International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.251-270
http://dx.doi.org/10.14257/ijsia.2015.9.11.24

Network Security and Metrology: A Survey

Reham Abdellatif Abouhogail

Electrical Quantities Metrology Dept
National Institute for standards
Cairo, Egypt
rehlatif@yahoo.com,
rehlatif@gmail.com

Abstract

Without the science of metrology, we lost the way of any research field. The science of metrology affects the science of network security in many sides. You have to measure in network security as you have to do in the other fields. You have to test and analyze and detect as in the other research areas. You must work hard to reach the standards level in network security as you make your best efforts to reach them in other science branches. From the other side, network security has a great effect on developing the science of metrology. In the present paper, many trends are introduced including the two viewpoints. The necessary requirements to research and development in network security and metrology are proposed. Finally, we declared how different metrology labs around the world are interested in this field.

Keywords*: Network Security; Metrology; Remote Calibration*

1. Introduction

For a long time, it was the only solution for solving the problems in the network to increase the bandwidth capacity, to have a larger tube and faster routers, and to improve traffic flow. From about 10 years, metrology has contributed to change this think with a focus on network management [1]. Today, metrology can provide new improve especially, in network security. Metrology is used to discover functional problems in networks, to measure error rate and to detect active or passive abnormal behavior items [1]. If there is no security metrology, then there will be no standards and no rules to do anything [2]. As metrology is very important to raise the quality of network security, metrology has many effects on network security. Metrology can be useful in many ways [1]:

1. To determine network availability: if there is any congestion in the traffic. Are consequently services and servers properly distributed in the network?
2. If there is any abnormal rate of collision, error in packets, *etc*.?
3. To make accounting as a relation to network usage, a detailed measurement of traffic is necessary.
4. To learn network handling: (who does what, when and how?)
5. To determine malicious actions.

Scariot *et al*. in [1] divides the effect of metrology to network security into two main types of elements: quantitative elements and qualitative elements.

1. Qualitative elements:

These elements are interested in device performance indicator values, like to provide information about traffic quality values. These elements give us information about traffic quality, either in absolute terms or in relative to physical

ISSN: 1738-9976 IJSIA

characteristics of the network, like available bandwidth. The target of this type is to know how data-flow happens. This helps to understand and to manage traffic, and to satisfy acceptable quality.

2. Quantitative elements:

These elements are interested in the details and the characteristic of the traffic. In this type, the traffic is categorized according to data types, protocols (TCP, ICMP, UDP, *etc*.), sender or receiver. The results are used to help the management of the traffic. The management includes the answer of the following questions as mentioned in [1]:

1. Which services are essential?
2. Where servers may be located to keep away from flow congestion?
3. Which changes of network structure may develop the quality of service?

In the other side, metrology can't progress without robust network security. There are several applications in which the internet is necessary for the metrology developing process. These applications like: remote metrology and transfer of measurement data through the internet. So we can say that this paper tries to answer all the questions related to the network security and metrology (who, why, how and what?) as follows:

1. Who works in network security and metrology?: Section 2 introduces the necessary background for any researcher who interested in this field.

2. Why we must work in this field?: Section 3 mentions the main points which the science of metrology affects the network security system.

3. How we can verify our work?: Section 3 describes the verification tools which are used to test the network security system either the verification tools which are used to test security protocols or network simulators which are used to test the network performance in general including the security parameter.

4. What are the effects of network security to metrology?: Section 4 describes the other side of effect which is the effect of network security to the science of metrology. Section 5 makes a tour around the world to see how the metrology labs see this branch. Finally, the paper conclusion is in Section 6.

2. The Necessary Background for the Security Metrology Researchers

Security metrology needs a background about the science of metrology. May be in the beginning, this will not require a high experience of metrology and the complex calculations of the uncertainty. Because this field is still not mature enough. It is sufficient to be aware of the meaning and the objective of the metrology science and believe that the metrology science is the way to develop and raise the quality of any field. If you can measure something, so you know something about it. If you can't measure something so you don't know anything about it. A deep background about security systems is required. A good experience in cryptography and cryptanalysis is recommended. The basics of networks and programming are also required. Then according to the application he will need to increase his experience. The person who searches in this field may require some experience in electronic circuit design if he has to implement something hardware. Many research fields in security metrology are in need to the scientists to study, discover and solve. The next section describes some of these research trends.

3. Metrology Effects in Network Security

Metrology affects network security in several areas. When metrology science is applied in network security the progress and development will be satisfied in an acceptable level. The following points list the main points that metrology should be applied to reach a good progress in network security.

1. Applying the Standards to the Implementation of Security Systems.
2. Network Security Metrics.
3. Measuring, Detecting and analyzing the Effects of Attacks.
4. Studying and Developing Network Simulators.
5. Verifying Security Protocols (verifying security protocols and study verification tools).
6. Improving the quality of Network Security.

3.1 Applying the Standards to the Implementation of Security Systems

Many researchers work in the implementation of security systems either using hardware implementation or software implementation. Using the standards will give a difference in the quality and reliability of the system. For example, there are many types of symmetric encryption algorithms, like: RC2, DES (Data Encryption Standard), 3DES, RC6, Blowfish, and AES (Advanced Encryption Standard) [3]. The Strength of Symmetric key encryption differs from one to other. When you use the standards, especially the last version it will give you good quality and we can say that you applied the rules of metrology to your system. Also, you have to improve your security system to be comparable with the level of standards. Abouhogail in [4] proposes New Multicast Authentication Protocol for Entrusted Members Using Advanced Encryption Standard. Using the standard AES in this research gives the system many benefits like for example: a good level of security strength, applicability of the system to the real time applications and raise the confidence in the system. Also, Searching in developing the standards of network security is considered a hot topic in security metrology. In [5], a new fast handover authentication scheme with privacy preservation to improve the capabilities of IEEE 802.16m [6] is presented which is considered an application to develop the standards of network security systems in the topic of WiMAX (Worldwide Interoperability for Microwave Access). WiMAX is a wireless broadband technology. The protocol proposed by Anmin Fu.et al. in [7] presents a privacy preserving fast handover authentication scheme based on pseudonym for IEEE 802.16m network. He also made a developing in the IEEE 802.16m [6] to decrease the computation cost required. Arun in [8] made a modification in the Mix-columns function of the AES algorithm which results in good throughput. He presented two implementations: one with online key expansion and the other with offline key expansion in a many core system. In [9], Dyken et al. presented a different trend in the optimization of the AES algorithm which was focused on how to decrease the power consumption of an FPGA (Field Programmable Gate Array) [10] based encryption scheme with least effect on performance. So using the standards in your applications or improving and developing new standards are considered a very interesting topic in network security metrology.

3.2 Network Security Metrics

The topic of security metrics is interested in the factors that we can measure to determine the level of security. Security cannot be measured as a universal concept due to the complexity, uncertainty, non-stationary, limited observability of operational systems, and malice of attackers [11]. Many other reasons behind this

difficulty in measuring security mentioned in [12] some of them will be declared in the following:

1. Some security requirements are difficult to be tested.
   Security requirements are difficult to be described to determine behaviors and functions to satisfy tested requirements. So to test the security you have to include all things in the system either good or bad. You have to include how the system will be used well and how the system may have occurrence of misuse. Actually, this is difficult in software, because it requires proving that certain situations are impossible.
2. The interaction between Security and Measurement
   You can decrease the level of security of the system if you measure it. This is done in two methods. First, when we describe the details of your system, the intruder may use this information to attack the system in other sides. Second, the technology we construct may lead to unintentional consequences. For example, raising the level of security to a system can change how people use it. Users may expose their selves to more risks, expecting more security will protect them.
3. Measurement is an expectation and an organization target
   Most organizations weight security's benefits in a different way. So, before determine how secure we are, we must set up security's value according to the objectives of other organizations.
4. Overoptimistic
   Managers and system users are overoptimistic in thinking that their systems are unlikely aims or thinking that the future will be as the past.

So we can say that network security metrics and security metrology are still in their first age, due to various reasons [11]. Security Metrics can be used to offer security evidence for security engineering, risk and security management, and internal and external evaluation. Searching in security metrics is a very important topic that helps to improve the science of security. As an application of searching in security metrics, in [5], new metric is presented for handover authentication protocols in wireless networks. It's the required time for base station and mobile station to detect the undesirable messages. The proposed scheme in [5] gives a minimum time of detection to these undesirable and fault received messages. This metric means the ability of the protocol to fall under the denial of service attack. As this time increases the protocol is considered more susceptible to denial of service attack. So you have first to select the topic. Second, study the standards in this topic. Third, study the literature of this topic to know what people interested to measure in this area. Then from the point of view of the metrology you have to think for other parameters could be measured in addition to the existing which help to develop, to upgrade and to solve the problems of the system.

3.3 Measuring, Detecting and Analyzing the Effects of Attacks

Any computer networks especially, wireless networks faces many and different types of threats (attacks). Threats in the world of computer networks have different shapes and different types of effects. The main two categories of attacks are active attacks and passive attacks. In the passive type of attack, the attacker reads data from the network but does not write or make any changes to it. In active attack, the attacker writes, modifies or delete something in the data of the network. Any types

of threats affect the security system goals. The security system has some goals to protect the communication. The most important goals of the security system are:

- **Confidentiality:** Confidentiality means that the data is kept secret from unintended listeners.
- **Data Integrity:** Data integrity means to keep the received data as the sent data.
- **Authentication:** This means that the one who makes some actions is the one we intended and the one that we have given him the authority to do this action.
- **Non-Repudiation:** When the system provides data integrity a receiver can be sure of both the sender's identity and that he is receiving the data that the sender meant to send. But, he cannot necessarily prove this fact to a third party.

In [2], Huang et al. designed a good security metrology system to solve the problem of compromise attacks. They put a standard; they call it the security ratings. They used negative-credit, and positive credit approach to control the problem of node compromise. In [13], detection and measuring of Blackhole [14] attack is presented. The application for a wireless network system especially for MANET (Mobile Ad Hoc Networks) [15] or for VANET (Vehicular Ad-Hoc-Networks) was the target of this paper. The research discussed the behavior of the famous wireless routing protocols under the effect of Blackhole attack and without this type of attack. Also, the paper measures the change in the performance parameters of the routing protocols under different number of Blackhole attack nodes. The performance parameters were the most important network performance metrics as:

Packet Delivery Ratio (PDR): it represents the ratio of total data received to total data sent from source to destination. So we can say that it measures the loss rate in the network.

Average End-to-End Delay: This is the average time that a packet takes to travel from the source node to the destination node in a network. This parameter is very important for certain type of applications like, voice and video transmission which is required small delay.

Packet Dropped: This parameter represents the total number of packets discarded by all nodes in the network.

Network Throughput: It is the average rate of successful messages delivered through the communication channel. It is represented in bits per second or packets per seconds. This parameter is affected by many affects like Unreliable communication, changes in topology, limited bandwidth and limited power. So the target of our research in this trend is to detect and analyze the effect of attacks on the network performance. This trend requires a good background about network communication in general then a good study about the selected application as a specific. The following subsection will help you to select the suitable network simulator to help you to perform your task.

3.4 Studying and Developing Network Simulators

This branch is interested in studying the different types of network simulators and trying to develop in them. To test or to measure the performance parameters for any network system there are many available network simulators tools like: NS2, NS3, OPNET, QuaLNet and OMNeT++ [16]. Some of them are commercial and others are open source. You can select the suitable simulator for your target application. In [17], a complete comparison between the different types of available network simulators is presented. The advantages and disadvantages of each simulator are described in detail. The programming language for each one is declared. It could be concluded from [17] that NS_2 and OMNeT++ are the best choices for research. NS_2,

the most popular simulator for academic research, is generally criticized for its complicated architecture. OMNeT++ is gaining popularity in academic and industrial world. Unlike NS_2, OMNeT++ has a well-designed simulation engine and supports hierarchical modeling. So, OMNeT++ is better for developing. Also, OMNeT++ has a great GUI which gives it advantage than NS2. However, OMNeT++ lacks the large number of external models that NS2 has. OPNET Modeler is a good choice for industrial researchers, people who need a wide set of built-in reliable models for building credible simulations in a fast way, rather than academic researchers. NS_3 is the fastest simulator among the selected simulators in terms of computation time. The community-based model concept of NS3 is a strong point and a disadvantage at the same time. Because NS_3 is non-commercial software this leads to a wide active community. This wide community helps to improve, extend and upgrade NS_3. But, on the other hand makes the NS3 simulator impossible to guarantee reliable customer support and solve bugs. QualNet is easy-to-use and clear user interface. It has high animation capabilities and support for multiprocessor systems and distributed computing. But, it is very expensive. Almost simulators can support your network performance testing that you need. But as can we see they differ from the point of cost free or commercial. They differ from the external shape some simulators have a good GUI and others haven't. They also differ between each other according to the used programming language as shown in Table 1. So we can say that by using network simulators, you can test the performance of your network. Security is considered one of the most important performance parameter of the network and we can test it using the network simulators also as in [14].

Table 1. Comparison Between Network Simulators According to the Used Programming Language.

The network simulator	NS2	NS3	Qualnet	Opnet	Omnet++
Programming language	Otcl& C++	Python& C++	C++	C& C++	C++

Table 2 Comparison between network simulators according to the Operating System

The network simulator	NS2	NS3	Qualnet	Opnet	Omnet++
Windows	√	√	√	√	√
Unix	√	√	√	√	√
Linux	×	×	√	×	√
Mac	×	×	√	×	√

Table 2 shows a comparison between the presented network simulators according to the common operating systems. From Table 2 windows and Unix are suitable for the five simulators. Also, from Table 2, we can observe that QualNet and OMNet++ can run on Linux and Mac operating systems.

So, the topic of studying and also developing network simulators is a very important topic for security network and metrology field. This trend needs a good background in programming in addition to the background in networks and routing protocols.

3.5 Verifying Security Protocols (Verifying Security Protocols and Studying Verification Tools)

A protocol definition in general is as mentioned in [18]: "a series of steps, involving two or more parties, designed to accomplish a task". From this definition, we note that the protocol has some conditions.

1. It must have a certain sequence.
2. It must contain more than one part.
3. It must have a target and execute a task. Other characteristics as mentioned in [18] are:
4. The parties participated in the protocol must know the protocol and all its steps.
5. The parties participated in the protocol must agree to follow its steps.

Security protocols are certain programs intended to secure Networks. The security protocols are designed to satisfy levels of security. Also, they are the necessary tool to achieve various goals according to the application. The main goals of the security protocols are application dependent, but as a general they are: authenticity, confidentiality, integrity, privacy, non-repudiation, key exchange, key distribution, etc. Intruders aim to prevent the goals of security by number of behaviors. Failing of security protocols can have serious consequences, resulting in loss of money or loss of trust of users in the application. Parties of the protocol are called agents and often called A (for Alice) and B (for Bob) as shown in Figure 1. A third party often called I (for Intruder) represents the enemy who wants to penetrate the protocol. A fourth party who judge in case of dispute for example is the server.

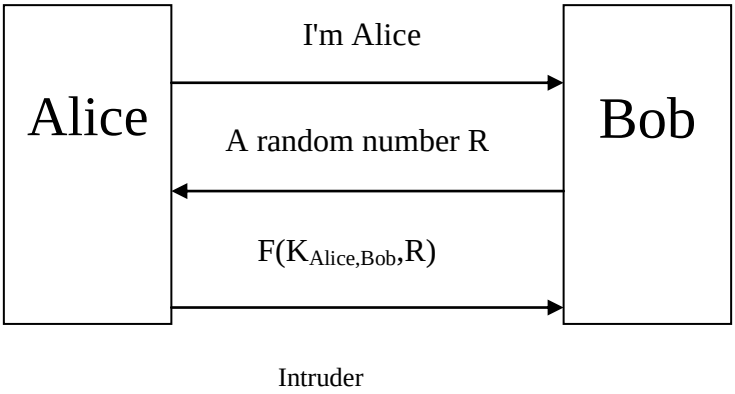

Figure 1. Example of Simple Security Protocol.

Verifying security protocols is a challenging task. There are some verification tools that are used to verify security protocols mentioned in [19]. Formal methods are used in the analysis of security protocols. The application of formal methods to security protocols became wide spread until the early 90's. In this sub-section, we give a description of the formal methods that are used to test the security protocols. There are four types for the verification of security protocol tools [20]: Type A (Modeling and Verifying Protocols using Specification Languages), Type B (Expert Systems), Type C (Algebraic-Term Rewriting) and Type D (Formal Logical Models). Details of each type are given in the following.

Type A (Modeling and Verifying Protocols using Specification Languages)

This type is the least popular type. It depends on model and verifies protocols using any suitable programming languages and using of verification tools that are not developed specifically for the analysis of such protocols. The main idea is to

model the security protocol as any other program and try to confirm its rightness. But, this method proves the rightness of the protocol but does not necessarily prove the goals of security declared in subsection (3.3). In [21], Sidhu suggests representing the protocol as a directed graph. In [22], Varadharajan approves the directed graph's method. However, Varadharajan in [23] uses LOTOS (Language of Temporal Ordering Specification) for specifying authentication protocols. Kemmerer in [24] saw that the protocol should preserve as state invariants.

Type B (Expert Systems)

In Type B approach, expert system is built. So, a protocol designer can use it to develop and examine different scenarios. These systems begin with an unwanted state and attempt to discover if this state is reachable from an initial state or not. This type identifies problems in the protocols better than Type A, but it doesn't guarantee the security of an authentication protocol. It also doesn't provide an automated technique for developing attacks on a protocol. So we can say that: Type B approach can find problems from the known types of problems, but if there are unknown types of problems, Type B cannot find them. As an example the Interrogator proposed by Millen [25]. Millen presented an expert system used in the analysis of security protocols. The interrogator is a software tool used to examine the protocol, asking what the penetrator might do to defeat it. The interrogator is written in Prolog [25]. The input to the system is a protocol specification and a goal of the penetrator, and the interrogator searches for a scenario involving penetrator actions. The Interrogator is developed for the analysis of key management. Longley and Rigby [26] present the rule-based system used to determine the weakness of a key management system according to certain types of attacks.

Type C (Algebraic-Term Rewriting)

This type develops a formal technique to analyze protocol based on the algebraic-term rewriting properties of cryptographic systems. This approach was introduced by Dolev and Yao [27], and modified by Meadows [28], and Woo&Lam [29] and others. Dolev and Yao are considered the first who propose the first algebraic representation for the security of protocols. Their protocols depend more with the distribution of secrets than authentication. Secrets and authentication are much related. The main distinction between the secrets and authentication is that: the authentication involves another part called authentication server. So we can say that the Dolev and Yao protocols examine only the scheme of two parties [30]. Thus, the majority of the protocol analysis techniques that use the Dolev-Yao model use additional modeling techniques to describe these protocols [31]. In general, the Algebraic-Term Rewriting of formal protocol analysis is very complex, thus its use as a verifier tool for security protocols is reduced. A famous example is the Needham- Schroeder protocol [32] on which G. Lowe discovered a weak 17 years after its publication [33]. The algebraic verification tool to verify security protocols has a benefit in modeling when you want to extend the model. So you can do it easily. But this kind of verification is not suitable for large system. It will be very hard and the probability of error will increase.

Type D (Formal Logical Models)

This type is the most common approach. This type applies formal logic models. These models are introduced for the analysis of knowledge and belief, like: BAN logic [34], the logic of Syverson [35]. The BAN logic, by Burrows, Abadi, and Needham [28] helps the user to be precise about what the goals and assumptions of a protocol actually are. It is often very difficult to determine these from several specifications. The BAN logic was designed scalable. In [36], Gong, Needham and Yahalom proposed the GNY model. It's considered a modification to the original BAN logic. GNY logic assumes that redundancy doesn't exist in encrypted messages. GNY logic represents a new notion called recognizability. It's an important notion. It represents that a principal expects certain formats in the messages it will receive. A CS modal logic of knowledge and beleif is another modification to BAN [37]. These logics were successfully used to generate concise proofs and have identified a number of flaws in protocols previously considered secure.

Type E Automation Tools

Automatic Tools are very useful tools to discover failures in security protocols. The previous methods cannot be easily applied by normal security protocol analyst. This is because protocols have to be redeveloped for each type, and it is so difficult. So, some tools are designed as automatic verifiers. The inputs to any such verifier are a description of the system to be analyzed and the required properties of the protocol. The output proves that the required properties are verified or reports that they are not. Brackin in [38] proposed a simple Interface Specification Language (ISL) and describes an Automatic Authentication Protocol analyzer (AAPA) which can automatically either confirm that the required protocols assure the desired properties, or identify precisely where these protocols fail [38]. Another proposed language named Common Authentication Protocol specification Language (CAPSL), to some degree stimulated by ISL, is being developed by Millen [39]. CAPSL is useful for determining the correctness of the protocols in theoretical level. CAPSL is proposed as a single common protocol specification language that can be used as the input format for any formal analysis technique, such as in [40], the NRL Protocol Analyzer, Higher Order Logic HOL [41] and model-checking with the Failures Divergences Refinement Checker FDR [42]. The objectives of the CAPSL design are usability, abstraction, completeness, extensibility, and scalability. CAPSL was designed to analyze the kind of protocol specifications that appear in textbooks and articles [43]. ProVerif [44] is an automatic cryptographic protocol verifier. This protocol verifier is based on an abstract representation of the protocol by Horn clauses. It can handle many different cryptographic primitives and an unbounded number of sessions of the protocol and message space. But, it does not support timed language specification and focus mainly on secrecy and authentication only [45]. Ventuneac et al. in [46] presented an automated verification technique to test security protocols based on the logic model (Type D). The automated system uses the CS modal logic implemented on a layered proving tree-based proving engine. After you get the correct results from the verification process to your system, you may want to reach to the higher level which is the modification. Table 3 gives a comparison between the 5 types of verification tools presented.

Once you select the topic of research and determine the points of weakness or the problems that your application faces. You have to go to the following subsection which presents to you the last trend in this section which is improving the quality of network security.

3.6 Improving the Quality of Network Security

The science of metrology is interested in improving the quality of any system. As the communication is considered a very important system in our day life so improving the quality of any communication system is considered a progress in the science of metrology. To reach a good level of secrecy in the communication system is considered an important improving in the quality of the communication system. So network security becomes a very important for many applications around us. They are very important for e-commerce like: bank transactions, NFC (Near Field Communication) applications [47] and e-voting. We can improve network security in many ways like the following points.

1. We can minimize the number of attacks that the system has no immunity towards them.
2. Minimizing the communication and computation overhead due to adding security functions.
3. Proposing new security protocols with better features or enhancing the known to overcome the problems that they face.

In [48], a confidentiality enhancement of the Secure Real Time Protocol (SRTP) is presented. The paper used chaotic systems to propose an alternative scheme to enhance confidentiality in SRTP. A Quality of Service analysis is presented. Lee in [49] presents two secure password authenticated key agreement protocols based on chaotic maps. One is based on synchronized clocks, while the other based on a nonce. In the two proposed protocols, users only keep their password and do not require additional equipment for storing a long-term secret key. In the next section, we will introduce the other side of interaction between network security and metrology which is the effects of network security in metrology.

Table 3. Comparison Between the Types of Verification Methods Used to Verify Security protocols.

	The Main Idea	Advantage	Disadvantage
Type A (Modeling and Verifying Protocols using Specification Languages)	Depends on model and verifies protocols using any suitable programming languages	proves the correctness of the protocol but not necessarily proves the goals of security	Doesn't require big experience.
Type B (Expert Systems)	Expert designers build it	protocol designer can use it to develop and examine different scenarios	1. Itdoesn’t guarantee the security of an authentication protocol. 2. It doesn't provide an automated technique for developing attacks on a protocol. 3. if there are unknown types of

			problems, cannot find them
TypeC (Algebraic-Term Rewriting)	based on the algebraic-term rewriting properties of cryptographic systems	Has a benefit in modeling when you want to extend the model. So you can do it easily.	1. Very complex. 2. Not suitable for large system.
Type D (Formal Logical Models)	uses formal logic models	Helps the user to be precise about what the goals and assumptions of a protocol actually.	Limited applications.
TypeE (Automation Tools)	Automatic verifier	Normal security protocol analyst can use it, not requires the protocol designer himself.	Still not common and not advanced enough.

3. Network Security Effects in Metrology

4.1 Remote Calibration

Inside all metrological labs, there is a regular need for instrument calibration, and a traceable connection to a national or international standard should be existed. Achieving traceability requires a laboratory to periodically send their standards to be calibrated at a National Measurement Institute (NMI), obtaining a certificate and correction values. The standards are measured under carefully controlled conditions at the NMI, but we will not be sure that these conditions will be satisfied when the standards are used at the normal working environment of the instrument. Additionally, in some cases, the value of the standards can be affected by transport which may cause an uncertainty component, which is difficult to assess. So one essential metrology service that can be carried over the internet is the calibration of instruments. Services that present remote calibration are known as iCals (Internet Calibration Services). The implementation of remote calibration via the internet varies significantly with each measurement example but there are some general rules the system must have one of them. They are as follows [50]:

1. Stable calibration object with simply confirmed performance check.
2. Simply transported measurement object from which the calibration is derived.
3. The software used for calibration is the same software which is used for uncertainty calculation.

Procedures for implementation of Remote Calibration:

We can conclude the general procedures the system must have to carry out remote calibration. They are as follows:

1. The computer is connected to the measurement system through GPIB (General Purpose Interface bus) or serial bus.
2. The operator is directed by the iCal system. This is under condition that the operator is accredited with using the system.
3. The iCal system generates the required final data with uncertainties calculations after the procedures are completed.
4. Providing the certificate.

Note that: Internet calibration is not applicable to all metrology areas, because physical constraints and human interaction are essential for some measurements. We can see real examples for remote calibration in [51], [52], [53] and [54].

4.2 Remote operation of measuring instruments

This subsection includes the other uses of the internet to provide access to a whole range of measurement services. Like for example:

1. Remote monitoring of equipment.
2. Web based access to: libraries, testing services, calibration history, measurement data, and simulation software.

The software utilities required for carry the measurements are already embedded in operating systems, as an example of these software Microsoft Windows virtual private network and remote desktop connections [55]. Another solution is to distribute software control applications as web pages, which can then be remotely accessed; this function is supported by LabVIEW program from National Instruments [56]. LabVIEW is a graphical programming language that uses icons instead of lines of text to create applications. LabVIEW has provided communication tools, including ActiveX, TCP, UDP, and Data Socket. LabVIEW web server can create HTML documents open front panel in web browser. The front panel can be remotely monitored and controlled through the web browser using TCP/IP services. This feature greatly expands the application as several persons sitting at different locations can simultaneously access the same front panel.

The most important examples of remote operation of measuring instruments are the instrument control and remote monitoring of sensors. Examples of remote monitoring of sensors can be seen in [57] and [58]. [59] and [51] presents examples of instrument control. The system implemented in [60] uses the Virtual Instrumentation Software Architecture (VISA) [59]. VISA is a standardized interface working between the control application and the instruments. VISA can deal with GPIB bus or serial bus. A small .Net component is used to load the VISA library. The component contains four orders: FindResources, Read, Write, and Query. The FindResources order is used to search the client-side instrument bus for connected instruments. The Write, Read and Query orders are used to send text messages to and from the instruments.

Use the LabVIEW VI Server to programmatically control front panel objects, VIs, and to dynamically load, edit, and run VIs on a computer or remotely across a network. You can control browser access to the VIs and configure which VIs remote applications can control.

The remote panels are configured using many steps, but the main two steps are as follows:

1. Enable the LabVIEW web server on the server machine.
2. Select the protocol TCP/IP as an example.
3. Choose the port number.
4. Connect and execute remote panels on the client machine by writing the address of the server, the port number and the name of file.

Remote metrology operations affect the security of the computer which causes risks when sending and receiving the measurement data. In the following subsection, the problem of security during metrology is presented with some alternative solutions. In the following subsection, most benefits of remote metrology are collected.

4.3 Benefits of Using Internet Connection in Metrology

The benefits of internet connection for metrology can be specific to the type of measurement application to which it is applied, but there are many benefits that are common to almost all such services. Internet connection gives the ability to build direct traceability to national standards. Through internet connection application the user can choose the suitable time for him. For metrology calibration as an example, the calibration is done in the user's environment, ensuring that measurement results exactly reflect the environment relevant to that user's situation. Appropriately high levels of accuracy can be transferred to the user's laboratory and this can be the maximum levels of accuracy. With remote calibration, the downtime of the equipment is reduced, and the equipment will be occupied only during the calibration process.

4.4 Practical Examples of Using the Internet in Metrology

In this section we will present three examples for applications of using the internet in metrology from other world labs. The first example is a Central LAZAR [61]. It's a remote laboratory works with specialists to improve the quality of metrological services. The second example is an application to remote calibration service. It's from PTB. The last is from NIS (National Institute of Standards) [62].

A Central LASAR [61] (Central of Remote Assistance Associated Laboratories) is proposed to minimize the gaps between metrology suppliers and the customers. They provide context platform and solutions for all metrology suppliers to satisfy the needs of their customers. Almost all metrology information generated by the system has customer's rights. All the system runs on a SSL (Secure Sockets Layer) platform, through https protocol, using a 1024 bits RSA Algorithm [3]. More than this, to guarantee the confidentiality of information traffic, all data is pre-coded through MIME base 64 algorithm, transforming the data in an illegible charcters sequence [63]. Some of the services Central LAZAR presents are listed below:

1. On line technical support for IT and software doubts.
2. Users and Customers management by implementing different permissions hierarchy.
3. Automatic technical modules management by including the restrictions for each customer.
4. Customers monitoring.
5. Customer database access but in a security way.

Infrared Remote Sensing is an increasingly important tool for studies of earth resources or environmental monitoring. However, measurements have to be traceable to SI units to be comparable world-wide and reliable in the long term. A new infrared calibration facility established by PTB provides highly accurate standard sources of infrared radiation for this purpose [64]. In [51], an automated system for the resistance remote calibrations in NIS is demonstrated. Many resistors can be calibrated automatically through the resistors automatic changer which is controlled by a prepared LabVIEW program.

4.5 Importance of Security in Using the Internet in Metrology

When using the internet for general instrument control and particularly when offering transfer of measurement data in open systems, several security threats appear. The information sent across the network should be impossible to modify or replay, at least not without detection. If an intruder could access to the system and appear as if it was the remote object then sends old method calls, serious problems

could be happened. Username and password are required to authenticate the specific customer. Using certificates like X.509 certificates signed by a trusted certificate authority. Examples for secure measurement data are presented in [53] and [60]. The system that is presented in [53] allows a person connected to a local area network (LAN) to control multiple electrical instruments located at other LANs via a public web server on the internet. The system is based on Microsoft.NET Remoting. The .NET Remoting has no default security features, but it is prepared for custom security implementation. The system uses the HTTPS protocol because it's well known and well tested protocol. The system in [60] is a project called SELMA (Secure Electronic Measurement Data Exchange). The goal of the project is to satisfy secure transfer of measured energy data from decentralized meters to the authorized users via open networks. SELMA has developed security architecture to establish trust in the electronic transfer of data from the meter to data acquisition systems and further to the customers. The introduced security mechanisms are based on public-key cryptography and more specifically on digital signatures that allow the signed measurement data to be verified and authenticated in combination with a suitable key management. Numbers of metrology labs around the world are interested in network security measurements which will be presented in the following Section.

5. Network Security and Metrology in the Metrology Labs

Network Security is an important division in number of metrology labs around the world. We will introduce them and their participation in this field in the following subsections.

5.1 National Institute of Standards and Technology (NIST)-USA [65]

The Computer Security Division (CSD), a part of NIST's Information Technology Laboratory (ITL), supplies standards and technologies to protect information systems against threats to satisfy the confidentiality, integrity and availability of information and services.

CSD participated in many challenges and opportunities leading to the development and implementation of high-quality, cost-effective security and privacy mechanisms that improved network security across the world and throughout the national and international information security area.

CSD continued to develop standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services. Also, it interested in recognizing the potential benefits of more automation in technical security operations. The CSD also continued to work closely with federal agencies to improve their understanding and implementation of the Federal Information Security Management Act (FISMA) to protect their information and information systems. CSD supported most intelligence community and national security community to build a unique framework for information security through the federal government. This plan is expected to result in larger standardization and more reliable and cost-effective security for all federal information.

5.2 PTB - Germany [66]

Division number 8 in PTB is called: Medical Physics & Metrological Information Technology. This division is interested in: Medical Metrology, Biosignals, Biomedical Optics, Mathematical Modelling and Data Analysis, and Metrological Information Technology. The working groups in Metrological Information Technology part are the following:

- Metrological Software.
- Data Communication and Security.
- Gaming Machines.

The Data Communication and Security working group carries out research and development in the field of measurement data communication and security. The work is focused on interfaces by

- developing test tools and test methods for device interfaces and
- Testing interfaces, and on distributed measurement systems, in particular
- Open communication concepts for measurement technology.
- Data exchange procedures for measuring devices in distributed systems.
- Security of measurement data transfer systems.

5.3 National Metrology Institute of Japan (NMIJ) -Japan [67]

They are occupied in supporting IT development and industrial contest by advancing technologies through research and development. Specific plans include infrastructural technologies such as high-reliability, high-performance, and green cloud data centers; the realization of strong and secure yet flexible data integration and network management systems; communication systems for smart grid; interactive information utilization technologies for images, voice, and other data; communication platforms that distribute sensing data; and technologies for the utilization of geographical information. They seek to share research results with society at large, not only in the form of technical contribution but also through supplying industry with its needs from easy-to-use platforms and services.

5.4 National Physical Laboratory (NPL)-UK [68]

Under the branch of commercial services in NPL a branch of measurement services. This sub branch divides into number of services. In the environmental monitoring service, there is a branch for measurement for security applications. This includes instrument and technique development for biological and chemical agents, validation of techniques and the keystone for metrological support.

5.4 National Institute for Standards-Egypt [62]

Under the division of Electrical Quantities Metrology Department there is a lab for the Information Technology. The lab is interested in many fields related to network security and metrology. Its research serves metrology and information technology together. As an example of this area of research are: computer-based metrology, metrological software, remote metrology, security of measurement data, simulation and modeling of measurement data, performance measurement, network metrology, dependability evaluation, quality of protection measurement, software testing, verification of security protocols, and Testing of electronic attacks.
As shown in Figure.2 we present the most metrology labs that are interested in network security and metrology.

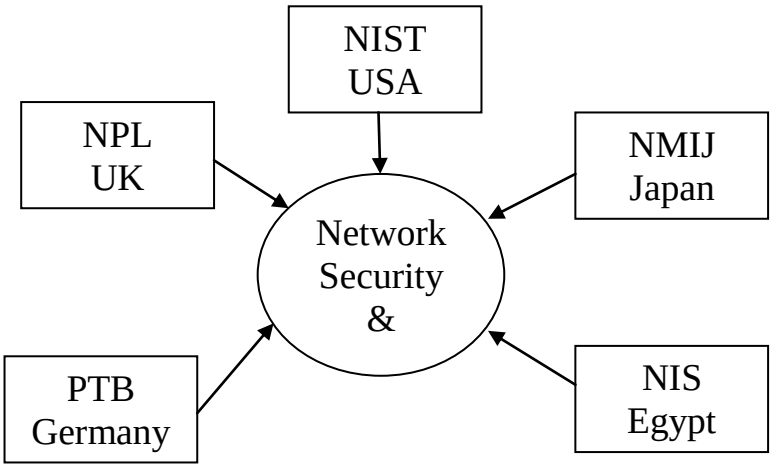

Figure 2. The Most Metrology Labs that are Interested in Network Security and Metrology

6. Conclusion

As we can see from the present paper, metrology has many effects to network security if applied. Metrology improves the quality of the network. Having a measurement to the "security level" of a system increases the trust in the system. Measuring and evaluating security would enable us to easily compare between two systems. As Scariot et al. said in [1]: to control and manage a network, you must visualize its behavior. The applicability of metrology to network security is still not mature enough due to number of obstacles. Some of them are mentioned in the present paper as the difficulty to test all security requirements; measurement and security interact, in addition to the small number of experts in this area. The description of them is considered the first step to try to get a solution for them. In our paper, we divide the effect of metrology to network security in six parts. They are:

1. Applying the standards to the implementation of security systems,
2. Network security metrics,
3. Measuring, detecting and analyzing the effects of attacks,
4. Studying and developing network simulators,
5. Verifying security protocols (verifying security protocols and studying verification tools) and
6. Improving the quality of network security. Each part is declared with the suitable examples.

We hope in the future that security organizations make their purchase decisions according to the security measurements or take into consideration the ratio between the security level and the price. So the vendors would be more active to improve the security level of their systems. In the other side, the metrology applications through the internet like remote calibration and remote operation of measuring instruments need a strong cryptographic mechanism. This is a very essential task to keep the security of the measurement data. Many metrology labs around the world are interested in the network security and metrology. Some of them are presented in the paper like: NIST in USA, PTB in Germany, NMIJ in Japan and NPL in UK and NIS in Egypt. Finally, I think we can summarize by the following sentence:"When you measure you can see, when you don't measure you can't see".

References

[1] J-F Scariot, Be Martinet, "NetSEC: metrology-based application for network security", Future Generation Computer Systems, Vol. 19, 2003, pp.303–311, **(2003)**.
[2] S. C.-H. Huang, S. Makki2, and N. Pissinou, "Accusation Resolution Using Security Metrology", WASA 2006, LNCS 4138, Springer-Verlag Berlin Heidelberg, pp. 435–444, **(2006)**.
[3] W. Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , **(2005)**.
[4] R. Abdellatif Abouhogail, "New Multicast Authentication Protocol for entrusted members using advanced encryption standard", the Egyptian Journal of remote sensing and space sciences, 16 Dec **(2011)**.
[5] R. Abdellatif Abouhogail, "Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks", International Journal of Security and Its Applications, of Security and Its Applications, Vol.8, No.5 **(2014)**, pp.361 -376.
[6] IEEE 802.16 Work Group, IEEE standard 802.16m-2011, "Air interface for broadband wireless access systems amendment 3: advanced air interface", Tech. Rep. IEEE; May **(2011)**.
[7] A. Fu, Yuqi ng Zhang, Zhenchao Zhu, Qi Jing, Jingyu Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network", Computers and Security, June **(2012)**, pp.741-749.
[8] M.S.Arun, V.Saminathan, " Parallel AES Encryption with Modified Mix-columns For Many Core Processor Arrays", International Journal of Engineering Science and Innovative Technology (IJESIT)Vol. 3, Issue 3, May **(2014)**.
[9] J. Van dyken, Jose G. Delgado-Frias, "FPGA schemes for minimizing the power-throughput trade-off in execurting the Advanced Encryption Standard algorithm", Journal of Systems Architecture (JSA), Vol. 56, **(2010)**, pp.116-123.
[10] http://www.xilinx.com/training/fpga/fpga-field-programmable-gate-array.htm.
[11] R. M. Savola, "Quality of security metrics and measurements", Computers & Security, 37, **(2013)**, pp. 78-90.
[12] S. L. Pfleeger and R. K. Cunningham, "Why measuring security is hard," Secur. Priv. IEEE, vol. 8, no. 4, **(2010)**, pp. 46–54.
[13] E. Farag Ahmed, Reham Abdellatif Abouhogail, Ahmed Yahya, "Performance Evaluation of Blackhole Attack on VANET's Routing Protocols", International Journal of Software Engineering and Its Applications, Vol.8, No.9, **(2014)**, pp.39-54.
[14] H. Singh and M. Singh, "Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs", International Journal of Advanced Trends in Computer Science and Engineering, vol. 2, no. 3, **(2013)** May-June.
[15] R. Abdellatif Abouhogail, "Security Assessment for Key Management in Mobile Ad Hoc Networks", International Journal of Security and Its Applications, Vol.8, No.1, **(2014)**, pp.169-182.
[16] S. V. Mallapur, and Siddarama R. Patil," A Novel Approach Of Simulation Tools For Mobile Ad-Hoc Networks",IJCSC, Vol. 3, No. 1, January-June **(2012)**, pp. 1-10.
[17] E. Ahmed, Reham Abdellatif Abouhogail, Ahmed Yahya, "A Comparison Study of Currently Used Network Simulators", Al-Azhar Engineering Thirteenth International Conference. Dec. **(2014)**.
[18] Bruce Schneier, Applied Cryptography, John Wiley& Sons, Inc, **(1994)**.
[19] Reham Abdellatif Abou Hogail, "Multicast Authentication Protocol", Ph.D thesis, Ch.3, Faculty of Engineering, Ain shams university, **(2008)**.
[20] A. D. Rubin and P. Honeyman, "Formal Methods for the Analysis of Authentication Protocols", CITI Technical Report 93-7, Center for Information Technology Integration, Dept. of Electrical Engineering and Computer Science, University of Michigan, Nov**.(1993)**.
[21] D. P. Sidhu, "Authentication protocols for computer networks", I. Computer Networks and ISDN Systems, pp. 297-310, **(1986)**.
[22] V. Varadharajan, "Verification of network security protocols", Computers and Security, 8(8):693-708, **(1989)**.
[23] Vijay Varadharajan, "Use of a formal description technique in the specication of authentication protocols", Computer Standards and Interfaces, pp.203-215, **(1990)**.
[24] R. A. Kemmerer, "Analyzing encryption protocols using formal verification techniques", IEEE Journal on Selected areas in Communications, 7(4), pp.448-457, May **(1989)**.
[25] J.K. Millen, S.C. Clark and Sheryl B. Freedman, "The Interrogator: Protocol Security Analysis", IEEE Transactions on Software Engineering, SE- 13(2), pp.274-288, Feb. **(1987)**.
[26] D. Longley and S. Rigby, "Use of Expert Systems in the Analysis of Key Management Systems", Security and Protection in Information Systems, pp. 213-224, **(1989)**.
[27] D. Dolev and A. Yao, "On the security of public-key protocols", Communications of the ACM, pp. 198-208, Aug. **(1983)**.
[28] M. Meadows, "A system for the specification and analysis of key management protocols" Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, pp.182-195, May **(1991)**.

[29] Thomas Y.C. Woo and Simon S. Lam, "A Semantic Model for Authentication Protocols" Proceedings of the 1993 IEEE Computer 164 Society Symposium on Research in Security and Privacy, pp. 178-194, May **(1993)**.
[30] A. D. Rubin and P. Honeyman, "Formal Methods for the Analysis of Authentication Protocols", CITI Technical Report 93-7, Center for Information Technology Integration, Dept. of Electrical Engineering and Computer Science, University of Michigan, Nov. **(1993)**.
[31] C. Meadows, "Formal Verification of Cryptographic Protocols: A Survey", Advances in Cryptology - Asiacrypt '94, LNSC 917, Springer-Verlag, pp. 133-150, **(1995)**.
[32] R . Needham and M. Schroeder. Using encryption for authentication in large network s of computers. Communication of the ACM , 21(12) :993–999, **(1978)**.
[33] V´eronique Cortier, "Verification of Security Protocols", Verification, Model Checking, and Abstract Interpretation, LORIA, CNRS, Nancy, France, Springer-Verlag Berlin Heidelberg, pp.5-13, **(2009)**.
[34] M. Abadi and M.R. Tuttle, "A Semantics for a Logic of Authentication", Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing, Montreal Canada, pp. 201-216, Aug. **(1991)**.
[35] Paul Syverson, "A logic for the analysis of cryptographic protocols", Technical Report 9305, Naval Research Laboratory, Dec. **(1989)**.
[36] L. Gong, R. Needham and R. Yahalom, "Reasoning about Belief in Cryptographic Protocols", Proceedings of the IEEE Computer Society Symposium on Security and Privacy, Oakland, California, USA, pp. 234-248, May **(1990)**.
[37] T. Newe, and T. Coffey, Formal Verification logic for hybrid security protocols, International Journal of Computer Systems, Science & Engineering, Vol.18, No.1, Jan **(2003)**, pp 17-25
[38] S. Gritzalis, D. Spinellis and P. Georgiadis, "Security Protocols over Open Networks and Distributed Systems: Formal Methods for Their Analysis, Design, and Verification", Computer Communications, Vol.22, No.8, pp.695-707, May **(1999)**.
[39] J. Millen, "CAPSL-Common Authentication Protocol Specification Language", Technical Report, the MITRE Corporation, http://www.mitre.org/research/capsl, **(1997)**.
[40] C. S. Escobar and J.Meseguer. A rewriting-based inference system for the NRL protocol analyzer and its meta-logical properties. Theoretical Computer Science , 367:162–202, **(2006)**.
[41] S. Brackin, "A HOL Extension of GNY for Automatically Analyzing Cryptographic Protocols", Proceedings of the 1996 IEEE Computer Security Foundations Workshop IX, IEEE Computer Society Press, Ireland, pp. 62-76, June **(1996)**.
[42] G. Lowe, "Breaking and Fixing the Needham-Schroeder Public-key Protocol Using FDR", in Proceedings of TACAS, pp. 147-166, Springer Verlag, **(1996)**.
[43] J. Millen and G. Denker, "MuCAPSL", DARA Information Survivability Conference and Exposition, Volume I, IEEE Computer Society, pp.238-249, **(2003)**.
[44] B. Blanchet, "Automatic verification of correspondences for security protocols", Principles of Security AND Trust - First International Conference, Volume 7215, **(2012)**.
[45] Luu Anh Tuan, "Modeling and verifying security protocols using PAT approach", Secure Software Integration and Reliability Improvement Companion (SSIRI-C), 2010 Fourth International Conference, Singapore, pp. 157-164, **(2010)**.
[46] Marian Ventuneac, Reiner Dojen, Tom Coffey, Automated Verification of Wireless Security Protocols using Layered Proving Trees, Wseas Transactions on Communications, I.2, V.5, Feb. **(2006)**.
[47] Ahmed H. Ali, Reham Abdellatif Abouhogail, Ibrahim F. Tarrad and Mohamed I. Youssef "Assessment and Comparison of Commonly used Wireless Technologies from Mobile payment Systems Perspective", International Journal of Software Engineering and Its Applications, Vol.8, No.2, Jan **(2014)**, pp.255-266.
[48] Mazen Tawfik Mohammed, Alaa Eldin Rohiem and Ali El-moghazy, "Confidentiality Enhancement of Secure Real Time Protocol", ICENCO, 29-30 Dec **(2012)**.
[49] Tian-Fu Lee, "Enhancing the security of password authenticated key agreement protocols based on chaotic maps", Information Sciences, 290, 2015, pp.63-71.
[50] The Handbook of Measuring System Design, John Wiley & Sons, Ltd, **(2005)**.
[51] Mohamed H. Abd El-Raouf, Rasha S. M. Ali, Mohammed S. Gadelrab, Construction and Remote Calibration of an Automated Resistance Measuring System, MAPAN-Journal of Metrology Society of India, **(2011)**.
[52] R.A.Dudley, N.M.Ridler, "Internet calibration direct to national measurement standards for automatic network analysers", IEEE Instrumentation and Measurement Technology Conference Budapest, Hungary, May 21-23, **(2001)**.
[53] A. Sand, H. Slinde, and Tor A. Fjeldly, "A Secure Approach to Distributed Internet-Enabled Metrology", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 56, NO. 5, OCTOBER **(2007)**.
[54] M. Desrosiersa *et.al*, "e-Calibrations: using the Internet to deliver calibration services in real time at lower cost", Radiation Physics and Chemistry 63, **(2002)**, pp. 759–763.

[55] T. Tasić, "Impact of Software and IT on Metrology", IX Symposium Industrial Electronics INDEL 2012, Banja Luka, November 01-03, **(2012)**.
[56] www.ni.com.
[57] C. S. Fraser, Bjorn Riedel, "Monitoring the thermal deformation of steel beams via vision metrology", ISPRS Journal of Photogrammetry & Remote Sensing 55, **(2000)**, pp. 268–276.
[58] M.M. Menon, R.E. Barry, A. Slotwinski, H.W. Kugel, C.H. Skinner, "Remote metrology, mapping, and motion sensing of plasma facing components using FM coherent laser radar", Fusion Engineering and Design 58 – 59, **(2001)**, pp. 495 – 498.
[59] Virtual Instrumentation Software Architecture. [Online]. Available: http://www.ni.com/visa/
[60] L. Lo Iacono, Christoph Ruland, Norbert Zisky, "Secure transfer of measurement data in open systems", Computer Standards & Interfaces 28, **(2006)**, pp. 311 – 326.
[61] A. M. de Oliveira1, Carlos Schneider 2, Gustavo Maestri, "The Remote Services Laboratory as A metrology Knowledge Management Integrator and its Impacts on Social Responsibility", XVIII IMEKO World Congress Metrology for a Sustainable Development, 17-22 Sep. **(2006)**.
[62] www.nis.sci.eg
[63] Netscape Coorporation, "SSL 3.0 Specification", http://wp.netscape.com/eng/ssl3/, accessed on 10th Feb. **(2006)**,
[64] Traceable Calibrations for Infrared Remote Sensing, PTB news.
[65] http://www.nist.gov/itl/csd/index.cfm
[66] http://www.ptb.de/index_en.html
[67] https://www.nmij.jp/english/
[68] http://www.npl.co.uk/

Author

Dr. Reham Abdellatif Abouhogail graduated from Faculty of Engineering Ain Shams University, obtained MSc with a Master of Electronics and Communications from Cairo University, obtained Ph.D from Faculty of Engineering Ain Shams University. She is now an associate professor in the National Institute for Standards, Giza, Egypt. She has 15 years of experience of research. Her area of research includes VLSI Design of Security Systems, Analysis of Security Protocols and Wireless Networks Security Systems. She has published many research papers in International journals and International conferences.