DESIGN AND ANALYSIS OF THE SECURITY ASSESSMENT FRAMEWORK FOR ACHIEVING DISCRETE SECURITY VALUES IN WIRELESS SENSOR NETWORKS

Adnan Ashraf[1], *Manzoor Hashmani*[1], *Bhawani S Chowdhry*[1, 3], *Marvi Mussadiq*[2], *Quintin Gee*[3], *Abdul Qadeer Khan Rajput*[1]

{[1]Mehran University of Engineering and Technology, [2]University of Sindh} Pakistan, [3]University of Southampton, UK} e-mail: adnanlooking@ieee.org

ABSTRACT

The paper presents a ready-to-use security assessment framework for wireless sensor networks (WSNs). The parameters in the proposed security assessment framework perform independent security assessment of WSNs and of their applications. Our proposed framework uses actual responses of the entities (such as nodes, communication link and network response) to assign numerical values for security assessment of WSNs. The method for calculating the optimal values for each security parameter of the framework is also discussed. Our proposed framework is designed to avoid unwanted impacts of the complexities of security algorithms, communication protocols and strong cryptography. Usually, the complexity of algorithms disguises the actual assessment of the WSN, but the independence of the proposed framework from these security-disguising objects makes this framework better than other assessment frameworks in terms of scalability.

Keywords **–** Wireless Sensor Network, WSN Security, Security Assessment Framework, Numerical Security Assessment

1 INTRODUCTION

In the past, security was not conceived of as a core issue during the development stages of various infrastructures. This is particularly so with the Internet. Once structures are established, it is often more difficult to integrate security than embedding security features at an early stage. It is common for security-related issues to become more complex in networking infrastructures because of massively increased number of assets in a shared environment of resources. Security specialists suggest that the security should be embedded at the start of the infrastructure development [1] [2]. Among other networks, the wireless sensor network (WSN) contains various self-organizing sensors that form a distributed, flexible network. Being without a fixed topology and distributed, the WSN becomes insecure and more vulnerable to attacks [3] [4].

978-1-4244-1643-1/08/$25.00 ©2008 IEEE

WSN is a security-fragile network and, in most applications, the use of acquired data is very significant, e.g. military monitoring, disaster recovery, bio-weapons, and emission of poisonous gases. Though the vulnerability issue is being addressed by research communities, there is also a rising demand for finding new security strategies [5] [6] [7]. In order to use these security-fragile networks for different applications in the real world, a more comprehensive, reliable, efficient and less complex security strategy needs to be developed.

The benefits of introducing new security strategies for networking are twofold. One is the protection of the existing assets of the current WSN and competitors' network technology, and the other is to help to mature the WSNs and Next Generation Networks [7] [8]. This need is more important than ever because of the popularity of short-life *ad hoc* networks. On the other hand, the security requirement of the WSN application needs to be assessed, too. Different security assessment frameworks serve theoretical or rule-based assessment of real world applications [8] [13], but fail to apply these rules to specific types of network.

In this paper, security assessment is addressed by a new approach of numerical assessment. We identify the general causes of assessment failure of WSNs by other security frameworks, and propose a new approach that is independent of assessment, and is more scalable. The design of the framework and its parameters are first introduced, followed by an analytical and mathematical representation for evaluating the security level of a WSN. Our future research will look at the greater flexibility in implementing our proposed Security Assessment Framework (SAFE) in different real environments.

2 SECURITY ISSUES IN WSNs

It is a general observation that key requirements of security and privacy (including authenticity, data access, and confidentiality) vary from one application to another. Likewise, the security features of a WSN vary depending upon the entities involved (protocols, cryptographic key distribution and management, etc.) in communication among sensors. It appears impossible to design the same

type of WSN for different types of application. Most of the time, the problem gets worse if the infrastructure is deployed without appropriate security assessment of the WSN, and of the application as well. Therefore, the use of a WSN in different applications becomes difficult [9]. This suggests that the security features of a WSN should properly address the security requirements of each application separately.

This leads us to believe that the selection of an appropriate WSN for different applications requires the best possible security assessment of the WSN, and of the application that intends to employ that WSN. Our motivation is the fact that, in spite of the advances in networks, security parameters and security tools, the desired assessment technique does not yet exist, at least in the WSN [10] [11] [12]. The challenge is to analyze and assess the security features (of the WSN), and the security requirements (of the application) in order to deploy secure WSN-based applications.

3 LITERATURE SURVEY

A few rule-based security assessment frameworks are available [10] [13] [14]. These assessment frameworks do not address the required appropriate assessment of security for both the WNS and the application [10] [14]. These established assessment frameworks are no more than process/rule-based models for implementing any security plan/framework. They follow a list of precautions and recommend the maintenance of a log of logs [12] [13] [14]. Various factors cause these rule-based/ theoretical security assessment frameworks to fail, especially in WSNs. These factors include the complex security algorithms, higher-bit encryption, hard-coded communication protocols, open system architectures, hybrid network models, and network deployment strategies [15] [16] [17] [18]. Some of these are elaborated below.

– Encryption: A few network experts observe that WSN security is hidden in developing new and complex encrypting schemes [14]. Probably they prefer an individual security concept model for mobile and *ad hoc* networks. More complex issues occur when experts deal with key interchange, distribution and management of these highly complex encrypting schemes over unreliable communication layers of WSN models. They then return to their previous energy efficient encryption schemes. (For example, when the energy issue was found to be a bigger challenge, experts changed their interest to developing smart codes) [12] [15].

– Complex algorithms: Highly complex and unbreakable encryption algorithms from ECC, AES, RAS, and others (employing 64, 128, 256, 1024, and 2048 bits) have been developed and the quest is continuing [12] [18]. Even today, encryption is neither conceived of, nor treated as, the final word for WSN security. We believe that a higher number of bits will never guarantee a permanent solution, as is clear from the history of encryption. An alternative to the call for higher bits is given by smart ECC: Elliptic Curve Cryptography. Higher bit supporters do not agree that, since the most powerful supercomputers would take thousands of years to break ECC or AES encryption, then the fear of insecurity should diminish. The cost of computation and the interlinked communication layers of the WSN will always act as a constraint on complex algorithms.

– Open systems: Another group seeks an open system security solution for WSNs as the ultimate approach [13]. Customization of security solutions gives security comfort at a personal level, but it offers a lower degree of interoperability among deployed security components/ services, it brings non-synchronization of network tools, and it delays updates among different types of interlinked WSNs. The lack of computation power in non-intelligent nodes become key constraints on open system implementation, since child sensor nodes are not designed to make crucial decisions.

– Hybrid models: Like other networks, sensor networks are mobile, *ad hoc* and sometimes disparate hybrid models [16]. In these models, the trust domain among sensor nodes can be rare or highly complex to achieve.

– Sensor deployment: The random deployment of wireless sensors by an airplane, in an enemy or mountainous area, for real-time disaster detection and recovery operations, is also an issue. There are other questions that cannot be numerically answered by these rule-based or theoretical frameworks. Such questions are: How strong is the security of a network when it is simulated? What are the network security requirements of the application? How strong is the security of a network when it is deployed? What is the security status after full deployment? What are the effects after any new security patch/updates? What is the overall security strength after updates? What are the measurable assessment analysis components? What is the segmented strength of the WSN after breakdowns? What is the security status of the network after buying solution 'A' instead of 'B', and *vice versa*? Existing frameworks require dozens of pages and several disks for archiving logs to answer these questions.

4 OUR PROPOSED SECURITY ASSESSMENT FRAMEWORK

To address security-related issues in network assessment, we propose a new framework. Our framework is unique within existing, rule-based, security assessment strategies [16] [17] [18]. It enables the security quantification of both the WSN and the application to be performed. The proposed framework determines numeric values for the security requirements (of the application), and security features (of the WSN). These values are used to evaluate the security strength of both the WNS and the application. Another use of this value is to label the level the security such as 'low',

'moderate', and 'high'. Further, this framework can be used to set limits for these security levels. Refer to the Figure 1.

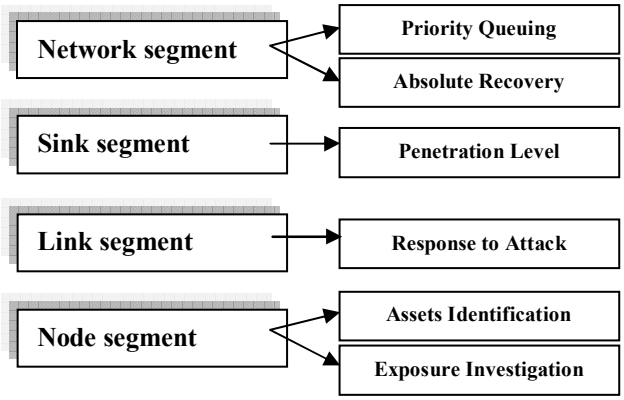


Figure 1. Proposed security assessment framework

5 STRUCTURAL AND FUNCTIONAL ANALYSIS

The proposed framework is distributed in four segments. Each segment has a different number of customized parameters (Figure 1) to determine the security requirements. These security requirements are then used to match the core security features [8].

The values of each parameter range from 0.0 to 1.0. The value is calculated using different mathematical methods (Table 1).

Table 1. Allocation of Values in the Security Assessment Framework

Segment	Parameter Name	Score	Method
Network	Priority queuing	0<x<1	0.2 (signed)
Network	Absolute recovery	0<x<1	SR/RR
Sink	Penetration level	0<x<1	SL–(CL/SL)
Link	Response to attack	0 or 1	Binary value
Node	Assets Identification	0<x<1	(TN–CN)/TN
Node	Exposure investigation	0<x<1	N nodes/sq. Unit

Network segment

Network segment is the first segment of the proposed framework. It has two security assessment parameters (Priority Queuing and Absolute Recovery) whose values give the information about other parameters for any WSN or application.

– Priority Queuing (PQ): PQ represents the status of disruption or destruction of any other parameter in the framework. It indicates a negative impact if the value of any other parameter reaches the variance limit in a certain time frame. In addition, such a parameter is listed as vulnerable and moved to the top of a priority list to be maintained for this purpose. This priority list is used to identify vulnerabilities as well as to address the vulnerability of the WSN.

Determining PQ: If the variance of any parameter, except the prioritization parameter, is observed to be greater than a given threshold, then that parameter is included in the priority list. Each of the entries listed reduces the WSN security by 0.2. The default value of the prioritization parameter is 1.0 in our framework; thus each decrement increases the vulnerability of the WSN. The variance value of 5 is observed in our test environment. The threshold of variance will vary depending on the type of WSN or WSN application.

– Absolute Recovery (AR): AR represents the recovery status of the WSN from any existing threat. It depends on the number of recovery requests and successful recoveries from attacks on the WSN.

Determining AR: The value of the parameter is calculated as the ratio of the number of successful recoveries to number of requests made for such recoveries. The default value of this parameter is 1.0. It is achieved by assuming all requests are recovered. The zero (0.0) value indicates that there are a negligible number of successful recoveries against the recovery requests and the WSN is vulnerable. The number is rounded off to one decimal place (Equation 1).

$$AR = \frac{SR}{RR} \qquad (1)$$

where, AR is Absolute Recovery
SR is number of Successful Recoveries
RR is number of Requests for Recoveries

Sink Segment

This segment contains one security assessment parameter (Penetration Level) whose values help determine the intensity of the damage to a WSN or an application.

– Penetration Level (PL): PL represents the strength of the host WSN or application to resist the damage occurring in any segment (Network, Sink, Link and Node) against the security layers. The security layers include encryption, password authentication, establishment of trust domain, certificate exchange, and sender verification.

Determining PL: For the reliability in the assessment procedure, we determine two values to calculate the PL parameter. These values are calculated for available security layers in the WSN or application.

One value (Secure Layer) is calculated as optimal value of the parameter. It is achieved by simulating the WSN in favourable conditions in a test environment. The other value (Compromising Layer) represents the number of secure layers that compromise the security of the WSN. The value is achieved by simulating the WSN in a real environment.

Assume an application-specific WSN. It is deployed with n secure layers, such that $n \geq 2$. If m threats (m is application-specific) pass through some security layers then those layers are called compromising layers. PL is now calculated, rounding as before (Equation 2).

$$PL = SL - \frac{CL}{SL} \quad (2)$$

where PL is Level of threat/attack Penetration
SL is number of Secure Layers
CL is number of Compromising Layers

Link Segment

This segment of our framework contains one security assessment parameter (Response to Attacks). It gives a binary value of effectiveness of the defence of the WSN to some instance.

– Response to Attacks (R2A): Usually, this parameter is important in those WSNs that have the support of a resource- rich and strongly defensive base node. It is zero in WSNs that are deployed purely on a temporary basis.

Determining R2A: This parameter is calculated across two time frames. The two instants are i) upon detection of an attack (resource node makes sure of attack), and ii) upon generating any sort of reaction by that node. If all attacks that are detected at time (T_0) are responded to by time (T_1) by the defence of WSN, then the parameter's score is 1. If any attack is not responded to within the time set by the WSN designer, then the parameter's score is 0.

Node Segment

This segment comprises two security assessment parameters (Assets Identification, and Exposure Investigation). It gives information about possession and assurance of node-to-node point communication.

– Assets Identification (AID): This parameter identifies the wireless sensor nodes that are cooperative. In *ad hoc* networks, every signed (secure) transmission adds value to the asset of the factor. Each node is allowed to communicate towards the immediate head node of that group only. Therefore, the number of reliable nodes is reported to the head of the each group. Similarly, information is passed to the sink that is considered as wireless sensor nodes.

Determining AID: In a network of 100 nodes (TN) the value of the parameter is 1 if all nodes respond as assets, i.e. all these nodes meet all security steps implanted in the WSN and WSN application. The AID is calculated as shown below (Equation 3).

$$AID = \frac{TN - CN}{TN} \quad (3)$$

where AID is Assets Identification
TN is total number of Communication Nodes
CN is number of Compromising Nodes

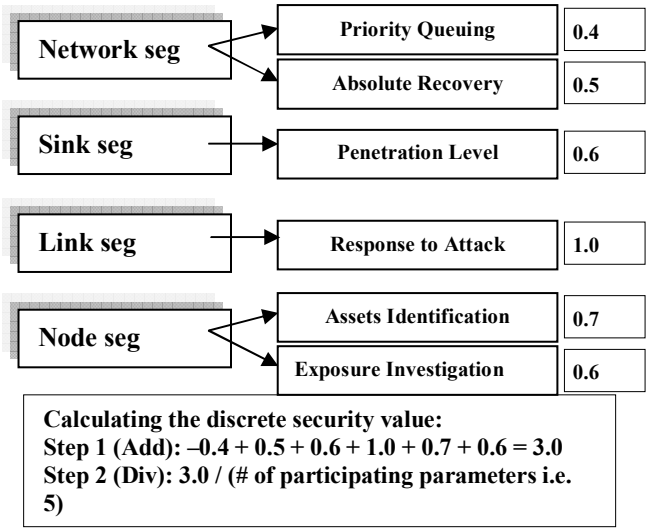
– Exposure Investigation (EI): The child leaves (sensor nodes) are inward-facing components of a WSN. EI determines how much exposure is being considered as direct exposure to the world. There can be some secret agents/nodes in a futuristic WSN model to spy on nodes of one's own WSN). To count only their participation in the security assessment our framework does not assume an intermediary sink as a node. Ignoring these sinks keeps this parameter independent of the asset identification parameter.

Determining EI: Suppose n nodes per square-unit (according to the requirement of the application) are placed in a WSN or subgroup/cluster of a WSN. Each node communicates across a range of a few metres. If one node is a sink, and 19 are children, then the Exposure Investigation has the value 1 for the WSN or subgroup/cluster of this WSN. The recommendations for the number of communicating sensors nodes in that area must be standardized first by reviewing the potential of the WSN and requirement of the WSN application.

6 PLAN FOR REAL WORLD EVALUATION OF THE FRAMEWORK

An example of one test result is shown below.

Figure 2. An example of discrete values in our proposed framework



As an extension to the present work, we are implementing our proposed security assessment framework (SAFE) in different real environments, e.g. military operations, disaster recovery in earthquake areas, and in flood disaster areas. We shall then compare these results with various organizations to determine the security level of WSN in different WSN applications.

7 CONCLUSIONS

In this paper, we identified the reasons why security assessment carried out by existing frameworks fails, particularly in WSNs and their applications. From this, we proposed a new framework for the security assessment of a WSN and its applications.

The proposed framework is implemented by allocating numeric values to the security requirements of the WSN application. Similarly, it quantifies the security features of a WSN.

We observe that the parameters and their values are independent of complex processes of cryptography. The method avoids any assessment impact due to the complex security algorithms of WSN. Further, we discussed the parameters of the proposed framework analytically and presented the basic mathematical operations to calculate them. The five indicated parameters of the framework collaborate to provide a final value as a net assessment. This single value represents the level or strength of the security made available by a WSN. The value of security is assumed by our proposed framework to range from 0.0 to 1.0.

8 ACKNOWLEDGEMENTS

This project is funded by the Ministry of Science and Technology (MoST), Pakistan in the Mehran University of Engineering and Technology, Pakistan.

REFERENCES

[1] Haenselmann, T. (2006) An FDL'ed Textbook on Sensor Networks, April 2006, pp 1-67, 72-100, 119-122, 149, 151-164. Available online from www.informatik.uni-mannheim.de/~haensel/sn_book/

[2] Arain, A.A., Mussadiq, M., and Hashmani, M. (2006) An analytical revelation for a safer network perimeter security, available on the CD of the Proceedings of International Conference on Information and Networking 2006 (ICOIN2006), Sendai, Japan, PaperID: icoin-2006-969.

[3] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) A survey on sensor networks, *IEEE Communications Magazine*, 40(8) pp 102-114.

[4] Gupta, S., Zheng, R., Cheng, A.M.K. (2007) ANDES: an Anomaly Detection System for Wireless Sensor Networks, in Proceedings of MASS 2007, IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007, pp 1-9.X

[5] Ricadela, A. (2005) Sensors everywhere, information week.com/ stories, January 24, 2005.

[6] McMillan, R. (2007) Black Hat: Researchers say forensics software can be hacked, IDG News Service, July 25, 2007.

[7] Wood, A.D., and Stankovic, J.A. (2002) Denial of service in sensors networks, *Computer*, 35(10) pp 54-62.

[8] Chong, C-Y., and Kumar, S.P. (2003) Sensor networks: evolution, opportunities, and challenges, *Proceedings of the IEEE*, 91(8), pp 1247-1256.

[9] Karlof, C., and Wagner, D. (2003) Secure routing in wireless sensor networks: Attacks and counter measures, *Ad Hoc Networks*, 1(2-3) pp 293-315, Elsevier.

[10] Undercoffer, J., Avancha, S., Joshi A., and Pinkston, J. (2002) Security for sensor networks, CADIP Research Symposium, Department of CS and EE, University of Maryland, Baltimore, Maryland, USA.

[11] Denning, D. (1982) *Cryptography and data security*, Addison Wesley.

[12] Kulik, J., Rabiner, W., and Balakrishnan, H. (1999) Adaptive protocols for information dissemination in wireless sensor networks, in Proceedings of 5th ACM/ IEEE-MOBICOM'99 conference.

[13] Park, S., Savvides, A., and Srivastava, M.B. (2000) SensorSim: A simulation framework for sensor networks, in Proceedings of the 3rd ACM international workshop on modeling, analysis and simulation of wireless and mobile systems, Boston, Massachusetts, USA.

[14] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E. (2002) SPINS: Security protocols for sensor networks, *Wireless Networks*, 8(5) pp 521-534.

[15] Kaplantzis, S. (2006) Security models for wireless sensor networks, Conversion report, Monash University, 20 March 2006.

[16] Czarlinska, A., and Kundur, D. (2006) Distributed actuation attacks in wireless sensor networks: Implications and countermeasures, in Proceedings of the 2nd IEEE workshop on dependability and security in sensor networks and systems, DSSNS 2006.

[17] Sabbah, E., Majeed, A., Kang, K-D., Liu, K., and Abu-Ghazaleh, N. (2006) An application-driven perspective on wireless sensor network security, in Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks, Torromolinos, Spain.

[18] Roman, R., Zhou, J., Lopez, J. (2005) On the security of wireless sensor networks, in Proceedings of the international conference on computational science and its applications, ICCSA-2005, LNCS 3482, pp 681-690.

Intentional Blank Page