

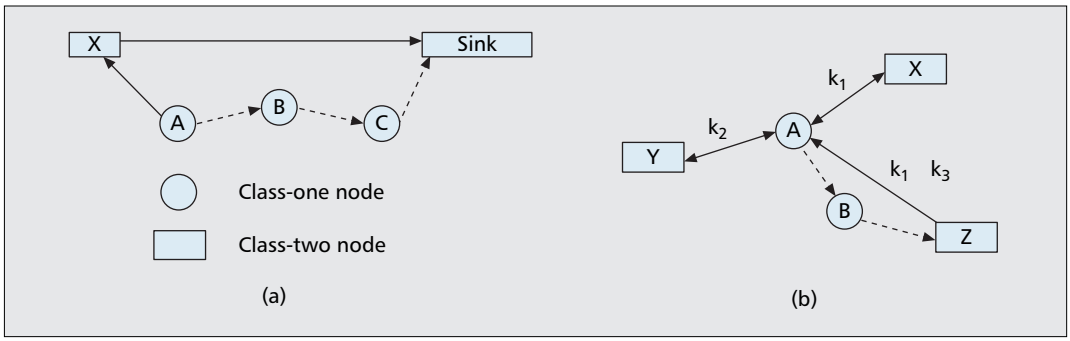


Figure 2. *Examples for a) the WSN; b) the proposed key management scheme.*

schemes in that the heterogeneity features now can be taken into account. To illustrate the advantages of the new scheme, we consider a typical heterogeneous WSN that is established to collect data in a distributed scenario. In this scenario, a sensor node submits its observation to a sink node (or sink nodes, depending on the configuration of the network) through the sensor network in a hop-by-hop manner, as shown in Fig. 2a, in which there are two classes of sensor nodes, in addition to the sink node.

Since the high-class nodes have a larger transmission range, it is natural that a low-class node tends to utilize the link between itself and a high-class node to submit the observations. For example, in Fig. 2a, Class-One, node A tends to use the path, A-X-Sink, to submit its report, instead of passing the message by all Class-One nodes, A-B-C-Sink. Clearly, a high-class node is more likely be chosen as the next-hop neighbor of nearby low-class nodes to forward data. Consequently, in this heterogeneous sensor network, the connectivity between a low-class node and a high-class node is more important than the connectivity between two low-class nodes.

We now design a special key management scheme within the new framework for the previous scenario. Specifically, we consider that there are two classes of the heterogeneous sensor nodes (i.e., $I = 2$). To simplify the discussion, we also assume that there is only one group, denoted as group 0, in the network.

The special key management scheme is a key-pool based key distribution scheme. In this scheme, we denote C_1 as the class of the less powerful sensor nodes and denote C_2 as the class of the more powerful sensor nodes. We consider that a C_2 node X is in the *neighborhood of* a C_1 node A if A can directly receive the message from X. Because the transmission range of A is less than the transmission range of X, A might be required to send messages to B through a multihop path. We define that a C_1 node is *connected to the network* if it *shares at least one key with C_2 nodes in its neighborhood*. We then define the key connectivity as the probability that a C_1 node is connected to the network. For simplicity, we consider only the direct key set up between a C_1 and adjacent C_2 nodes.

An example of this scheme is illustrated in Fig. 2b, where node A is a C_1 node and node X, Y, and Z are C_2 nodes. In this example, nodes X, Y, and Z are the only C_2 neighbor nodes of node A. In addition, node A shares key K_1 with node X, K_2 with node Y, and K_1 and K_3 with node Z, respectively. In this example, node A is connected to the network through three different keys: K_1, K_2, and K_3. In such a case, if node A wants to submit new information to the sink node, first it can randomly select a key from K1 to K_3; then it can randomly select a neighbor node that shares the same key with it. For example, in Fig. 2b, if K_1 is chosen as the key, nodes X and Z can be randomly selected. In this manner, we can see that the communication is more resilient, while the connectivity also can be maintained.

To understand the behavior of the previous key management scheme, we conducted an extensive quantitative study to evaluate its performance, in terms of key connectivity, reliability, and resilience. In our experiments, we consider a small area of the WSN that consists of 100 C_1 nodes and a number of C_2 nodes, denoted as N_2. We also assume that the size of the key pool is 20,000, and the number of keys in any C_2 node is fixed at 1000.

Reliability of the New Schemes: Key Connectivity of the New Schemes in Normal Conditions — According to the definition, *key connectivity* is the probability that two or more sensor nodes store the same key. Obviously, enough key connectivity must be provided for a WSN to perform its intended functionality. Figure 3a shows the connectivity of the proposed scheme versus the number of keys in a C_1 node with a different number of C_2 nodes. First, we can observe that the connectivity can increase with the increase of the number of keys. For a fixed number of keys in each C_1 node, we can see that a small increase of the number of C_2 nodes can significantly increase the connectivity, especially when the number of keys in a C_1 node is small to medium. From another perspective, we can see that to achieve a specific connectivity, the number of keys that must be stored in each C_1 node can be decreased with the increase of N_2. For instance, if the connectivity is 0.99, about 90 keys are required for $N_2 = 1$, about 45 keys are required for $N_2 = 2$, and about 30 keys are needed for $N_2 = 3$.

To highlight the impact of the number of C_2 nodes, we demonstrate in Fig. 3b the probability distribution of the number of shared keys with different N_2. In this example, we assume the number of keys in each C_1 node is 50. We can observe that with the increase of N_2, the shape of the distribution tends to shift to the right,

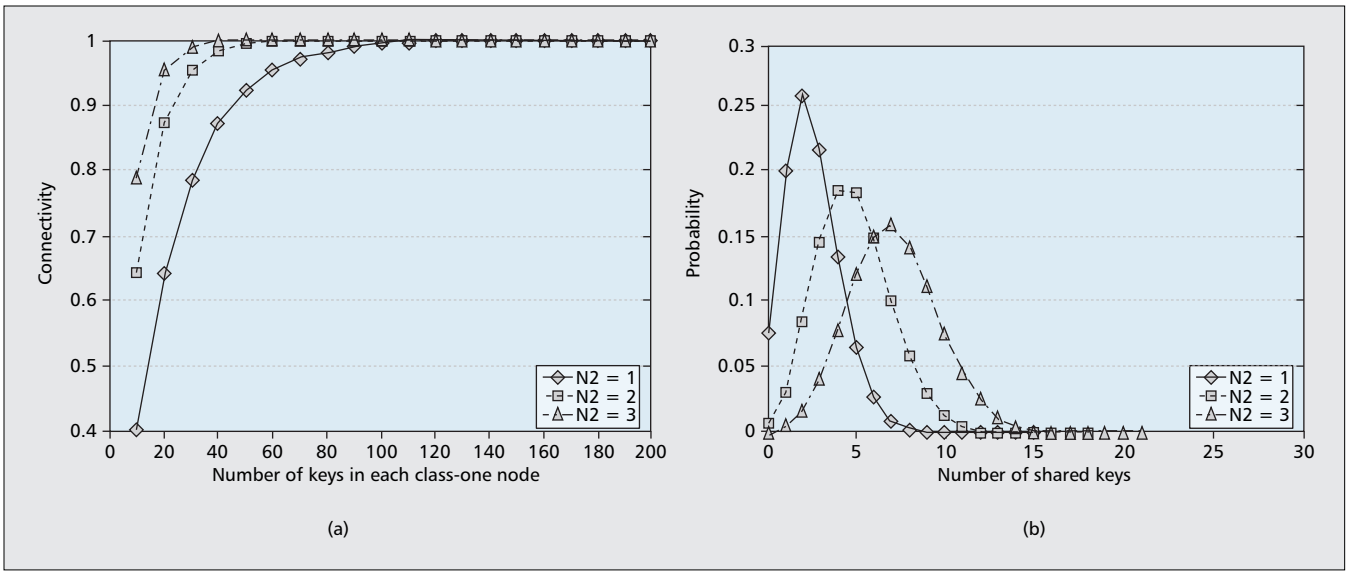


Figure 3. *Connectivity of the key-pool based scheme in normal conditions: a) impact of number of keyes in a C_1 node; b) distribution of shared keys (50 keys per C_1 node).*

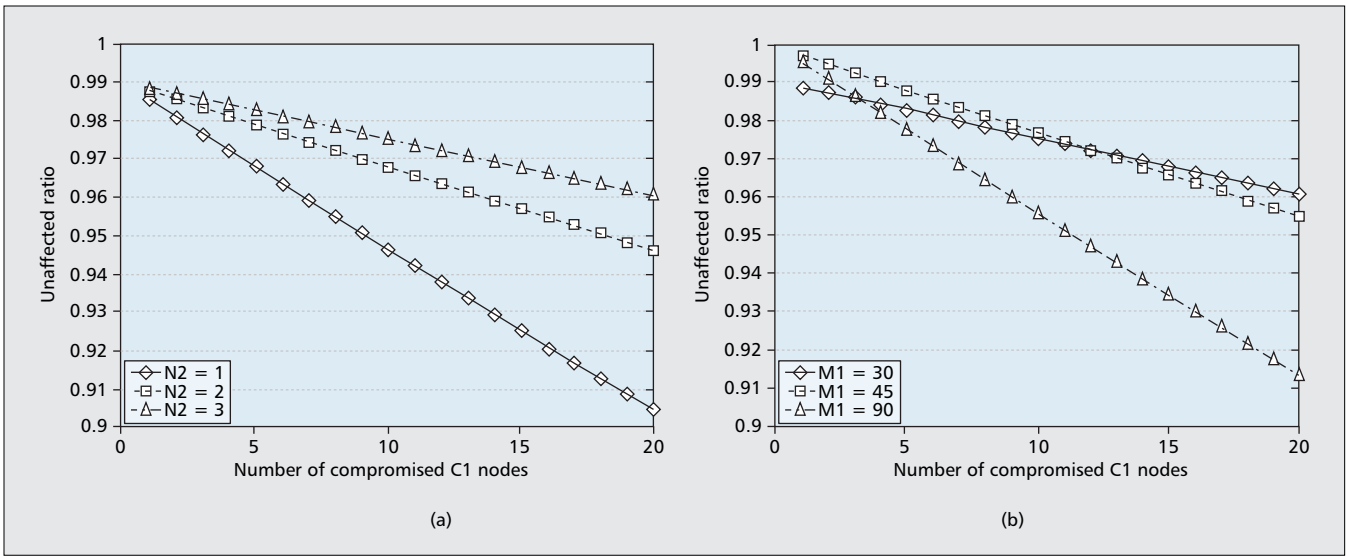


Figure 4. *Resilience of the key management scheme in attack conditions.*

which implies that a C_1 node can share more keys with neighboring C_2 nodes; and with the increasing of the shared keys, the network becomes more reliable.

Resilience of the New Schemes: Key Connectivity of the New Schemes in Attack Conditions — To evaluate the resilience of the new schemes, we study the performance of the sensor network when some C_1 nodes are compromised. Here we assume that C_2 nodes are more tamper resistant. In Fig. 4a we consider the scenario in which the keys per C_1 node are selected in a manner such that the network connectivity is 99 percent under normal conditions. We also assume that the compromised C_1 nodes cannot be detected. In such a scenario, the data transmission from an unaffected C_1 node may be eavesdropped on by a nearby compromised node. Therefore, it is important to study the percentage of communications that are not affected. From Fig. 2 we can see that with our scheme, a C_1 node can still transmit data securely to C_2 nodes even if some of the keys are compromised. For example, if K_1 is the only key that is compromised, we can see that node A still has a 66 percent chance to forward the data to any one of the C_2 nodes (with K_2 or K_3). This phenomenon can be observed clearly from Fig. 4a, where we find that a high percentage of secured communications still can be maintained even if a large number of C_1 nodes have been compromised. Moreover, we can see that more C_2 nodes can help to increase the fraction of unaffected communications, given the same number of compromised C_1 nodes.

In Fig. 4b, we consider scenarios in which we fix $N_2 = 3$ and let M_1 be 30, 45, and 90, where M_1 is the number of keys that can be stored in a C_1 node. In this case, $M_1 = 30$ can represent the lowest reliability because the connectivity of the network will be less than 99 percent if one C_2 node fails. At the other extreme, we notice that

The results of our experiment show that a good design can improve both security and survivability of a WSN. We also illustrate that there is a trade off between security and survivability in some scenarios.

$M_1 = 90$ can represent the situation with the highest reliability, because the connectivity of the network will be greater than 99 percent even if two C_2 nodes fail. Clearly, we can see the trade off between the reliability and resilience from this example. For example, if the number of compromised nodes is larger than three, $M_1 = 30$ can have better resilience than that of $M_1 = 90$.

Further Discussion

From the design example and the previous discussion, we can see that with a small number of powerful sensor nodes that have reasonable storage, processing, and transmission capabilities, the WSN can achieve good key connectivity, reliability, and resilience. We can further analyze the more general framework of the distributed key management schemes with the heterogeneous WSN. For instance, we can derive the relationship of reliability of the key management scheme in terms of the number of C_2 nodes and the number of keys in a C_1 node and the resilience of the key management scheme in terms of the number of C_2 nodes, the number of keys in a C_1 node, and the number of compromised C_1 nodes. We can derive the two functions in the following two equations:

$$O_{Rel} = f(u, v) \quad (1)$$

$$O_{Res} = g(u, v, w), \quad (2)$$

where u is the number of C_2 nodes, v is the number of keys in a C_1 node, and w is the number of compromised C_1 nodes; O_{Rel} is the key connectivity of the scheme under normal conditions (no compromised nodes), O_{Res} is the resilience of the new scheme, which is the key connectivity in terms of the number compromised C_1 nodes. We can see that key connectivity is the most important reliability and resilience metric of the key management. From the definitions of key connectivity, reliability, and the resilience in the previous section, we have $f(u, v) = g(u, v, 0)$; that is, Eq. 1 is a special case of Eq. 2 when $w = 0$. Equation 2 represents quantitatively the interaction of survivability and the security in terms of key management schemes under our WSN security architecture. Future studies will be performed on the interaction of survivability and the security in terms of other security attacks and security mechanisms in our WSN security architecture.

From the performance study on the interactions between survivability and security for WSN, we present an optimal design method for survivable and secure WSNs. Using the heterogeneous WSN security architecture again, we can observe from Eq. 2 that if we fix v and w and increase u — the number of C_2 nodes, O_{Rel}, should be increased; if we fix u and w, and increase v — the number of keys in a C_1 node, O_{Rel}, should be increased; and if we fix u and v, and increase w — the number of compromised C_1 nodes, O_{Rel}, should be decreased. In reality, u, v, and w are related to each other; for example, if we increase v — the number of keys in a C_1 node, the system becomes less secure, and w — the number of compromised C_1 nodes could be increased. Therefore, there is a trade off on the system survivability, O_{Rel}, in terms of v and w. Moreover, if we increase u — the number of C_2 nodes, the cost of the WSN also is increased.

Based on the previous observations, we can formulate a set of optimization problems to maximize a weighted average of the survivability functions and at the same time, to minimize the WSN cost function, under the constraints that the number of C_2 nodes u is within a set U, the number of keys in a C_1 node v is within a set V, and the number of compromised C_1 nodes w is within a set W. We will perform a detailed study of different design scenarios for survivable and secure WSN and create design strategies consistent with both sets of requirements for survivability and security of a WSN.

Conclusions

In this article, we have addressed the design issues for secure and survivable wireless sensor networks that are vulnerable to physical and network-based security attacks, accidents, and failures. Based on the study about the security and survivability requirements, we have developed an architecture for security and survivability in WSN with heterogeneous sensor nodes. To better understand the interactions between survivability and security, we also designed and analyzed a key management scheme within the architecture. The results of the experiment show that a good design can improve both security and survivability of a WSN. We also illustrate that there is a trade off between security and survivability in some scenarios.

Acknowledgments

This work was supported in part by the U.S. National Science Foundation under the NSF Award Number 0424546 and in part by an NSF EPSCoR start-up grant in Puerto Rico.

References

[1] S. Avancha *et al.*, "Security for Wireless Sensor Networks," Ch. 12, *Wireless Sensor Networks*, C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds. Kluwer, 2004.
[2] I. Akyildiz *et al.*, "A Survey on Sensor Networks," *IEEE Commun. Mag.*, Aug. 2002.
[3] K. Lu, Y. Qian, and J. Hu, "Analysis and Design of A Key Management Scheme for Wireless Sensor Networks," *Proc. IEEE IPCCC '06*, Phoenix, AZ, Apr. 10–12, 2006.
[4] K. Lu and Y. Qian, "On the Performance of a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks," *Proc. IEEE MILCOM '06*, Washington, DC, Oct. 23–25, 2006.
[5] M. Yarvis *et al.*, "Exploiting Heterogeneity in Sensor Networks," *Proc. IEEE INFOCOM '05*, Mar. 2005.
[6] Y. Law *et al.*, "A Formally Verified Decentralized Key Management for Wireless Sensor Networks," *Personal/Wireless Commun.*, LNCS, vol. 2775, 2003, pp.27–39.
[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proc. IEEE Symp. Research in Sec. and Privacy*, May 2003.
[8] S.-P. Chan, R. Poovendran, and M. T. Sun, "A Key Management Scheme in Distributed Sensor Networks Using Attack Probabilities," *Proc. IEEE GLOBECOM '05*, Nov. 2005.
[9] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comp. and Commun. Sec.*, Nov. 2002.
[10] C. Blundo *et al.*, "Perfectly-Secure Key Distribution for Dynamic Conferences," *Proc. CRYPTO '92*, LNCS, vol. 740, 1993, pp. 471–86.
[11] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *Proc. 10th ACM Conf.*

Comp. and Commun. Sec., Oct. 2003.

BIOGRAPHIES

YI QIAN (yqian@ece.uprm.edu) received a Ph.D. degree in electrical engineering from Clemson University. He is an assistant professor in the Department of Electrical and Computer Engineering at the University of Puerto Rico at Mayagüez (UPRM). His current research interests include network security, network design, network modeling, simulation, and performance analysis for next generation wireless networks, wireless sensor networks, broadband satellite networks, optical networks, high-speed networks, and the Internet. Prior to joining UPRM in July 2003, he worked in the telecommunications industry for several years.

KEJIE LU (lukejie@ece.uprm.edu) received his B.S. and M.S. degrees in telecommunications engineering from Beijing University of Posts and Telecommunications, China in 1994 and 1997, respectively. He received a Ph.D. degree in electrical engineering from the University of Texas at Dallas in 2003. In 2004 and 2005, he was a postdoctoral research associate in the Department of Electrical and Computer Engineering, University of Florida. Currently, he is an assistant professor in the Department of Electrical and Computer Engineering, at the University of Puerto Rico at Mayagüez (UPRM). His research interests include architecture and protocols design for computer and communication networks, performance analysis, network security, and wireless communications.

DAVID TIPPER (dtipper@mail.sis.pitt.edu) is a graduate of the University of Arizona (Ph.D. EE, M.S. SIE) and Virginia Tech (B.S.EE). He is an associate professor in the Telecommunications and Networking Program with a secondary appointment in the Electrical Engineering Department at the University of Pittsburgh. His current research interests are network design and traffic restoration procedures for survivable networks, network control, and performance analysis techniques. Prior to joining the University of Pittsburgh in 1994, he was an associate professor of electrical and computer engineering at Clemson University, South Carolina.