Improved Classification and Framework Association of Security Vulnerability, Threats and Attacks in Wireless Sensor Networks

Adnan Ashraf[1], AbdulRauf Rajput[1], Marvie Mussadiq[2], Bhawani S. Chowdhry[3], and Manzoor Hashmani[4]

[1] CREST Research Scholars, Mehran UET, Pakistan
[2] IT Consultant, Xevious Co.
[3] Fellow-Postdoc, Southampton University-UK
[4] Foreign Faculty Professor, Mehran UET
adnanlooking@ieee.org

Abstract. Security of wireless sensor network (WSN) remained an open research area throughout the current decade. New research and developments seems protecting sensor networks from various security threats but at the same time raise many questions, confusions and conflicts regarding their own viability. Such viability issues become major hindrances in security assessment of WSNs against posed security threats. This results in less reliable sensor networks and applications. In our strong opinion, there are two root-causes of this problem; 1) a comprehensive list of security threats is overlooked as researchers' work appear limited in classification of security threats and, 2) security threats are not associated with security frameworks. In this paper, we perform classification of security threats comprehensively whereas, associating these threats to a security framework; we lead in this direction. We find that specifically to assess the impact of these threats.

Keywords: WSN security, Security vulnerability, Threats and Attacks, Security Framework.

1 Introduction

The focus of this paper is the long standing open problem of developing some approach for achieving maximum security in wireless sensor networks, particularly an approach to address the fundamental security objectives that vary in applications. Such varying security objectives of applications do not allow a single security approach to best-fit another application. This is because of security objectives of an application in a sensor network could be mirrored exactly in another application depending upon the interests to be sought from that network [1] [2]. Hence, a most preferable security objective in an application can be ranked as moderated in another type of application, such as sensor-ID (source of information) in military operations and in smart-parking.

Ranking of security objectives should be carefully performed by first analyzing security threats posed to WSN and its application. In this paper, first we compile a

R. Mehmood et al. (Eds.): EuropeComm 2009, LNICST 16, pp. 269–274, 2009.

comprehensive list of security threats. Then, by classifying the security threats we associate them analytically with security assessment framework [3] [4]. We observe that such work has not been done before, in this way.

2 Related Work

Study of security vulnerability, threat and attack (VTA) aids in the development of countermeasures and security frameworks of wireless sensor network. Here we briefly review the related work, at-present issues and motivations. We observe a relatively little work in the area of classification of security threats. In the existing partial work, most of the researchers used security terms interchangeably, such as vulnerability, attacks and threats [5] [6] [7]. Using alternate terms may create problems and mislead the prospective researchers. It is not logical to use these terms interchangeably because of wide differences in these terms. In this paper, we differentiate these terms for research community for sake of research in right directions and then we comprehend a list of security threats for wireless sensor networks.

From literature, we observe that classification of WSN is based on features and mechanism that WSN exhibits today. For example, distance to base station (single or multi hops), data dependency (aggregating or non-aggregating), deployment (deterministic or dynamic), control schemes (self or non-self configurable) and application domain (features dependent) [8] [9] [10]. In a WSN, the exposure of features is application specific therefore a WSN should be selected for an application by security and reliability, instead of features, that it offers. We present here a revised classification of security VTA.

The most recent and maximum work in classification of security models of WSNs appeared by S., Kaplantzis [9] in 2006. While interchanging terms of security threats, vulnerability and attacks in WSN, the researcher has dispersed many of those in network layers [12]. Contrary to the classic work in WSN security we propose an analytical association of security threats with security framework.

3 Classification Needs of Security VTAs in WSN

It's obvious from through literature survey that WSN still experiences classical (bit modified for WSN) approaches of traditional wireless or wired networks. Probably, this is due to the likely names of attacks that are present in classical wireless networks. On the contrary, VTA (vulnerability, threat and attack) have quite different impact in the WSN due to its unique in-network communication processing. Hence, classification of VTA and development of security frameworks should be revisited to counter such security VTA.

In this paper, our approach for classification and association of security VTA is proposed to remodel application-specific WSNs that may fulfill their missions in timely manner, in hostile environments.

3.1 Security VTAs

A profound study leads to differentiate among security related terms that are being interchangeably used among researchers in published literature (discussed in section 2). In

order to eliminate these ambiguities from the future literature we compile a list of vulnerabilities, threats and attacks in the light of standard definitions.

The *vulnerability* is a weak-point in the system or a network that may be exploited, whereas a *threat* is considered as an external or internal influence that may exploit the *vulnerability* (weak-point). An *attack* is the occurrence of a *threat*, causes an unwanted event to be occurred in a system such as data steal, denial of service, sniffing, spoofing, etc [11] [13][14]. An *attack* can also be termed as an *exposure* in a system.

Thinking WSN, for example, the *wireless medium* is prone to exposure or attack and it's a known vulnerability. This vulnerability may be (or may not be) exploited depending upon the nature of WSN environment. Any object blocking this communication medium from responding shall be considered as a *threat* under definition of external influence. Similarly, if any inherent feature (or circuitry) causes unwanted delay of communication signals it'll also be a *threat*.

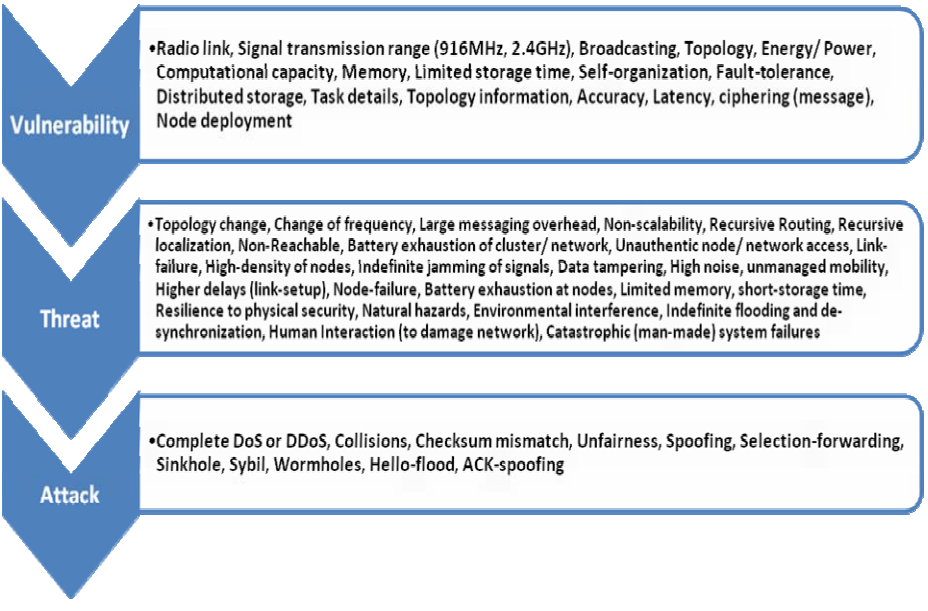

Fig. 1. A general view of vulnerability, threats and attacks in WSNs

At preliminary stages as the threat and the losses caused by such threats are unknown therefore, threats are usually considered as 'security threats'. Therefore, we comprehend a list of vulnerability, threats and attacks found in WSN in Fig 1. Concluding this section we observe that differentiating vulnerabilities, security threats and attacks resolves the terminology conflict. In the next section we classify the *security threats* while associating them to security framework.

3.2 Re-classification of Security Threats Using Security Assessment Framework

Usually, security VTAs are classified as physical-threat, accidental-error, natural, man-made, unauthorized access, malicious-user, etc. It is notable that if traditional

ciphering, topology, routing and security schemes are not appropriate for WSN then how can a traditional way of security classification be appropriate for WSN? We take this opportunity first to classify the security threats using security assessment framework [3] [4] in table 1.

Table 1. Classification and Association of Security VTAs with Discrete Security Assessment Framework

NETWORK	*Vulnerability:* Average energy exhaustion (network), low computational capacity, limited network storage time, self-organization, fault-tolerance level, distributed storage, task details, simple ciphering, and node deployment
	Threat: Topology change, change of frequency, large messaging overhead, non-scalability, recursive routing, system failures
	Attack: Complete DoS or DDoS
LINK	*Vulnerability*: Radio link, Signal transmission range (916MHz, 2.4GHz), Broadcasting, Topology-less infrastructure, Ad hoc Topology information
	Threat: Non-Reachable, Link-failure, High-density of nodes, Indefinite jamming of signals, Data tampering, High noise, unmanaged mobility, Higher delays (link-setup)
	Attack: Collision or checksum mismatch, Unfairness, Spoofing, Sybil, Wormholes, Hello-flood, ACK-spoofing
SINK	*Vulnerability*: Energy exhaustion @ Sink, Task details
	Threat: Unauthorized access
	Attack: Sinkhole, de-synchronization
NODE	*Vulnerability*: Energy exhaustion @ node, Resilience to physical security, Limited memory, short-storage time
	Threat: Node failure, Recursive localization, Indefinite flooding
	Attacks: Selective Forwarding
OTHERS	*Vulnerability*: ---
	Threat: Natural hazards, Environmental interference, Human Interaction (to damage network), Catastrophic (man-made)
	Attack: Nil

4 Security VTAs

This paper performs a critical analysis of available literature on security classification. Criticizing the trend of interchanging terms for security VTAs, it elaborates the possible losses of this trend to research.

A comprehensive list of security VTAs is helpful to model new security protocols, frameworks, as well as to assess the existing security solutions. It allows better understanding with security issues in WSN. Customization of VTA list can also be done as

per demand of an application. Similarly, any low priority constraint, threat or attack can be eliminated from the VTA list for a specific type of WSN.

Administrators of WSN will then, have a simplified management of network. Renewing policy is considered as energy hungry process in WSN. By classifying VTA, any layer of network under attack can be known and then revitalized using selective forwarding for policy renewing or countermeasures.

Distribution of security VTAs is done by assessing impact of each entry in the list and, taking into account, the infected area that could be involved in sharing losses in a WSN. Furthermore, confidentiality as task details (at node) is assumed as network asset. This ensures an uncompromised security strategy used throughout our work.

In short, we can be able to distinguish the presence of any VTA component in security layers of WSN using the assessment framework. From an application s' perspective, any vulnerability, threat or attack can be subjugated if any network layer or segment of the framework is protected by that VTA component. This is the real benefit of associating security VTA to a security framework.

5 Conclusion and Future Work

This paper differentiates among concepts of security vulnerability, threat and attack by redefining them from WSN s' perspective. On the basis of this differentiation we are able to comprehend a list of security VTAs. It helps to eliminate ambiguities regarding security literature on VTAs. Then, by examining each of VTAs we associate it with a security assessment framework for analysis. Impact of these security VTAs on a sensor network depends on various factors and is an open research issue. Also, we plan to review this approach with other security frameworks, in future to achieve good assessment in WSN applications.

References

1. Zia, T., Zomaya, A.: A security Framework for Wireless Sensor Networks. In: SAS 2006 – IEEE Sensors Application Symposium, Houston, Texas, USA, February 7-9 (2006)
2. Zou, K.C.Y.: Uncertainty-aware and Coverage-oriented Deployment for Sensor Networks. Journal of Parallel and Distributed Computing 64(7), 788–798 (2004)
3. Ashraf, A., Hashmani, M., Mussadiq, M., Chowdhry, B.S., et al.: A Pretty Safe Strategy for Analyzing Discrete Security Assessment Framework in Wireless Sensor Networks, Communications in Computer and Information Science, November 14, 2008. Book of Wireless Networks, Information Processing and Systems, vol. 20, pp. 445–448. Springer, Heidelberg (2008)
4. Ashraf, A., Hashmani, M., Mussadiq, M., Chowdhry, B.S.: Design and Analysis of the Security Assessment Framework for Achieving Discrete Security Values in Wireless Sensor Networks, Electrical and Computer Engineering, 2008. In: CCECE 2008. Canadian Conference on Electrical and Computer Engineering, May 4-7, pp. 855–860 (2008)
5. Ilyas, M., Mahgoub, I.: Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems (2004) ISBN 0-8493-1968-4, TK7872.D48.H36
6. Muraleedharan, R., Osadciw, L.A.: Jamming Attack Detection and Countermeasures. In: Wireless Sensor Network Using Ant System, Department of Electrical Engineering and Computer Science, pp. 13244–11240. Syracuse University, Syracuse

7. Crespo, R.G.: Slides on Mobile Systems Security, WSN Security Threats', Copyright Departmento de Engenharia, Electrotecnica, e de Computadores (Fall 2006)
8. Akojwar, S.G., Patrikar, R.M.: Classification Techniques with Cooperative Routing for Industrial Wireless Sensor Networks. In: Advances in Computer and Information Sciences and Engineering, pp. 503–508. Springer, Netherlands (2008)
9. Kaplantzis, S., Mani, N.: A Study on Classification Techniques for Network Intrusion Detection. In: Proceedings of the IASTED International Conference on Networks and Communication Systems, year of publication (2006)
10. Kim, Y., Jeong, S., Kim, D.: A GMM-Based Target Classification Scheme for a Node in Wireless Sensor Networks. IEICE Transactions on Communications E91-B(11), 3544–3551 (2008); doi:10.1093/ietcom/e91-b.11.3544, The Institute of Electronics, Information and Communication Engineers
11. Kim, D.S., Shazzad, K.M., Park, J.S.: A Framework of Survivability Model for Wireless Sensor Network. In: Proceedings of the First International Conference on Availability, Reliability and Security, pp. 515–522 (2006) ISBN:0-7695-2567-9
12. Kaplantzis, S., Mani, N.: Security Models of Wireless Sensor Networks, final review report for PhD (2007), `http://users.monash.edu.au/~skap3/`
13. Barnum, S., Gegick, M.: Defense in Depth, pp. 2005–2009. Cigital, Inc., on 2005-09-13, Copyright (2005)
14. The Living Dictionary, Series of Longman Dictionary of Contemporary English, Copyright Pearsons Education (2008)