

Applying Key Infrastructures for Sensor Networks in CIP/CIIP Scenarios

Cristina Alcaraz and Rodrigo Roman

Computer Science Department,
University of Malaga,
29071 - Malaga, Spain
{alcaraz,roman}@lcc.uma.es

Abstract. It is commonly agreed that Wireless Sensor Networks (WSN) is one of the technologies that better fulfills features like the ones required by Critical (Information) Infrastructures. However, a sensor network is highly vulnerable against any external or internal attacks, thus network designers must know which are the tools that they can use in order to avoid such problems. In this paper we describe in detail a procedure (the KMS Guidelines), developed under our CRISIS project, that allows network designers to choose a certain Key Management System, or at least to know which protocol need to improve in order to satisfy the network requirements.

Keywords - *Critical Information Infrastructures, Sensor Networks, Key Management, Key Infrastructures.*

1 Introduction

According to the European Commission, *Critical Infrastructures* consist of "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States." [1]. These infrastructures depend on a spectrum of highly interconnected national (and international) software-based control systems for their smooth, reliable, and continuous operation. This information infrastructure underpins many elements of the aforementioned Critical Infrastructures, and is hence called *Critical Information Infrastructures* (CII).

CII are characterized by unique requirements for communications performance, including timing, redundancy, centers control and protection, and equipment control and diagnostics. One of the technologies that can fulfill these requirements are *Wireless Sensor Networks* (WSN)[2]. However, these networks are highly vulnerable against physical and logical attacks from a malicious adversary. Therefore, it is essential for a network designer to have the right set of tools and protocols for protecting the Wireless Sensor Network itself.

One of these tools are the *Key Management Systems* (KMS), which distributes some security credentials (i.e. keys) along the nodes of the network.

However, due to the great number of existent KMS, it is not clear which KMS is suitable for a certain scenario. The purpose of this paper is to introduce the KMS CRITIS Guidelines, a tool that will help network designers into choosing the right KMS for its WSN in a C(I)IP environment. The rest of this paper is organized as follows. In section 2 we explain in more detail the challenges of protecting a CII and its relationship with WSN. In section 3 we introduce our KMS CRITIS Guidelines, and explain the procedure for choosing a certain KMS. Afterwards, in section 4, we will describe and apply our Guidelines to some actual and possible C(I)IP scenarios. Finally, we conclude the paper in section 5.

2 The Importance of WSN for C(I)IP

2.1 CIIP Challenges

In a Critical Infrastructure, the interconnected nature of networks means that single, isolated disturbances can cascade through and between networks with potentially disastrous consequences. Therefore, it is indispensable to have a resilient and robust information infrastructure that could deal with any situation, being a physical or computational attack to the system or an abnormal behavior of any component inside the overall system. Such infrastructure must be able to issue alerts and warnings in order to help human users and the information subsystems to react against adverse scenarios. Those alerts could be issued even in the case that a problem is not taking place but the context seems to be slowly changing into a problematic situation. In a worst-case scenario, the information infrastructure must be able to react and protect itself in real time, and to assure the seamless continuation of its services.

As any Information infrastructure, the CII must be thoroughly tested in order to assure that the system and its response mechanisms will work under any kind of context. However, it is usually not feasible to test and obtain results about a CII without endangering the operation of the entire system itself. As a result, it becomes imperative to create models and simulations that show how the system should behave in presence of problems. As an input to these models and any decision-making tools, it is also of vital importance to analyze an infrastructure and quantify the possible problems in order to correctly model the protection system.

In all these processes, it is essential to guarantee the security of information that is considered of critical importance, from a political, economic, financial or social standpoint. Adding Information Security provisions such as authorization, authentication, encryption, and other basic security services is not enough to manage these complex scenarios and applications, due to the complex and dynamic nature of these infrastructures. Finally, since these Information Infrastructures compose a very heterogeneous environment, it is crucial to provide a set of policies and methods to allow an effective and secure interaction of the elements of a CII, both internal and external.

As we have seen, CII are characterized by unique and complex requirements, and are vulnerable to many different types of disturbances. Although strong

centralized control is essential to reliable operations, CII require multiple high-data-rate communication links, a powerful central computing facility, and an elaborate operations control center. All of them are especially vulnerable when they are needed most - during serious system stresses or disruptions. Therefore, intelligent distributed control is strongly required to keep parts of the network operational. Such intelligent control, alongside with other features, can be provided by Wireless Sensor Networks.

2.2 The Importance of Wireless Sensor Networks

Both the scientific community and the governments around the world have recognized the importance of Wireless Sensor Networks as an integral part of the protection of Critical (Information) Infrastructures. In the 2004 National Plan for Research and Development in Support for CIP [3], the U.S. Department for Homeland Security stated that one of the strategic goals was “*to provide a National Common Operating Picture (COP)*” for Critical Infrastructures, where the core of the systems would be an intelligent, self-monitoring, and self-healing sensor network. As a result, many projects regarding sensor networks and C(I)IP are being funded by the different U.S. agencies. Moreover, the Research Network for a Secure Australia (RNSA) has launched a major R&D initiative called the Cooperative Research Center for Security (CRC-SAFE), which aims to develop research and commercialization opportunities for CIP in Australia. One of the research programs of that initiative, Electronic Systems Security, will examine and develop solutions to security problems that arise in systems that are utilized in the critical infrastructure environment, including Wireless Sensor Networks [4].

A Wireless Sensor Network can be abstracted as the “skin” of a computer system, where hundreds or thousands of inexpensive and intelligent nodes (“cells”) are able to sense the physical events of their surroundings, such as temperature, humidity, light intensity, radiation, and others. They can be also connected to any external system, acquiring, processing, and supplying information about its status. Every node is battery-powered, communicates with the other using a wireless channel, and is totally independent. The Sensor Network, as a whole, is connected to one or many central systems (“brains”) called Base Stations, which provides an interface for accessing the data collected by the network.

An interesting property of the Sensor Network is that every node has computational capabilities, thus the network can work autonomously if the circumstances requires so. A typical sensor node such as MICAz [5] has a 8Mhz micro-processor with 128Kb of program flash memory and 512Kb of serial flash memory. Regarding their communication capabilities, nowadays most of the existing sensor nodes follows the IEEE 802.15.4 standard for Personal Area Networks, with a maximum data throughput of 250 Kbps.

As a sensing system, the tasks of a Wireless Sensor Network are focused on sensing the events of its surroundings, and providing that information to a set of users, being humans or machines or both. Those tasks include the following: Alerting (a Sensor Network is able to feel whether a problematic situation is

either going to happen or actually happening, and alert any user), Monitoring (a Sensor Network is able to continuously monitor its environment, adapting itself to the ever-changing context), Querying (a Sensor Network is also able to provide information “On-Demand”), and Distributed Computing (it is also possible to use the network as a distributed computing platform under extreme circumstances).

Both these tasks and the ability to work under severe conditions render Wireless Sensor Networks as an essential component in the overall scheme of protecting a Critical (Information) Infrastructure. A Sensor Network is capable of offering a redundant and resilient system that can provide an accurate diagnosis of a certain context, feeding systems such as Early Warning Systems. It can also provide the foundation of an intelligent distributed control system, both monitoring and supervising parts of the system even in situations where there is no central management available.

Moreover, due to its computational and wireless capabilities, a Sensor Network can be easily set up in a physical context where it is needed. For example, in case a control system is faced with a serious disruption that renders the operation of its subsystems unusable, a sensor network can be deployed “on the spot” that would provide reliable and robust information about the physical infrastructure or the status of any component.

2.3 CRISIS And Key Management

Although Wireless Sensor Networks can be regarded as an integral part of the protection of Critical (Information) Infrastructures, it has many problems and open issues by itself. Due to the extreme constraints of the network infrastructure, a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations. Protecting the information flow not only requires a set of power-efficient encryption schemes, but also an effective key infrastructure in terms of key storage policies, key distribution procedures and key maintenance protocols. Collecting the information from a static or dynamic set of nodes and routing it through the error-prone, unreliable network is a difficult task as well. Moreover, the network should be able to monitor over any failures or security breaches in any of its members while self-configuring and self-healing itself.

We have recently started a project, named CRISIS (CRITICAL Information Infrastructures Security based on Internetworking Sensors) [6], that tries to solve some of the previous problems in the context of a Critical Information Infrastructure. This on-going project focuses on the design of security solutions for Critical Information Infrastructures by means of the development of protection, control and evaluation mechanisms, where Wireless Sensor Networks are introduced as a main technological platform for this task.

More concretely, one of the areas of the project pursues the definition and design of *Advanced Authentication Services*, where, at low level, a network designer must choose a Key Management System (KMS) for the Sensor Network. In a

Wireless Sensor Network, Key Management is an essential part of its core behavior, since the wireless nature of the communication flow allows any malicious adversary to easily get access to the information of the network, eavesdropping or injecting packets. Therefore, a node must negotiate with its peers (offline or online) some security credentials in order to set up a secure communication channel.

The creation of a secure and optimal KMS is one of the most prolific areas in WSN research, spanning multiple research branches [7]. However, at present, a network designer has no means to know whether a certain protocol is suitable for its needs. For example, the requirements for a KMS in a sensor network that monitors a nuclear power plant are not the same as the requirements of a sensor network that is deployed after a radiation leak. As a result, we have studied the existent protocols and developed a manual (the KMS CRITIS Guidelines) that allows a network designer to choose a certain existent KMS, or at least to know which protocol needs to improve in order to satisfy the network requirements.

3 KMS CRITIS Guidelines

In this section we present the KMS CRITIS Guidelines (henceforth known as “The Guidelines”). Such Guidelines classifies the KMS according to their properties, rather than their features or the underlying mechanisms employed in their construction, such as Key Pools or Combinatorial Designs. This classification differs from other papers that survey the area, such as [7], in that it is oriented to help a network designer on choosing or constructing a certain KMS based on the properties of the network. Due to the extension of the Guidelines, we will only provide the protocols and main properties for configurations that could be relevant in the protection of Critical (Information) Infrastructures.

3.1 Main properties of a KMS

The main purpose of a Key Management System is to allow the nodes in a sensor network to securely negotiate a set of pairwise keys, which will be used in creating secure communications channels via security primitives like RC5 or Skipjack in TinySec [8] or AES in the 802.15.4 standard. However, every KMS gives some priority to certain objectives, optimizing certain properties while neglecting others. Those properties are the following:

Memory footprint. In a context where a sensor node is usually very constrained in terms of memory (a MICAz mote has only 4KB of RAM and 512KB of Flash memory [5], whereas a TMoteSky mote has 10KB of RAM and 1024KB of Flash memory [9]), it is essential for certain applications to reduce the memory footprint as much as possible. Many protocols are designed to reduce the memory space reserved to the security credentials (i.e., keys), primarily by reducing the number of keys to be used for bootstrapping the entire infrastructure.

Security. The purpose of any KMS is to provide the nodes in the network with some security credentials that the cryptographic primitives need for their

operation. The whole process of distributing the keys must be secure by default. However, in certain scenarios, there are extra security requirements that must be fulfilled. *Confidentiality* is one of those requirements, because in some protocols it is necessary to bootstrap the security credentials.

Network resilience. In order to provide the right data, a sensor node must be located near the source of the possible events. However, this also implies that any node is vulnerable against physical capture, revealing its security credentials. In order to avoid the disruption of the network services, some protocols are designed to increase the network resilience, that is, the ability to cope with stolen credentials and rogue nodes.

Connectivity. This network property is related to the chance of two sensor nodes sharing the same security credentials. In scenarios where the location of a sensor inside the network is unknown before the deployment, or where the sensor can change its position inside the network, it is essential to have a high connectivity. There are protocols that tries to provide the maximum connectivity while having a decent memory footprint or network resilience.

Scalability. It is widely believed that someday there will be sensor network deployments of thousands of nodes, even hundreds of thousands. Besides, it is sometimes necessary to increment the number of nodes inside a network to increase the sensing (or communication) coverage. For those reasons, a key distribution protocol should be able to negotiate the security credentials regardless the number of nodes in the network (*Scalability*), or to include new nodes after the deployment finishes (*Extensibility*).

Communication Overhead. In most KMS, the nodes must negotiate with its peers the security credentials that they will share. Due to the size of the data included inside the negotiation packets and the retransmissions that could happen during those negotiations, there are some protocols that are specialized in decreasing the overall communication overhead.

Energy. A sensor node relies on batteries for powering itself, thus it must minimize its internal operations (sensing, communication,...) in order to live as much time as possible. Since the negotiation of the security credentials is a time-consuming and energy-consuming task (inferring the security credentials, sending/receiving data to/from other peers,...), it is the purpose of some protocols to minimize the energetic impact of their operations.

3.2 The Guidelines

The Guidelines, as is, is a table composed of three columns. The first column specifies the main property of the protocols shown on its right. The second column specifies the name of the protocol in our Guidelines (*AT*-number), followed by the “official” name of the KMS. The third column shows the advantages (✓) and disadvantages (×) of every protocol, that is, which properties does and does not fulfill a certain protocol.

Due to space restrictions, the description of every advantage and disadvantage is reduced to the following nomenclature:

- Every property is abbreviated: Memory Footprint (Mem.), Security (Sec.), Network Resilience (Res.), Connectivity (Conn.), Scalability (Sca.), Extensibility (Ext.), Communication Overhead (Comm.), Energy (En.).
- Some protocols have special requirements for being applied: i) The location of the nodes is known prior to the deployment (*LOC*). Also, when the requirements/properties of a certain protocol are affected by the variables used on its design, we use: *DES*{ α }.

For applying the Guidelines, a network designer must first find out which properties are essential for a KMS in its scenario (we will call them main properties), and which properties are not essential but important (we will call them secondary properties). After that, he must consult the protocols whose first column are equal to one of the main properties, and seek a protocol that has all the properties in the advantages and none in the disadvantages. If no protocol suits his needs, he can still know the weak points of the existents protocols and construct a new one.

The Guidelines itself are shown in Table 1, at the end of the paper. This way, it will be more easy for network designers to consult and apply the Guidelines.

4 C(I)IP Scenarios

There have been a large number of C(I)IP scenarios that involve sensor network technology in their operations, such as control of physical infrastructures, control of industrial machinery, monitoring of gas and oil transportation, and homeland security. Even so, these are just a fraction of the possible scenarios where sensor networks could be applied. In this section, we will present both scenarios where sensor networks are being applied or could be applied, and we will make use of our Guidelines in order to suggest a certain KMS to be employed or improved for an specific scenario.

4.1 Actual C(I)IP Scenarios

These are some of the actual projects where Sensor Networks have been or are being applied to areas related to Critical (Information) Infrastructure Protection.

Monitoring of Ageing Infrastructures. The Smart Infrastructure KIC (Knowledge Integration Community) [10] is a community of researchers at Cambridge and MIT. This community grew out from the “New technologies for condition assessment and monitoring of ageing infrastructure” project, where the research team was invited to develop and deploy a prototype wireless sensor network system to monitor the condition of a stretch of London Underground tunnel, which has some tunnels over 75 years old. In this trial, sensors transmitted the data to the Base Stations located in the columns, and then the data was forwarded to a central database.

Detecting Equipment Vibration. Intel is conducting a trial deployment of a wireless sensor network to monitor the health of semiconductor fabrication equipment in one of its plants in Oregon [11]. Specifically, the network

senses the vibration signature of water purification equipment, providing data for early warning systems. In this deployment, groups of up to six sensors connect to battery-powered wireless motes form clusters, and a Crossbow Stargate computer, equipped with IEEE 802.11 (Wi-Fi) connectivity, serves as a cluster head. The deployment of wireless sensor networks, which can be installed inexpensively and provide more frequent and more reliable data, could decrease the response time in case of an emergency, reducing both the equipment and the service downtime.

Management of Mobile Assets. As on 2004, BP had a fleet of some 12,000 freight railcars transporting a range of products as diverse as polypropylene and natural gas liquids. Their journeys can be relatively short or cross-border, delivering products from its manufacturing plants to customers. Due to the hazardousness of some of these products, it is necessary to know about the status of the cars and its contents. BP, together with Intel [11], ran a trial where each car carried sensors to measure the temperature of the contents, the weight of the load, accelerometers to record impact, and a GPS transponder to give location. Every sensor was connected to a central station, where the data was transmitted using to a geostationary satellite, for onward relay to BP's control center. The trial was a success, and nowadays BP is expanding the trial with new services such as 'pinging' the cars - interrogating them from mobile devices such as laptop computers and cell phones.

Identifying hazards to safety-critical structures. The DISCOVERY (Distributed Intelligence, Sensing and Coordination in Variable Environments) project, developed by CSIRO (Commonwealth Scientific and Industrial Research Organisation), Australia's national science agency, aims to create fully autonomous underwater sensor networks to protect critical infrastructure and water resources [12]. Ultimately these networks, that can be deployed either on demand or in advance, will be used to identify hazards to safety-critical structures such as off-shore oil rigs, to respond to contamination of water supplies such as oil spills, to track oil spills to their sources (in a three-dimensional environment) and to establish absorption perimeters. The sensor network should be able to optimally distribute and coordinate sensing, computation, and actuation, providing efficient multi-agent communication and information fusion.

4.2 Potential C(I)IP Scenarios

The scenarios described in the previous section are only a subset of what could be accomplished using Wireless Sensor Networks for Critical (Information) Infrastructure Protection. In this section we preview some possible new scenarios yet to be developed.

Self-Powered Communication and Diagnosis System. In moments of crisis (e.g. a network failure inside a chemical plant), the control systems that form a Critical Information Infrastructure must react timely and effectively, providing the users with the appropriate information about the source and the extent of the problem. However, these control systems are also vulnerable by itself: their information networks can fail, and they can be unavailable in scenarios

involving power loss. In such cases, Sensor networks can behave as a self-powered redundant communication and diagnosis system, routing both information about the computer it monitors and information about its physical environment to any existent control system.

Testing of Existent Sensor Systems. Some Critical Information Infrastructures, such as the radiation detection subsystem inside a power plant, must provide accurate data about the physical state of its environment. As a result, it is essential to test the behavior of the system as frequently as possible in order to prevent false alarms or failures in times of crisis. Due to its features, a Wireless Sensor Network can be a valuable asset for this purpose. A sensor network can be easily set up in the same places where the sensors of the CII system are located, automatically creating an information network which allows the system administrators to discover and take measures against any anomalies in the actual sensing system.

4.3 Applying the Guidelines to C(I)IP Scenarios

In this section we will apply the Guidelines for every scenario described above. As a result, we will obtain a KMS that can be immediately used to provide security credentials to the sensor nodes in a real environment. Note that, in certain scenarios, there is no KMS that can fulfill all the requirements of that scenario.

Monitoring of Ageing Infrastructures. In this scenario, the main property a KMS must fulfill is Connectivity (Sensors are working in a hard to deploy, hostile environment), while the secondary properties are Resilience and Security (Due to the importance of the infrastructure). Applying the Guidelines, the protocol that best suits those needs is *AT-4*, although *AT-24* could be applied, too.

Detecting Equipment Vibration, Management of Mobile Assets. In these scenarios, the main properties a KMS must fulfill are Connectivity (Sensors are working in a hostile environment - an industrial machine) and Resilience (Due to the importance of the data's reliability), while the secondary properties are Security (In the case that the deployment area is not totally secure) and Energy. Applying the Guidelines, the protocol that best suits those needs is *AT-1* if the deployment site is totally secure. If not, the best protocol should be *AT-23*.

Identifying hazards to safety-critical structures. This scenario is fairly complex, since all the properties are essential being Connectivity (due to the mobile nature of the nodes) and Resilience (due to the importance of the data) primary ones. There is no protocol that can suit perfectly to this scenario, although *AT-4* could be applied if such scenario must be deployed immediately.

Self-Powered Communication and Diagnosis System. In this scenario, the main properties a KMS must fulfill are Resilience (Due to the "public" nature of the node), Connectivity (Sensors are working in a hostile environment) and Scalability (The network itself can grow if required), while the secondary property is Security (In the case that the deployment area is not totally secure).

Applying the Guidelines, the protocols that best suits those needs could be *AT-24* and *AT-25*.

Testing of Existent Sensor Systems. In this scenario, the main properties a KMS must fulfill are Resilience (Due to the “public” nature of the node and the importance of the data), Connectivity (Sensors are working in a hostile environment), Scalability (Due to the staggered deployment), and Communication (Also due to the staggered deployment). Applying the Guidelines, the protocols that best suits those needs could be *AT-16* if the nodes know their deployment location, or *AT-13* and *AT-24*.

5 Conclusion

We have discussed why Wireless Sensor Networks are essential for protecting Critical (Information) Infrastructures, and how such technology is not exempt of security problems. As a step into developing secure WSN for C(I)IP in real scenarios, in this paper we have presented the KMS CRITIS Guidelines, a tool that allows network designers to either choose a certain Key Management System or discover which protocols could use as a foundation for its own protocol.

As a final note, while developing the KMS CRITIS Guidelines, we have discovered that most of the Key Management Protocols i) have no step for allowing the maintenance of the keys, ii) does not allow the introduction of new nodes, and iii) are not designed with a certain scenario in mind. We conclude that security experts should take these three considerations into account. The third one is interesting: Evidently, there is an inherent risk of designing too many KMS, but since WSN are scenario-centric, the resulting networks will be much more secure.

References

1. Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism*, COM (2004) 702 final, Brussels, 20 October 2004.
2. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. *Wireless sensor networks: a survey*. Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol.38, No. 4, pp. 393-422, March 2002.
3. *2004 US National Plan for Research and Development in Support for CIP*. April 8, 2005. Retrieved from http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf
4. D. Bopping. *CIIP in Australia*. 1st CI2RCO Critical Information Infrastructure Protection conference. Rome, March 2006.
5. Crossbow Technology, Inc. Wireless Measurement Systems. <http://www.xbow.com>.
6. J. Lopez, J. A. Montenegro, R. Roman. *Service-Oriented Security Architecture for CII based on Sensor Networks*. 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), Lyon (France), June 2006.

7. A. Camtepe, B. Yener. *Key distribution mechanisms for wireless sensor networks: a survey*. Rensselaer Polytechnic Institute, Computer Science Department, Tech. Rep. 05-07, March 2005.
8. C. Karlof, N. Sastry, D. Wagner. *TinySec: a link layer security architecture for wireless sensor networks*. In Proceedings of 2nd International Conference on Embedded Networked Sensor Systems (SensSys'04), November 2004.
9. Moteiv Corporation. <http://www.moteiv.com>.
10. *Smart Infrastructure*. The Cambridge-MIT Institute. <http://www.cambridge-mit.org/smartinfrastructure>
11. *Sensor Nets / RFID*. Intel Corporation. http://www.intel.com/research/exploratory/wireless_sensors.htm
12. *Distributed Intelligence, Sensing and Coordination in Variable Environments*. CSIRO. <http://www.ict.csiro.au/page.php?cid=97>
13. L. Eschenauer, V.D. Gligor. *A key-management scheme for distributed sensor networks*. Proceedings of the 9th ACM conference on Computer and communications security (CCS '02), ACM Press, November 2002, pp 41-47.
14. W. Du, J. Deng, Y. S. Han, P. Varshney. *A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge*. In IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 2, pp 62-77, January-March 2006.
15. W. Du, J. Deng, Y.S. Han, P.K. Varshney. *A pairwise key pre-distribution scheme for wireless sensor networks*. Proceedings of the 10th ACM conference on Computer and communications security (CCS '03), ACM Press, October 2003, pp 42-51.
16. R.D. Pietro, L.V. Mancini, A. Mei. *Random key-assignment for secure Wireless Sensor Networks*. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN '03), ACM Press, October 2003, pp 62-71.
17. H. Chan, A. Perrig, D. Song. *Random Key Predistribution Schemes for Sensor Networks*. In 2003 IEEE Symposium on Security and Privacy, pp. 197-213, May 2003.
18. J. Lee, D.R. Stinson. *Deterministic Key Predistribution Schemes for Distributed Networks*. 11th International Workshop on Selected Areas in Cryptography (SAC 2004). Canada, August 2004. Revised Selected Papers published in Lecture Notes in Computer Science 3357 (2005), pp 294-307.
19. D. Liu, P. Ning, R. Li. *Establishing Pairwise Keys in Distributed Sensor Networks*. ACM Transactions on Information and System Security, Vol. 8, No. 1, pp. 41-77, February 2005.
20. R.J. Anderson, H. Chan, A. Perrig. *Key Infection: Smart Trust for Smart Dust*. Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP 2004), October 2004, pp 206-215.
21. D. Liu, P. Ning. *Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks*. ACM Transactions on Sensor Networks (TOSN), Vol. 1, No. 2, pp. 204-239, November 2005.
22. A. Camtepe, B. Yener. *Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks*. Proceedings of the 9th European Symposium on Research Computer Security (ESORICS'04), September 2004, pp 293-308.
23. D.D. Hwang, B. Charles Lai, I. Verbauwhede. *Energy-Memory-Security Tradeoffs in Distributed Sensor Networks*. Proceedings of the 3rd International Conference on Ad-hoc Networks and Wireless (ADHOC-NOW 2004), July 2004.
24. J. Hwang, Y. Kim. *Revisiting Random Key Pre-distribution Schemes for Wireless Sensor Networks*. Proceedings of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks (SASN '04), ACM Press, October 2004, pp 43-52.

Memory	AT-8 - Basic Probabilistic Key Predistribution [13]	✓: Mem., Sca. ×: Sec., <i>DES</i> {Conn., Comm., Res.}
	AT-16 - Key Predistribution by using Deployment Knowledge [14]	✓: Mem., Conn., Res. ×: <i>DES</i> {Conn., Res.}, Comm., <i>LOC</i>
	AT-13 - Blom Key Predistribution [15]	✓: Mem., Conn., Comm., Res., Sca. ×: Ext., <i>DES</i> {Mem., Res.}
Security	AT-11 - Co-operative Pairwise Key Establishment [16]	✓: Sec., Res. ×: En., Comm.
	AT-05 - Random Pairwise Key [17]	✓: Sec., Sca. ×: <i>DES</i> {Conn., Res., Mem.}
Network Resilience	AT-13 - Blom Key Predistribution [15]	✓: Res., Mem., Conn., Comm., Sca. ×: Ext., <i>DES</i> {Mem., Res.}
	AT-14 - Multiple Space Key Predistribution [15]	✓: Res., Sca. ×: <i>DES</i> {Conn., Mem., Comm.}, En.
	AT-07 - Q-Composite [17]	✓: Res. ×: En., Sca., <i>DES</i> {Mem., Res., Conn.}
	AT-21 - Deterministic Multiple Space Blom DMBS [18]	✓: Res., Ext., Comm., Sca. ×: Mem., Conn.
	AT-25 - Polynomial Based Key Predistribution [19]	✓: Res., Comm., Sca. ×: Mem., En.
	AT-24 - Grid Based Key Predistribution [19]	✓: Res., Conn., Comm., Sca. ×: Ext., Mem., En., <i>DES</i> { <i>LOC</i> }
	AT-01 - Key Infection [20]	✓: Res., Conn., Sca., Mem. ×: Comm., Sec.
Connectivity	AT-16 - Key Predistribution by using Deployment Knowledge [14]	✓: Conn., Mem., Res. ×: <i>DES</i> {Conn., Res.}, Comm., <i>LOC</i>
	AT-23 - Closest Pairwise Key Predistribution, Extended [21]	✓: Comm., Mem., Conn., Res. ×: <i>LOC</i>
	AT-24 - Grid Based Key Predistribution [19]	✓: Conn., Res., Comm., Sca. ×: Ext., Mem., En., <i>DES</i> { <i>LOC</i> }
	AT-03 - Symmetric Design [22]	✓: Conn., Comm. ×: Sca., Mem., Res.
	AT-04 - Hybrid Designs - Generalized Quadrangle [22]	✓: Conn., Sca., Mem., Res. ×: <i>DES</i> {Conn., Sca.}
Scalab.	AT-18 - Multiple ID-Based one-way Function [18]	✓: Sca., Mem. ×: Res., Conn., Comm.
	AT-04 - Hybrid Designs - Generalized Quadrangle [22]	✓: Sca., Conn., Mem., Res. ×: <i>DES</i> {Sca., Conn.}
Comm.	AT-23 - Closest Pairwise Key Predistribution, Extended [21]	✓: Comm., Mem., Conn., Res. ×: <i>LOC</i>
	AT-10 - Cluster Key Grouping [23]	✓: Comm., Sca. ×: <i>DES</i> {Conn., Res., Mem.}
Energy	AT-01 - Key Infection (for small networks) [20]	✓: En., Res., Conn., Sca., Mem. ×: Comm., Sec.
	AT-17 - Transmission Range Adjustment (for small networks) [24]	✓: En., Mem., Conn. ×: Comm., Sec.

Table 1. KMS CRITIS Guidelines - Reduced Version