SNR Based Digital Estimation of Security in Wireless Sensor Networks

Adnan Ashraf[1], AbdulRauf Rajput[1], Marvie Mussadiq[2], B.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 in wireless sensor networks (WSNs) is usually thought as privacy, auditing, intrusion detection and protection. In general, the quality of signal processing is considered as issue of middleware layers. The higher values of *signal to noise ratio* (SNR) are vital for target detection and estimation which is the most critical objective of WSN. Despite of the fact that SNR has a significant impact on objectives of WSN, not much investigation is found in literature about SNR and its security impact on such networks. The entire WSN can be rendered as useless due to SNR degradation and therefore, SNR is a prevailing security threat in WSNs. In the light of modern concepts of security, the safety should accompany the availability, scalability, efficiency and the quality parameters of inter-node communication. We show that SNR can identify suspicious activities which can exploit the performance and quality of communication in a sensor network. Also, by varying range of transmission radii and observing its impact on SNR we demonstrate that SNR-values, SNR-variance and pre-defined network threshold of SNR-variance, together can be useful in security assessment of WSN.

Keywords: Security Assessment, Digital Estimation, Signal to Noise Ratio or SNR, Wireless Sensor Network.

1 Introduction

Generally, security in network administrators' dictionaries is ranked as low, moderate and high in networks. Traditionally, these levels assume their base on security policies or descriptive rules. When requirements of these levels vary from one network application to other then there is a a common practice to understand the rule, and decide whether to apply that rule or not [1]. For example, an inventory monitoring application requires a different security level than a missile monitoring application. Different will be the security levels in the military monitoring applications during the time of war and peace. Similarly, the different levels of WSN security are suggested in these applications of physical world [2].

R. Mehmood et al. (Eds.): EuropeComm 2009, LNICST 16, pp. 35–45, 2009.

Wireless sensor network is being predicted as a pathway to the *smart network environments* (SNEs). In SNEs information resources like notebooks, i-phones and intelligent thin-clients can be replaced by intelligent sensors tied up with human fingertips. Security is still an obstacle in commercial deployments of WSN. In a WSN, the *target sensing* requires various sensors to capture different signals from different applications of the real world [3] [4]. The quality of signal is monitored by SNR values being a fundamental factor in event detection and target estimation. When signals travel from source to destination then SNR decreases with the distance [5] [6]. The entire WSN can be rendered as useless by SNR degradation and therefore, SNR is assumed as a threat for WSN security.

In this paper, we observe the SNR impact on WSN security. In our work, the impact on WSN security is calculated using discrete security assessment framework [7] [8]. We show that SNR values contribute to assess the security of a sensor network. By varying range of transmission radii and observing its impact on SNR, our simulation shows that the average, variance and threshold of SNR is useful to assess the WSN for a desired level of security. The proposed combinations of SNR based values are helpful to know the presence of such suspicious activities that may exploit the signal processing capabilities of a sensor network.

2 Problem Formulation

Various frameworks have been developed to achieve secure and efficient routing along good throughput for wireless sensor networks. High throughput does not guarantee noise free signals. Knowing that noisy signals is a threat to communication, every network tends to own some pre-defined threshold figures of signaling quality essential to achieve network objectives. Hence increasing noise is a threat to sensors' intercommunication it is imperative to know that 'how much noise a system may accept to avoid the state of *compromised security*'.

One idea to overcome this limitation is to take an optimal value of SNR. In other words, this SNR-value represents the ground capabilities of signal processing being exercised in a sensor network. No specific literature is available on SNR based security computation of WSN as security frameworks did not address this issue before. We observe by simulating a WSN and diffusing it with attacks that SNR never goes optimal. Therefore, we approach variance of SNR rather than observing SNR-threshold only. The SNR-threshold is the contour describing the maximum capabilities of signal processing that a sensor network experiences. We find our proposal of SNR-variance capable to identify odd changes in the network easily.

Traditional way of observing SNR values burdens the storage of *base station* (BS) or sink node where, every value is kept intact in order to monitor the network history [9]. In fact, every value of SNR is not important to record due to limitations in the processes of topology-building, routing-selection and memory-refreshing in a WSN. Consequently, the network behavior may dramatically change.

Consider a case, where SNR-value at one point is optimal and the change of topology suddenly routes the traffic through a noisy channel. In the next point of time, assume that WSN being a self-organized network recovers the situation fortunately, and transmits proceeding packets through a good channel. In this situation, we will

not be in worry of storing SNR-values in memory of *base station* (BS). The challenge to compute the security impact for this state of network at any point of time is vital for monitoring purposes. One motive of our work is to address this challenge and analyze the security impact of such a situation on security of WSN.

One method of improving the quality of sensed value is the dense deployment of sensors. In dense deployment, many sensors are placed as close to the target as possible. This also increases the number of opportunities for the line-of-sight observations essential for accurate range estimations and SNR is improves evidently. In this case, the accurate estimation is responsibility of the algorithm used for that purpose, and this would be a big challenge.

Another way to improve reliability of network communication is to deploy sensors with enough density for multiple sensed values to be aggregated and filtered at cluster heads or at some intermediary point. The later demands efficient algorithms for distributed computations, efficient use of node memory and concise reports routed towards *base station* (BS) or sink node for estimation [10][11][12]. In our literature survey the solutions of these challenges is discussed as priority objective.

3 Literature Survey

WSNs consist of tiny nodes with low computation power and low energy resources thrown in unattended environment. When networks are adaptive with environment then the deployment part observes complex management which raises security risks in WSNs.

With the advancement of application areas, the security of WSN has been seriously questioned. The impact and nature of attacks vary among application-specific WSNs and raise the demand of uncompromised security even higher. The total security becomes utmost desire of WSN-applications due to self organizing nature, topology less infrastructure, deployment in hostile environment, limited energy, less storage and low power of computation. The existing security schemes, protocols, ciphering technologies are descriptive (rule or log based) security models and do not provide the total security in sensor networks. Shaping an optimized security is still a challenge in WSN based applications.

Many models and security frameworks have been proposed for sensing, target ranging or estimation, data aggregating, deployment mechanisms, efficient routings [5][6][10]. Some of these consider energy-levels of the network as a base of networks' strength. In a strong opinion of the majority researchers there are many network modalities that add up to the security of a network. Indeed, the problem is; how to estimate impact of each network modality on the security strength of a WSN? We find such assessment framework literature already proposed by Arain [7] [8].

David & Deborah [10] introduced a routing scheme (rumor) for power cost reduction and allow for queries to be delivered to events in the networks. This scheme builds a tradeoff between setup overhead and delivery reliability. As it is not concerned with security of the sensor network therefore, the reliability of occurrence of events is unsure.

Md & Choong [11] proposed the adoption of a probabilistic secrete sharing protocols between two nodes which acknowledge each other; they incorporate these

secretes with bidirectional verification and multi-path routing to multiple sink nodes to defense against attack.

Antonio et al [12] gave optimal power savings based on a small number of feedback bits. In such cases, an unwanted low power state of the network, during signal transmission or receiving causes the SNR degrading as an ultimate threat for WSN objectives.

Rajani [13] suggested a cross layer protocol design to detect the attack imposed by malicious node. He analyzed the attack using swarm intelligence algorithm, and by adding influence algorithm he improve the performance. Here again, the network performance is evaluated on the basis of average percentage of threat detection and energy consumption.

Rajani & Dr. Lisa [14] proposed novel avoiding method for sensor networks under jamming attack by using evolutionary algorithm. The performance parameters such as hops, energy, distance, packet loss, SNR, BER and packet delivery influences the decision taken in anti-Jamming techniques. The security assessment of this approach in WSN is still missing part of the research [15] [16] [17].

Arain [8] suggests the discrete security assessment framework for WSN security using network modalities of the applications' concern. Therefore, in this paper, we demonstrate that SNR based digital estimation of security of a WSN using SNR is possible in the *Discrete Security Assessment FramEwork* (DSAFE).

4 Security Estimation of Wireless Sensor Networks

Literature survey reveals that network applications demand security with highly scalable, efficient, intelligent and robust sensor environments. In addition to these security demands there exist different real world applications facing different security threats and therefore require different security levels from a WSN. Therefore, our objective of doing security estimation of a WSN is very critical for those network applications which are aimed for life saving and mission critical applications [18] [19] [20] [21]. Once, knowing the security capabilities of various WSNs a network application can choose the one that fulfills its security requirements optimally. For estimating security of WSN we worked with discrete security framework (DSAFE) which performs digital estimation of the network.

For the sake of continuity and interest of readers we give a brief introduction of digital estimation.

4.1 Theory of Digital Estimation of Security

The security defined by Arain [8] can be stated as *a set of tools and techniques for protecting assets of wireless sensor networks*. This protection is meant for all resources, hardware, processes and applications at some advanced level. Also, the author indicates that an attack is occurred in discrete manner such as damaging individual assets of a network whereas traditional security models and frameworks provide descriptive policies for security. This makes sensor networks less efficient to security threats [22] [23] [24] [25].

Indeed, we find that the policy/rule-based approaches of performing security assessment provide qualitative estimations only. These qualitative approaches are not helpful in determining those network segments having weak defense or kind of vulnerabilities. In order to develop an intelligent and adaptive network security protection system the quantitative or digital estimation of WSN security is very helpful. Such framework of digital estimation is already extracted, as [7] in recent past as shown in Table 1.

Table 1. Digital Estimation of Security using Discrete Security Assessment Framework

Segment	Parameter Name	Score	Precision (1-digit)
Network	Priority Queuing	0≤x≤1	0.2 (signed)
	Absolute Recovery		Successful Recovery ÷ Recovery Request
Sink	Penetration Level		Secure Layer- (Compromised Layer ÷ Secure Layer)
Link	Response to Attack		'0' or '1' known as R2A
Node	Assets Identification		(Total Nodes – Compromised Nodes) ÷ Total Nodes
	Exposure Investigation		N nodes/ Sq. Unit
Note: All values to be rounded-off to zero decimal points. The precision is removed as error.			

Using the figures in table 1, one can estimate the security strength of a given WSN in discrete fashion. It was then, followed by its evaluation strategies [9]. The discussion of evaluation strategies of D-SAFE is beyond the scope of this paper.

4.2 SNR-Based Digital Estimation of WSN

Though, many network modalities do exist for security estimation but this paper uses *signal to noise ratio* in simulations to know, merely security impact of SNR. In fact, the trend of ignoring SNR-values encouraged us to evaluate impact of SNR in WSN-security. In our strong opinion, doing digital estimation of WSN-security using SNR we may achieve following benefits.

- Controlled security level as per applications' requirements
- Development of an *intelligent security control* to work with some proactive value of network parameters
- On-demand network isolation for privacy and confidentiality from adversary nodes
- Planning of early maintenance to avoid communication-losses to assets of network and of application.
- Identification of fault in communication parameters in a WSN

In simulation, we use methodology of *Discrete-Security Assessment Framework* (D-SAFE) and a WSN simulator (i.e. JSIM). We simulate a WSN comprising 6-nodes in JSIM environment. The basic WSN model contains two target nodes for event or target sensing and broadcasting them to the next layer of 3 sensor nodes using two-hope and one-hop transmission respectively. The optimal hop-cost is also given for each node in the Fig 1. The sensing nodes are intermediate path to transport data from target node to the sink node and vice-versa.

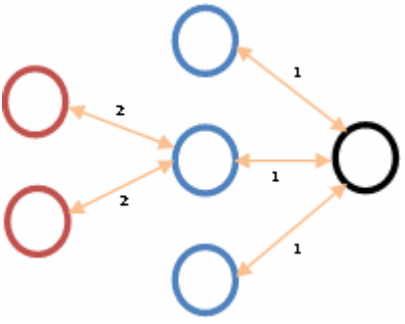


Fig. 1. Column-wise (L-R): Single (sink) node, three (sensing) nodes and two (target) nodes

Now, information like node count, SNR-values, number of hopes, data-packet size, total packet transmission time, packet loss, probability of number and type of attacks, window size and throughput is achieved from the WSN.

Referring to Fig 2, we observer that traditionally SNR values for a transmission cycle are obtained and aggregated at sinks. This indeed, burdens the limited memory resources of a wireless sensor network. Also, the recursive operations of aggregating SNR-values are not energy efficient for WSN. On the contrary, the SNR-values can be useful for real-time security estimation of sensor networks using D-SAFE.

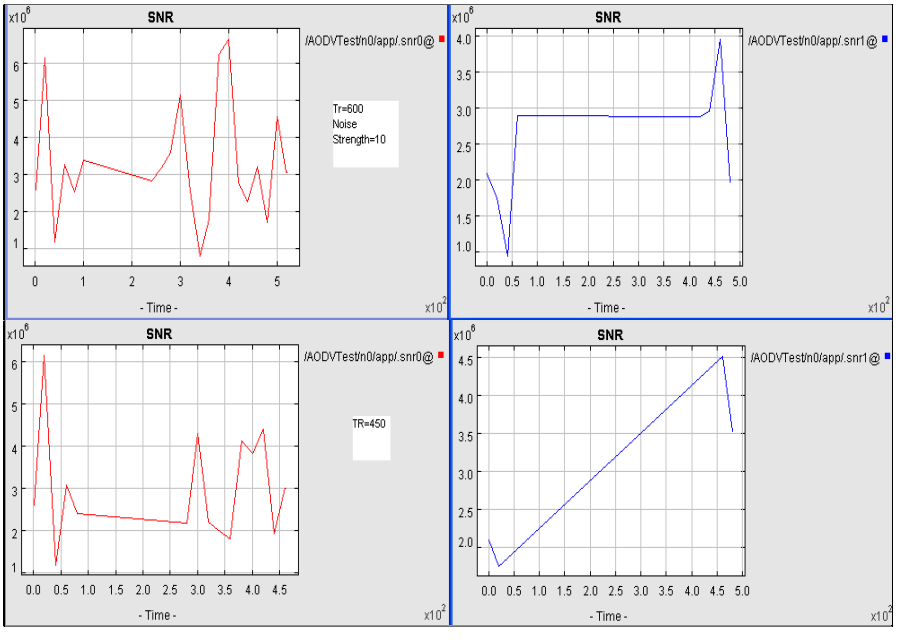
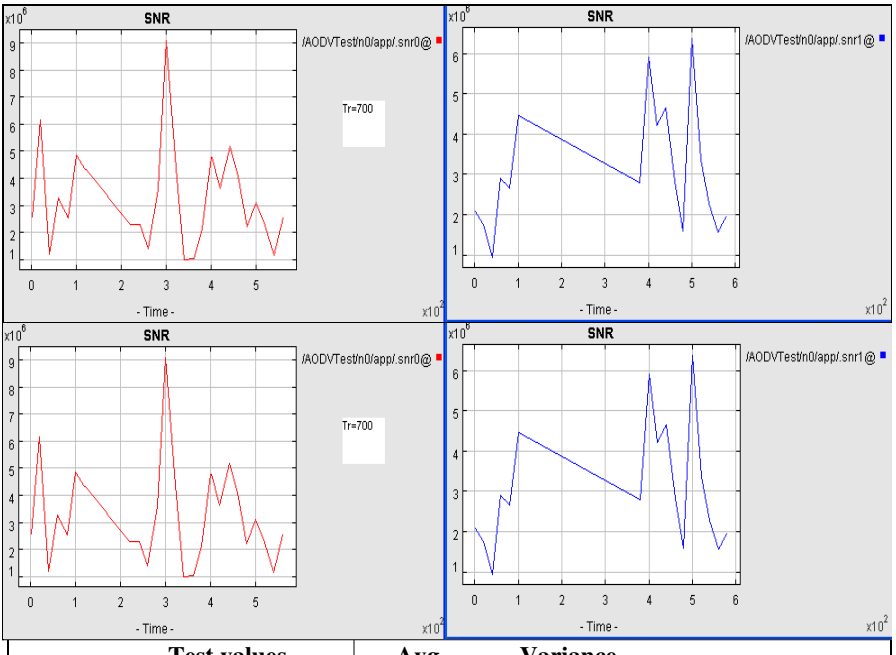


Fig. 2. A few simulated readings from numerous SNR-values, averages and variance



Test values	Avg	Variance
1st run	2.59	1.4 units
2nd run	2.81	0.8 units
3rd run	3.28	1.7 units
4th run	3.51	2.45 units

Fig. 2. (*continued*)

Instead of aggregating SNR-values and consuming more energy of the network in forwarding SNR information recursively, we propose that the variance of the SNR-average may be forwarded to the sink. Our proposal assumes that observation time is in accordance to the size of memory available at head node (sink, cluster-head, base station). Instead of transmitting the SNR figures alongside the data packet, the SNR-average may be calculated and retained at any part of network.

After certain duration, the variance of SNR-average is calculated and then it is transmitted over the network. In the proposed technique, calculation of SNR-variance is not performed in every time-slot and therefore it adds into total network time and total energy. For intelligent decision, the threshold of SNR-variance can be publicized among the head-nodes. We set the threshold 1.5×10^3 in all simulations of our experiments. When SNR-variance is found exceeding the threshold, then D-SAFE assumes the impact as vulnerability. Each of vulnerabilities weakens the total network strength. We recommend the use of proposed technique for the efficient use of memory.

Applying digital estimation of WSN security of D-SAFE and the proposed technique of SNR-variance the obtained result is shown in Fig 3. Also, by changing radii of random nodes and attacking the network communication in different ways we accomplish digital estimation of WSN-security.

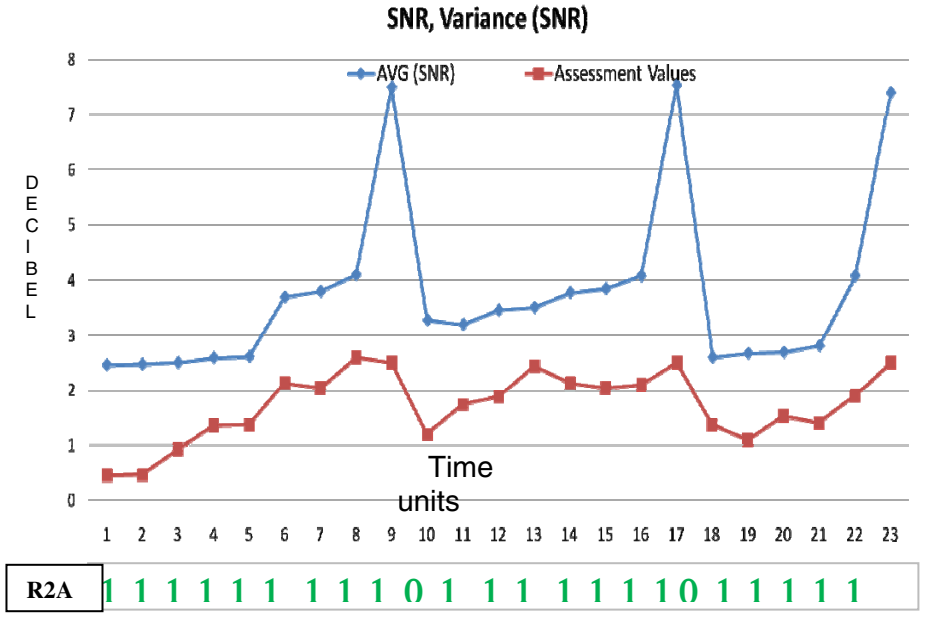


Fig. 3. Assessment graphs of SNR-variance and D-SAFE

In the Fig 3, the series of binary digits is D-SAFE assessment for its one of parameters. In D-SAFE, the SNR belongs to the *response to attack* (R2A) parameter. At two time slots (i.e. 10 and 18) the value of R2A parameter D-SAFE in [9] becomes zero. Here, we assume all values of table 1 as ideal except of R2A. Now, by substituting the resultant R2A in the following equation (1) of D-SAFE [7], the impact of SNR on WSN-security can be observed.

$$\text{Security Assessment Value} = \text{AVG}\,(\text{AR} + \text{PL} + \text{R2A} + \text{AI} + \text{EI}) \quad (1)$$

We know (from table 1) that R2A becomes zero during two time slots (i.e. 10^{th} and 18^{th}). After substituting and then converting the resultant value of D-SAFE in percentage we get 80%. This concludes in particular, that WSN offers 80% security at these two time slots. The overall security estimation of WSN in this SNR based simulation is 80% while SNR degrades. This state occurs only when variance of SNR-average exceeds the predefined threshold of SNR-variance (i.e. 1.5×10^3 in our experiment).

4.3 Analysis of Results for Accuracy of Digital Estimation

As a general observation if, any layer of WSN s' communication stack can be attacked then other WSN-layers must have protection mechanisms for sake of sensor network security. Analyzing the graphs in Fig 2 and Fig 3, we realize that SNR is too vital to be known for security even in hostile environments. We observe that the D-SAFE (Discrete Security Assessment Framework) validates the concept of separate assessment of values for each layer in WSNs.

In D-SAFE, the SNR is classified as link segment association and the detecting any abrupt change in variance alarms the situation by putting the pre-defined weight in priority queue for the parameter. Just as, in our simulation each average value of SNR represents an average of 10 SNR-values. If there are 6 SNR-average values then it means almost 60 SNR-values need to be transmitted within the network (i.e. from target node to sink node).

Our proposed technique of SNR-variance utilizes comparatively small amount of network energy as not all values are required to be sent towards sink-node. This makes the transmission of SNR-signals less recursive therefore consumes less operational energy too. On the basis of likely simulations and results, we show that using SNR-value, SNR-average, SNR-variance and threshold of SNR-variance we can identify the weaker areas in WSN. This will allow development of improved sensor networks and will enable us to predict the behavior of network components, if redeployment is desired.

5 Conclusion and Future Work

The security estimation is a challenge for the commercialization of sensor networks. We observe that security frameworks (like D-SAFE) for discrete assessment of WSN assist for quantifying WSN-security. To enrich our assessment work we perform SNR based digital estimation of WSN-security. We also figure out the parameter (SNR) impact on security of sensor networks. As, high SNR-values don't assure for high quality communication WSNs, therefore, our work of SNR based security-estimation of WSN is helpful for determining network attacks.

We are extending our work by utilizing some energy-efficient algorithms for real-time SNR values in a WSN. Our future experiment will be in environment which may exhibit unknown circumstances. Then, by knowing SNR impact on WSN-security and behavior of sensing nodes in this environment we will tend to predict the results from redeploying sensing nodes at same location. In our strong opinion the SNR value may be used to embed demand-base quality of communication in networks-of-future. Then, it would be very useful to utilize such advanced networks for transmission of multimedia contents and video streams.

Acknowledgments. We are very much thankful to the Director and staff of NFC-IET Multan, PAKISTAN for their immense support to conduct a part of research in the vicinity. A special thanks to Sehar Khalid for supporting our work.

References

1. Ashraf, A., Mussadiq, M., Hashmani, M.: An Analytical Revelation for a Safer Network Perimeter Security. In: The proceedings of International conference on Information Networking (ICOIN 2006), Sendai-Japan (2006)
2. Muraleedharan, R., Osadciw, L.A.: Jamming Attack Detection and Countermeasures. In: Wireless Sensor Network Using Ant System. Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, pp. 13244–11240
3. AKylidiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE communication Magazine 40(8), 102–114 (2002)

4. Wang, D., Zhang, Q., Liu, J.: The self-protection Problem in Wireless Sensor Networks. ACM Transactions on Sensor Netwoks 3(4), Article 20 (October 2007)
5. Zou, Y., Chakrabarty, K.: Uncertainty-aware and coverage-oriented deployment for sensor networks. Journal of Parallel and Distributed Computing 64(7), 788–798 (2004)
6. Ilyas, M., Mahgoub, I.: Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. In: LLC 2005. CRC Press, Boca Raton (2005), Library of Congress Card Number 2004043852, ISBN 0-8493-1968-4, http://ww.crcpress.com
7. 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. In: Canadian Conference on Electrical and Computer Engineering CCECE 2008, May 4-7, pp. 855–860 (2008)
8. Arain, A.A., Hashmani, M., Mussadiq, M., et al.: A Pretty Safe Strategy for Analyzing Discrete Security Assessment Framework in Wireless Sensor Networks. In: Book of Wireless Networks, Information Processing and Systems, November 14, 2008. CCIS, vol. 20, pp. 445–448. Springer, Heidelberg (2008)
9. 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)
10. Braginsky, D., Estrin, D.: Rumor Routing Algorithm For Sensor Networks. In: WSNA 2002, September 28, Atlanta, Georgia, USA Copyright 2002 ACM 1-58113-589-0/02/0009 (2002)
11. Abdul Hamid, M., Mamun-Or-Rashid, M., Hong, C.S.: Routing Security in Sensor Network:HELLO FLOOD Attack and Defence. In: ICNEWS (2006)
12. Marqus, A.G., Wang, X., Giannakis, G.B.: Minimizing Transmit Power for coherent Communications in Wireless Sensor Networks with Finite-Rate Feedback. IEEE Transactions on Signal Processing 56(9) (September 2008)
13. Muralee dharan, R., Ann Osadciw, L.: Jamming attack Detection and Countermeasures. In: Wireless Sensor Network Using Ant System, SPIE (2006) ISSN 0277-786X
14. Muralee dharan, R., Ann, L.: Cross Layer security protocol Using Swarm Intelligence. In: IEEE long Island System, Application and Technology conference(LISAT 2007), Farmingdale, New York (May 2007)
15. Chong, C.-Y., Kumar, S.P.: Sensor Networks: Evolution Opportunities, and Challenges. Proceedings of the IEEE 91(8), 1247–1256
16. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: SPINS: Security protocols for sensor networks. Wireless Networks 8(5), 521–534 (2002)
17. Kaplantiz, S.: Security Models for Wireless Sensor Networks. Conversion report, Monash University, March 20 (2006)
18. Ricadela, A.: Sensors Everywhere, January 24 (2005) http://informationweek.com/stories
19. Roman, R., Zhou, J., López, J.: On the security of wireless sensor networks. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3482, pp. 681–690. Springer, Heidelberg (2005)
20. Sabbah, E., Najeed, A., Kang, K.-D., Liu, K., Abu-Ghazaleh, N.: 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 (2006)
21. Park, S., Savvides, A., Srivastava, M.B.: 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 (2000)

22. Karlof, C., Wagner, D.: Secure Routing in Wireless Sensor Networks: Attack and Counter Measures. Ad Hoc Networks 1(2-3), 293–315 (2003)
23. Wood, A.D., Stankovic, J.A.: Denial of Service in Sensor Networks, pp. 54–62 (2002)
24. Czarlinka, A., Kundur, D.: 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)
25. Ngai, E.C.H., Jiangchuan Liu Lyu, M.R.: On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks Communications. In: IEEE International conference on ICC 2006, Istanbul, June 2006, vol. 8, pp. 3383–3389 (2006) ISSN:8164-9547, ISBN: 1-4244-0355-3