# Towards Survivable and Secure Wireless Sensor Networks

**Yi Qian[*], Kejie Lu[*], and David Tipper[+]**

[*] Department of Electrical and Computer Engineering
University of Puerto Rico at Mayagüez
Mayagüez, Puerto Rico 00681
Email: { yqian, lukejie}@ece.uprm.edu

[+] Department of Information Science and Telecommunications
University of Pittsburgh
Pittsburgh, PA 15260
Email: dtipper@mail.sis.pitt.edu

**Abstract** – In this paper, we present a comprehensive study on the design of secure and survivable wireless sensor networks (WSNs). Our goal is to develop a framework that provides both security and survivability features that are crucial to applications in WSNs, which are vulnerable to physical and network based security attacks, accidents, and failures. To achieve such a goal, we first examine the security requirements and survivability requirements. We then propose an architecture for security and survivability in WSNs with heterogeneous sensor nodes. To understand the interactions between survivability and security, we also design and analyze a key management scheme. The experiment results show that 1) a good design can improve both security and survivability of WSNs; and 2) in some situation, there is a trade-off between security and survivability.

**Keywords:** – Wireless sensor networks, survivability, security, reliability, availability, energy efficiency.

## I. INTRODUCTION

A wireless sensor network (WSN) consists of battery-operated sensor devices with computing, data processing, and communicating components. In WSNs, the sensor nodes can be deployed in controlled environment such as factories, homes, or hospitals; they can also be deployed in uncontrolled environment such as disaster or hostile area, in particular battlefield, where monitoring and surveillance is crucial. Clearly, *security* in WSNs is extremely important for both controlled environment (e.g., health-care, automation in the transportation, etc.) and uncontrolled and hostile environment (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 interruptions. Hence, *survivability* should also be taken into account in developing WSNs.

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 WSNs 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 high risk of physical attacks to unattended sensors. More importantly, these two factors may couple with each other. With the popularity of the WSNs 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 WSN.

In this paper, we present a comprehensive study on security and survivability for WSNs. Our goal is to develop a framework, secure and survivable 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 WSNs with heterogeneous sensor nodes. With the architecture, we identify metrics that quantify the performance of WSN. We also address the issues of the interaction between security and survivability for WSNs. For instance, node failures or coordinated physical/cyber attacks on sensor nodes will result in security breaches and impact WSN performance simultaneously. Similarly, a security attack compromising network components (e.g., sensor node, or cluster head) could impact network survivability techniques. On the other hand, a survivability strategy for restoring the performance could very likely be inconsistent with the security requirements. As a case study, we investigate a distributed key management schemes for WSN with heterogeneous sensor nodes.

The remainder of this paper is organized as follows. Section II gives the requirements of security and survivability for WSN. Section III discusses the detailed architecture for WSN survivability and security design. Section IV presents the study to understand the interaction between survivability and security for WSN. Section V gives the summary of this study and the future work.

## II. SECURITY AND SURVIVABLITY REQUIREMENTS IN WSN

### A. SECURITY REQUIREMENTS FOR WSN

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

**Confidentiality:** Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in sensors' environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information. Based on the sensitivity of the data stolen, an adversary may cause severe damage since he can use the sensing data for many illegal purposes, e.g. sabotaging, blackmail. Furthermore, by stealing routing information the adversary could introduce his own malicious nodes into the network in an attempt to overhear the entire communication. If considering 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 confidentiality objective since 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 ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then the behavior of the network could not be predicted and most of times will not outcome as expected.

**Integrity:** Moving on to the integrity objective, there is the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as environment and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Therefore, there is urgent need to make sure 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 multi components and handles sensitive information. In the case of WSNs, we need secure management on base station level; since sensor nodes communication ends up at the base station, issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management. Furthermore, clustering requires secure management as well, since each group of nodes may include a large number of nodes that need to be authenticated with each other and exchange data in a secure manner. Therefore, secure protocols for group management are required for adding and removing members, and authenticating data from groups of nodes.

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

B. SURVIVABILITY REQUIREMENTS FOR WSN

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

**Availability:** *Availability* ensures that services and information can be accessed at the time that they are required. In WSNs 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 targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network. If a node serves as an intermediary or collection and aggregation point, what happens if the node stops functioning? The protocols employed by the WSN need to be robust enough mitigate the effects of outages by providing alternate routes.

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

Evidently, there is a coupling between security, reliability, availability, and energy efficiency of WSNs. 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.

## III. AN ARCHITECTURE FOR SECURE AND SURVIVABLE WSN

### A. THE ARCHITECTURE

As the first step of the secure and survivable WSN design, we present a WSN security architecture with heterogeneous sensor nodes. In WSN, the physical security of wireless links is virtually impossible because of the broadcast nature and resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Consequently, security attacks on information flow can be widespread, e.g., 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 WSNs are similar to those of wireless ad-hoc networks due to similarities between the two types of the 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 be failed, thus affecting the operation of the whole network. 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 getting more attention. Particularly, with the advances in antenna technologies like multiple-input multi-out (MIMO) antenna systems [3], directional antennas [4], and cooperative communications [5], the heterogeneity in terms of transmission range for wireless sensor nodes become a practical solution. Recent studies also show that such heterogeneity can increase the network performance and network lifetime without significantly increasing the cost [6]. Although it has been proved in [6] that optimal deployment of the heterogeneity is very hard in general, it shows that only a modest number of reliable, long-range backhaul links and line-powered nodes are required to have a significant impact.

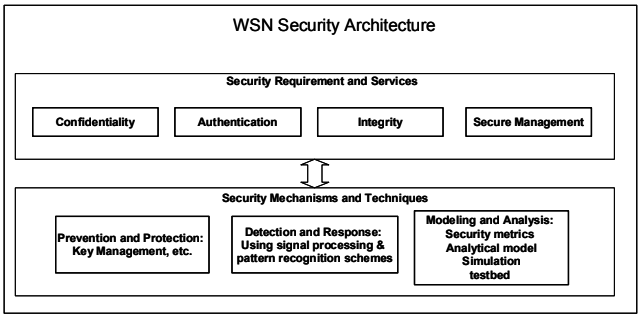



Figure 1: A General Architecture for WSN

To enhance security and survivability, we propose a general framework for WSN with heterogeneous sensor nodes. Individual security mechanism in WSN has been dealt with to a certain extent, but research and development of security architectures has been less extensive. To provide secure communications for the WSNs, all the aspects of security requirements and services need to be met and provided. Up to 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 WSN. Consequently, it is also important to address the reliability issue in the design of secure architecture for heterogeneous WSN using the modeling and analysis techniques.

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

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 bi-directional 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 direct communication link of a Class $n$ node, the Class $m$ node might need 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 WSNs assumed in this paper and the hierarchical WSNs in [7, 8]. In the hierarchical WSNs, the base stations (or cluster supervisors) are centralized nodes, and more importantly, they are acting like key distribution centers. By contrast, in the heterogeneous WSNs, 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.

### B. THE SECURITY 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 large network, and must be flexible against 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 lower number of compromised links. *Reliability* is the capability to keep the functionality of the WSN even if some sensor nodes are failed.

### C. THE SURVIVABILITY METRICS

The survivability concerns can be provided with the design goals of scalability, efficiency, key connectivity, resilience, and reliability. *Scalability* is the ability to support a large number of wireless sensor nodes in the network. Security mechanisms must support large network, and must be flexible against substantial increase in the size of the network even after deployment. *Efficiency* is the consideration of storage, processing and communication limitations on sensor nodes. *Key connectivity* is the probability that two or more sensor nodes store the same key or keying material. Enough key connectivity must be provided for a WSN to perform its intended functionality. *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 lower number of compromised links.

## IV. SECURE AND SURVIVABLE WSN DESIGN

To understand the interaction between survivability and security of our WSN security 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 can also see the trade-off between the reliability and the security in some examples.

### A. A KEY MANAGEMENT STUDY

Key management is one of the most important prevention and protection schemes for security mechanisms of WSN. To provide secure communications for the WSNs, all the messages should be encrypted and authenticated. Consequently, security solutions for such applications depend on existence of strong and efficient key distribution mechanisms for uncontrolled environments of WSNs. We illustrate how to design an effective key management framework under the general heterogeneous WSN security architecture. Up to now, almost all the existing key management 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 key management scheme for heterogeneous WSNs. Consequently, it is also important to address the reliability issue in the design of key management scheme. Energy conservation is a critical issue in WSNs since 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, pair-wise key establishment shall be 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 pair-wise key establishment techniques such as public key cryptography and key distribution center [9]. Instead, sensor nodes can use pre-distributed keys directly, or use keying materials to dynamically generate pair-wise 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 the random key distribution [10] and the polynomial based key pre-distribution protocol [11], and is inspired by the approaches of [12]. Similar to the studies in [10], we consider that there are three steps in the framework to establish pair-wise keys between the sensor nodes: 1) initialization, 2) direct key setup, and 3) path key setup. 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 setup step is for any two nodes trying to establish a pair-wise 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 path key setup step, trying to establish a pair-wise key with the help of other sensors.

Our scheme uses a pool of randomly generated bivariate polynomials to establish pair-wise keys between sensor nodes, with the consideration of $I$ classes of heterogeneity among the wireless sensor nodes. In this manner, existing distributed key management schemes can all be included in the framework. For example, if $I = 1$, which means that the sensor network is homogeneous, we have the following special cases: when all the polynomials are 0-degree ones and the sensor network is homogeneous, the polynomial pool degenerates into a key pool [10]; and when the polynomial pool has only one polynomial and the sensor network is homogeneous, the key distribution scheme degenerates into the polynomial based key pre-distribution [11].

The main challenge in this scheme is how to assign polynomial shares to different classes of nodes. We can

clearly observe that the major issue in our scheme is the subset assignment problem, which specifies how to determine the set of polynomials and how to assign the polynomial shared for each sensor node in group *j* with class *i*. During the key distribution procedure, a number of factors must be considered, include 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.

## B. UNDERSTANDING OF THE INTERACTION BETWEEN SURVIVABILITY AND SECURITY

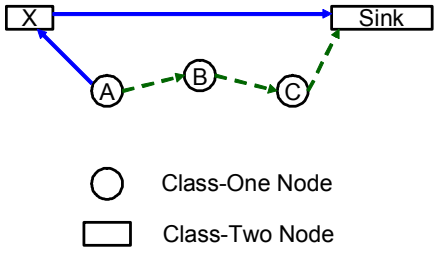
Based on the discussion in the previous section, we can see that our new key generation scheme is essentially different to most existing schemes in that the heterogeneity features can now be taken into account. To illustrate the advantages of the new scheme, we now consider a typical heterogeneous WSN that is established to collect data in a distributed scenario. In this scenario, a sensor node shall submit 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.2(a), 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 nature that a low class node will tend to utilize the link between itself and a high class node to submit the observations. For example, in Fig.2(a), Class One node A will tend to use the path "A-X-Sink" (the solid lines) to submit its report, instead of passing the message all by Class One nodes "A-B-C-Sink" (the dash lines). Clearly, a high class node will 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 will be more important than the connectivity between two low class nodes.

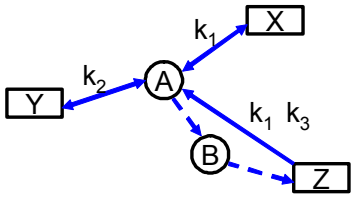
We now design a special key management scheme within the new framework for the above scenario. Specifically, we consider that there are two classes of the heterogeneous sensor nodes, i.e. $I = 2$. To simplify the discussion, we also assume that there is only one group, denoted as group 0, in the network.

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 $C_2$ 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. Since the transmission range of A is less than the transmission range of X, A may need to send messages to B through a multi-hop 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 only consider the direct key setup between a $C_1$ and adjacent $C_2$ nodes.

An example of this scheme is illustrated in Fig.2(b), where node A is a $C_1$ node and node X, Y, and Z are $C_2$ nodes. In this example, node 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, and $K_2$ 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, it can first randomly select a key from $K_1$ to $K_3$, then it can randomly select a neighbor node that shares the same key with it. For example, in Fig.2(b), if $K_1$ is chosen as the key, then node X and Z can be randomly selected. In this manner, we can see that the communication is more resilience, while the connectivity can also be maintained.




(a) An example for WSN




(b) An example for the proposed scheme

Figure 2: Examples for the WSN and the proposed key management scheme

To understand the behavior of the key management scheme above, we have conducted extensive quantitative study to evaluate their performance, in terms of key connectivity, reliability, and resilience. In our experiments, we consider a small area of WSN which consists of 200 $C_1$ nodes and a number of $C_2$ nodes, denoted as $N_2$. We also assume that, the size of key pool is 50,000 and the number of keys in any $C_2$ node is fixed to 2,000.

**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. Clearly, enough key connectivity must be provided for a WSN to perform its intended functionality. Fig.3 shows the connectivity of the proposed scheme versus the number of keys in a $C_1$ node with different number of $C_2$ nodes. We can first 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 $C_1$ node is small and 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, then about 113 keys are required for $N_2 = 1$, about 57 keys are required for $N_2 = 2$, about 38 keys are required for $N_2 = 3$, and about 29 keys are needed for $N_2 = 4$.

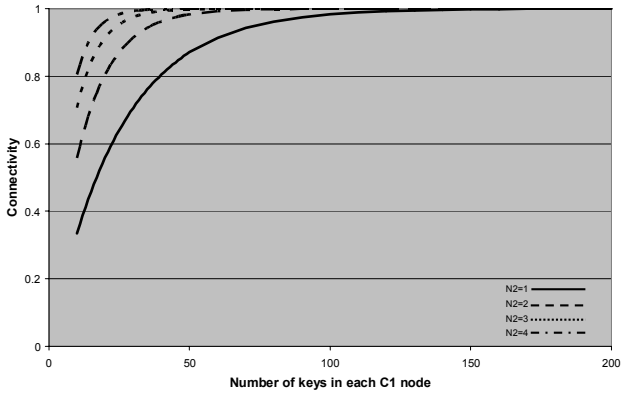



Figure 3: Connectivity of proposed key management scheme in normal conditions

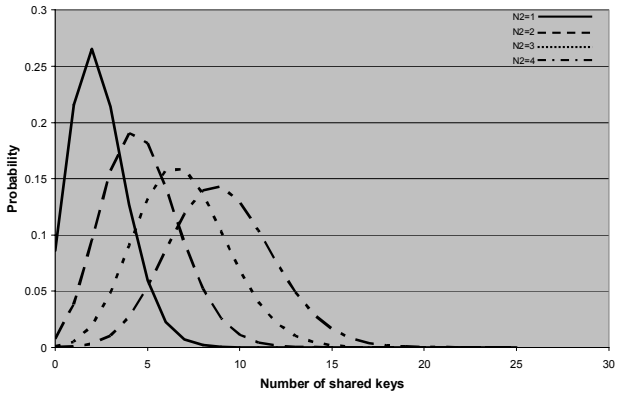



Figure 4: Probability of the Number of shared keys

To highlight the impact of the number of $C_2$ nodes, we demonstrate in Fig.4 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 60. We can observe that, with the increase of $N_2$, the shape of the distribution tends to shift to the right hand side, which implies that a $C_1$ node can share more keys with neighboring $C_2$ nodes. And with the increased 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.5, we consider the scenario in which the keys per $C_1$ node will be selected in a manner such that the network connectivity is *99%* 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 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 schemes, 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, then we can see that node *A* still has 66% chance to forward the data to any one of the $C_2$ nodes (with $K_2$ or $K_3$). This phenomenon can be clearly observed from Fig.5, where we find that a high percentage of secured communications can still 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 $C_1$ node.

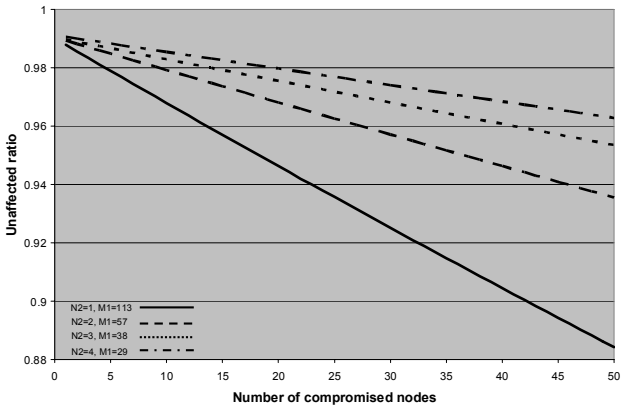



Figure 5: Resilience of the key management scheme in attack conditions (Connectivity = 99% in normal conditions)

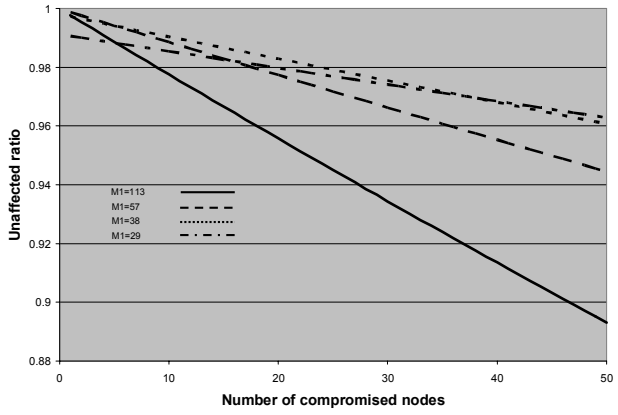



Figure 6: Resilience of the key management scheme in attack conditions ($N_2$=4)

In Fig.6, we consider scenarios in which we fix $N_2$=4 and let $M_1$ be 29, 38, 57, and 113. In this case, $M_1$=29 can represent the lowest reliability because the connectivity of the network will be less than 99% if one $C_2$ node is failed. On the other

extreme, we notice that $M_1$=113 can represent the situation with the highest reliability because the connectivity of the network will be greater than 99% even if three $C_2$ nodes are failed. Clearly, we can first observe the trade-off between the reliability and resilience from this example. For example, if the number of compromised nodes is larger than 5, $M_1$=29 can have better resilience than that of $M_1$ = 113. Moreover, we also notice that, given a certain number of compromised nodes, an optimum configuration may exist that can lead to the highest resilience. For instance, if the number of compromised node is 20, than $M_1$=38 has the best performance in terms of unaffected ratio.

## V. CONCLUSIONS

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

## REFERENCES


[1]. S. Avancha, J. Undercoffer, A. Joshi, and J. Pinkston, Chapter 12 Security for Wireless Sensor Networks, in Wireless Sensor Networks, Kluwer Academic Publishers, 2004, edited by C. S. Raghavendra, Krishna M. Sivalingam, and Taieb Znati.

[2]. I. Akyildiz, W. Su, Y. Sankarasubramanian, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazines, August 2002.

[3]. D. Gesbert, M. Shafi, D. S. Shiu, P. J. Smith, and A. Naguib, "From theory to practice: an overview of MIMO space-time coded wireless systems", IEEE Journal on Selected Areas in Communications, vol. 21, no. 3, pp. 281–302, Apr. 2003.

[4]. R. Ramanathan, J. Redi, C. Santivanez, D.Wiggins, and S. Polit, "Ad Hoc Networking With Directional Antenna: A complete System Solution", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 3, pp. 496–506, Mar. 2005.

[5]. S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks," *IEEE Journal on Selected Areas of Communications*, Vol. 22, No. 6, pp. 1089-1098, Aug. 2004.

[6]. M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting Heterogeneity in Sensor Networks," in *Proc. of IEEE INFOCOM'05*, Mar. 2005.

[7]. Y. Law, R. Corin, S. Etalle, and P. Hartel, "A Formally Verified Decentralized Key Management for Wireless Sensor Networks", Personal/Wireless Communications, LNCS, Vol. 2775, pp.27–39, 2003.

[8]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", Proceedings of IEEE Symposium on Research in Security and Privacy, May 2003.

[9]. S.-P. Chan, R. Poovendran, and M. T. Sun, "A Key Management Scheme in Distributed Sensor Networks Using Attack Probabilities", Proceedings of IEEE GLOBECOM'2005, November 2005.

[10]. L. Eschenauer, and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", Proceedings of 9th ACM Conference on Computer and Communication Security, November 2002.

[11]. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences", Proceedings of Advances in Cryptology - CRYPTO'92, LNCS 740, pages 471–486, 1993.

[12]. D. Liu, and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", Proceedings of the 10th ACM Conference on Computer and Communications Security, October 2003.