ENHANCEMENT OF SERINS TO MITIGATE PASSIVE WORMHOLE ATTACK IN WIRELESS SENSOR NETWORKS

ALI MODIRKHAZENI

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JUNE 2011

I dedicate this thesis to my parents and lovely grandmother. Without their patience, understanding, support, and most of all love, the completion of this work would not possible.

ACKNOWLEDGMENT

First, I would like to take this opportunity to express my sincere and utmost gratitude to my project supervisor. *Dr. Norafida Ithnin* for this vision, guidance and support throughout the duration that I undertook to complete this project successfully. Also I would like to thank friends for their help facilities and for their nice guidance during my project preparation. Last but not least, I would like to thank my parents, my siblings and all my friends that have given their moral support during the ups and down of my project work life cycle.

ABSTRACT

Wireless Sensor Networks is consisting of number of limited sensor devices which are communicated over the wireless media. There are a lot of its application in military, health and also industry. Stated that the sensor devices are limited resources, the network may experience a variety of conventional techniques of attack and the attacks that are not desirable because of limited resources is a characteristic of the type of network. One severe attack in WSNs is passive wormhole attack which attacker forwards data from one part of network to another part through the wormhole. In this dissertation, neighbor discovery approach has been proposed in order to enhance SeRINS to detect and mitigate passive wormhole attack which bring considerable amount of communication over load to entire network and is a means of lunching DoS attack. The simulation results shows that when enhanced SeRINS through the proposed neighbor discovery approach, it can detect and mitigate almost 100% of passive wormhole attacks.

ABSTRAK

Wireless Sensor Networks (WSN) adalah terdiri dari sejumlah peranti pengesan terhad yang berkomunikasi diantara satu dengan yang lain melalui media tanpa wayar. Terdapat pelbagai aplikasi WSN jenis ini digunakan di dalam bidang ketenteraan, kesihatan dan juga industri. Disebabkan rangkaian ini mempunyai ciri-ciri sumber pengesan yang terhad, ianya terdedah kepada pelbagai jenis ancaman konvensional dan serangan yang tidak diingini. Salah satu ancaman kepada rangkaian ini adalah serangan wormhole pasif yang mana penyerang akan mengarahkan data dari satu bahagian di rangkaian ke bahagian lain melalui wormhole. Disertasi ini telah mencadangkan kaedah penemuan tetangga sebagai penambahbaikan kaedah SeRINS bagi mengesan dan mengurangkan serangan wormhole pasif yang menyebabkan jumlah beban komunikasi keseluruh rangkaian meningkat dan kemungkinan berlakunya serangan DoS. Keputusan simulasi menunjukkan penambahbaikan kaedah SeRINS menggunakan kaedah penemuan tetangga yang dicadangkan boleh mengesan dan mengurangkan hampir 100% dari serangan wormhole pasif.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

CHAPTER 1

INTRODUCTION

1.1 Overview

Wireless Sensor Networks is usually consisting of huge number of limited sensor devices which are communicated over the wireless media. There are a lot of its application in military, health and industry. As sensor devices are limited, the networks exposed to various kinds of attacks and conventional defenses against these attacks are not suitable due to the resource constrained nature of these kinds of networks. Therefore, security in WSNs is a challenging task due to inheritance limitations of sensors.

In general, network is a set of computing nodes (such as computer and sensor device) which are connected and communicated over a common transmission medium such as cable. According to type of transmission medium, it can be classified into two major categories which are wired network and wireless network. Wired networks, as its name suggests, communicate over tangible transmission

medium such as cable or optical fiber. Wireless networks, in contrast to wired networks, exchange information through intangible medium such as radio frequency.

Wireless network, itself, includes following two sections which are Mobile Ad-Hoc Network (MANET) and Wireless Sensor Network (WSN). The term "MANET" refers to automated system of mobile hosts that are connected and communicated over a wireless media. In this kind of wireless network, there is no fixed infrastructure and the network topology may dynamically change due to free movement of nodes (Agrawal, 2006). The term "WSN", refers to the set of computing sensor nodes that is operating together using wireless connection.

1.2 Problem Background

It is necessary to provide wireless sensor network not only with the acceptable reliability of services but also adequate level of security. Many of WSN applications such as military and healthcare are critical and required certain level of security. In these kinds of applications, any malicious changes in the network information may cause catastrophic consequences.

Security in wireless sensor network is different and more challenging from conventional wired networks due to several reasons. First in WSNs communication media is wireless therefore malicious attacker does not require to physically tap into wires to gain access and it can easily eavesdrop, inject wrong data and modify information due to open communication media. Additionally WSNs suffer from lack of clear line of defense such as gateways which is applied in order to control illegal

access in conventional wired networks. Another reason is limited resources such as restricted battery and processor which are applied in sensor devices.

In order to achieve security in wireless sensor networks, security requirements considered. These requirements are Confidentiality, Integrity, Authentication and Availability. Confidentiality is the ability of hiding message to an unauthorized attacker. It means that if an illegal and unauthorized adversary access to the message, it cannot understand it. Integrity is another security requirement which provides a mechanism to know whether the message had been tampered or not. Authentication is ability to identify the reliability of message origin. And availability which grantees that network services are on hand as they needed. This factor identify whether message can move on to network or not. If the node can use its resource, then the availability is provided to the network for forwarding the message. The mentioned security requirements are often called the basic security requirements as almost every researcher had referred to them. Beside of basic security requirements, it is possible to have additional security requirement such as Data Freshness, Robustness against attacks, Resilience, Broadcast Authentication, Self Organization and Scalability. The detail discussion regarding to security requirements will be presented in Chapter 2.

Due to inherited nature of wireless sensor networks, these types of networks are exposed to variety types of attacks. Researchers can classify attacks in WSN regarding to the different criteria. Attacks can be classified into passive and active depending on how much attacker involve. In the active attacks, attacker will change the actual data, drop them or inject its own fake data. In another words, it involved. Unlike active attacks, passive one will not make any changes to the data. It just monitors the network, eavesdrop or analyze the traffic. According to the other point of view which is domain of attack, attacks classified into internal and external attacks. Internal attacks are lunched through the compromised nodes which share the secret key with other nodes. Unlike internal attacks, external attacks are performed by the nodes which do not belong to the network. This classification is also known as

insider and outside attacks. In another classification which is more common among the researchers, attacks classified base on the layers of wireless sensor networks into application layer, transport layer, network layer, data link and physical layer attacks. More details on WSN's attacks can be found in the Chapter 2.

One of the most severe attacks to detect and defend in wireless sensor network is wormhole attack (Zhao, Wei, Dong, Yao, & Gao, 2010) (Prasannajit B, Anupama, Vindhykumari, Subhashini, & Vinitha, 2010) (Karlof & Wanger, Secure Routing in Wireless Sensor Network: Attacks adn Countermeasures, 2003) , (Rehana, 2009), (Chen, Makki, Yen, & Pissinou, Sensor Network Security: A Survey, 2009). In this attack, a malicious attacker receives packets from one location of network, forwards them through the tunnel (wormhole) and releases them into another location. The illustration of wormhole attack in wireless sensor networks is shown in Figure 1.1.

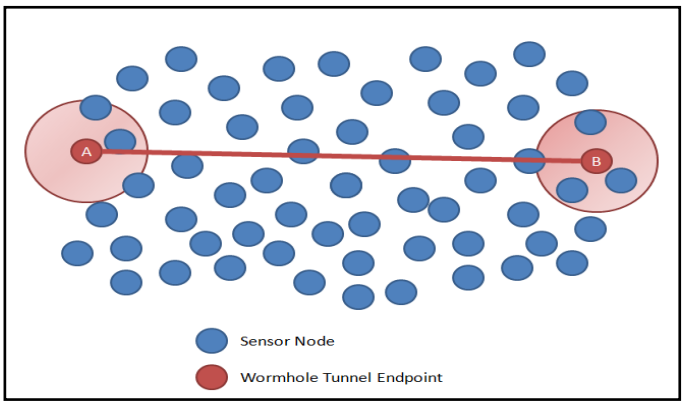

Figure 1.1 Illustration of Wormhole Attack in WSNs

Previous researchers classify wormhole attacks base on different points of view such as passive and active wormhole. This classification is based on whether attacker node belongs to the network or not. In the passive wormhole, two tunnel endpoints are not belonging to network but in active wormhole they are part on

network. More discussion on wormhole attack classifications will be presented in Chapter 2.

If wormhole peacefully transfers data to faraway location in the network, it could have positive effect. But the problem will arise when attacker receives the traffic through the wormhole. It can lunch selective forward attack or perform cryptanalysis attack. Additionally wormhole can effects considerable amount of communication. It also has negative effects on localization protocols or protocols which are depending on geographical information. By transmission of data from one place of network and broadcast to the other part, the total number of sends and receives of entire network will increase and therefore energy of node will decrease as energy consumption in WSNs has a direct relationship with number of sends and receives. And as energy of nodes be depleted, data cannot move in the network and this will lead to DoS (Denial of Service) attack.

1.3 Problem Statement

The common approaches to detect wormhole attack in WSN are the usage of additional tools such as GPS or Antenna and some other approach required accurate time synchronization. In this attack attacker transmits data of one part of network to the other part through the wormhole tunnel which its endpoints are not visible to the network or is not part of it. Secure routing protocols in WSNs are responsible for providing adequate level of security and they should be strong against the attacks. This dissertation tries to enhance secure routing protocol in WSN in order to detect passive wormhole attack and mitigate its effect on the network which is leading to DoS without any additional tools or accurate time synchronization. Additionally

most of previous approaches had been focusing at active wormhole attack. The problem main question is mentioned below.

"How to enhance SeRINS routing protocol to mitigate passive wormhole attack in wireless sensor networks?" The main question is divided to below sub-main questions. And these questions will be answered during this dissertation.

1. How to select an appropriate secure routing protocol to be enhanced?
2. What is the appropriate approach to for detection and mitigation of wormhole attack?
3. How to integrate SeRINS with appropriate wormhole countermeasures.

1.4 Project Aim

The aim of this study is to enhance a secure routing protocol in wireless sensor network in which it can detect passive wormhole attack and mitigate its effect on the network load, total number of send and receive, which is a mean to lunch DoS attack without applying any additional tools or accurate time synchronization.

1.5 Objectives

Objectives of this research are as follows:

1. To study and analyze existing secure routing protocols in wireless sensor network.
2. To propose an approach to detect passive wormhole attack in SeRINS and mitigates its effect which will leading to DoS attack.
3. To evaluate the enhanced SeRINS regarding to wormhole attack detection and mitigation.

1.6 Project Scope

In this study, the scope of the proposed algorithm is mainly based on the following items:

1. SeRINS will be applied during the dissertation.
2. Wormhole attack, as the main attack, will be considered through the project.
3. *C++* as the language which will be applied to implement protocols.
4. *Omnet++* as a network simulator

1.7 Significant of Study

As the objectives of the study will be achieved, the secure routing protocol is able to detect and mitigate the effect of passive wormhole attack without any additional tools which is more affordable and cost effective. Additionally as the results will enhance secure routing protocol to provide better level of security and it also address the issue of availability which is necessary to critical application such as military.

1.8 Organization of the Research

This research consists of six chapters. Chapter 1 presents introduction, problem background, problem statement, aim, objectives, scopes and significant of this research and provide the overview of the dissertation. In the Chapter 2 some basic backgrounds about Wireless Sensor Networks, security issues in WSNs is presented. Additionally it will present discussions concerning routing in WSNs and discuss about previous findings concern wormhole attack countermeasure in wireless sensor networks. Discusses on the methodology used in this research will be presented in Chapter 3. Additionally Chapter 4 will present data analysis is presented in this chapter. It will elaborate proposed technique and experimental results as well. And finally Chapter 5 concludes the dissertation and presents suggestion for future works.

REFERENCES

1. Acs, G. ´., & Butty´an, L. (2007). *A Taxonomy of Routing Protocols for Wireless Sensor Networks.*
2. Acs, G., Buttyan, L., & Vajda, I. (2007). The security proof of link-state routing protocol for wireless sensor netwoek. *Mobile Adhoc ans Sensor System.*
3. Agrawal, C. d. (2006). *Ad Hoc and Sensor Networks.* World Scientific Publishing Co. Pte. Ltd.
4. Al-Karaki, J. N., & Kamal, A. E. (2004). Routing tecniques in Wireless Sensor Networks: A Survey. *IEEE Wireless Communications* , 6-28.
5. Amin, F., Jahangir, A. H., & Rasifard, H. (2008). Analysis of Public-Key Cryptography for Wireless Sensor Networks Security. *World Academy of Science, Engineering and Technology 41* , 529 - 534.
6. Azer, M. A., El-Kassas, S. M., & El-Soudani, M. S. (2010). An innovative approach for wormhole attack detection and prevention in wireless sensor networks. *International conference on Networking, Sensing and Control (ICNSC)* (pp. 366 - 371). IEEE .
7. Blom, R. (1985). Theory and application of cryptographic techniques. *Eurocrypt 84 workshop on advances in cryptology* (pp. 335–338). Berlin: Springer.
8. Blundo, C., Santis, A. D., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M. (1992). Perfectly-secure key distribution for dynamic conferences. *12th annual international cryptology conference on advances in cryptology* (pp. 471-486). Springer.
9. Boukerche, A., Ahmad, M. Z., Turgut, D., & Turgut, B. (2009). A TAXONOMY OF ROUTING PROTOCOLS IN SENSOR NETWORKS. In *Algorithm and Protocols for Wireless Sensor Networks.* Wiley.

10. Bronshtein, I., Semendyayev, K., Musiol, G., & Muehlig, H. (2007). *Handbook of Mathematics.* Springer.
11. Butty´an, L., D´ora, L., & Vajda, I. (2005). Statistical Wormhole Detection in Sensor Networks. In *Authenticated Queries in Sensor Networks, Lecture Notes in Computer Science* (pp. 128 - 141). Springer.
12. Cha, W., Wang, G., & Cho, G. (2004). A Pair-Wise Key Agreement Scheme in Ad Hoc Networks . In *Lecture Notes in Computer Science.* Springer.
13. Chan, H., & Perrig, A. (2005). PIKE peer intermediaries for key establishment in sensor networks. *24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, (pp. 524 - 535). Pittsburgh.
14. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor network. *2003 Symposium on Security and Privacy*, (pp. 197 - 213).
15. Chan, H., Perrig, A., & Song, D. (2003). Random Key Predistribution schemes for sensor networks. *Security and Privacy. 2003 Symposium on Carnegie Mellon Univ.*, (pp. 197-213).
16. Chang, C., Tsay, P., & Lin, C. (2005). SVD-Based Digital Image Watermarking Scheme. *Pattern Recognition Letters*, (pp. 1577-1586).
17. Chen, X., Makki, K., Yen, K., & Pissinou, N. (2008). A Proactive Secure Routing Algorithm Defense against Node Compromise in Sensor Network. *IEEE* (pp. 557-559). IEEE.
18. Chen, X., Makki, K., Yen, K., & Pissinou, N. (2007). Node compromised modeling and its application in sensor networks. *IEEE Symposium on Computers and communication.* Aveiro.
19. Chen, X., Makki, K., Yen, K., & Pissinou, N. (2009). Sensor Network Security: A Survey. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11* , 52-73.
20. Cheng Weifang, L. X. (2006). A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks. *WASA* , 478-489.
21. Cho, Y.-G., Kang, J., & Nyang, D. (2007). Proactive Code Verification Protocol in Wireless Sensor Network. In *Lecture Notes in Computer Science* (pp. 1085–1096). Springer.
22. Choi, K. J., & Song, J.-I. (2006). Investigation of feasible cryptographic algorithms for wireless sensor network. *Advanced Communication Technology, 2006. ICACT 2006*, (pp. 1379-1381).

23. Cordeiro, C. D., & Agrawal, D. P. (2006). *Adhoc and Sensor Network : theory and applications.* World Scientific Publishing Pte. Ltd.
24. Cormen, T. H., Leiserso, C. E., Rivest, R. L., & Stein, C. (2003). *Introduction to algorithms.*
25. Creswell, J. W. (2003). *Research design: qualitative, quantitative, and mixed method approaches.* Sage.
26. Daemen, J., & Rijmen, V. (1998). *AES Proposal: Rijndael.* submitted to NIST as a candidate for the AES.
27. Du, X., Xiao, Y., Guizani, S., & Chen, H.-H. (2006). A Secure Routing Protocol for Heterogeneous Sensor Networks . *IEEE GLOBECOM 2006.* IEEE.
28. Eschenauer, L., & Gligor, V. D. (2002). A Key-Management Scheme for Distributed Sensor Network. *The 9th ACM conference on computer and communication security,* (pp. 41-47). Washington.
29. Eschenauer, L., & Gligor, V. (2002). Key Management Scheme for Distributed Sensor Networks. *9th ACM Conference on Computer and Communication Security*, (pp. 41-47).
30. Ganeriwal, S., ˇCapkun, S., Han, C.-C., & Srivastava, M. B. (2005). Secure time synchronization service for sensor networks. *4th ACM workshop on Wireless security* (pp. 97-106). New York: ACM Press.
31. Graaf, R. d., Hegazy, I., Horton, J., & Safavi-Naini, R. (2010). Distributed Detection of Wormhole Attacks in Wireless Sensor Networks. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 208-223). Springer.
32. Gui, N., Chen, R., Cai, Z., Hu, J., & Chen, Z. (2009). A Secure Routing and Aggregation Protocol with Low Energy Cost for Sensor Networks. *2009 International Symposium of Information Engineering and Electronic Commerce* (pp. 79-84). IEEE Computer Society.
33. Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). *Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs.*
34. Hu, L., & Evans, D. (2004). Using Directional Antennas to Prevent Wormhole Attacks. *Network and Distributed System Security Symposium (NDSS).*
35. Huang, Q., Cukier, J., Kobayashi, H., Liu, B., & Zhang, J. (2003). Fast authenticated key establishment protocols for self-organizing sensor networks.

2nd ACM international conference on Wireless sensor networks and applications (pp. 141-150). ACM Press.

36. JIANG, Y.-x., & ZHAO, B.-h. (2007). A Secure Routing Protocol with Malicious Node Detecting and Diagnosing for Wireless Sensor Networks. *2007 IEEE Asia-Pacific Services Computing Conference* (pp. 49-55). IEEE Computer Society.
37. Karlof, C., & Wanger, D. (2003). Secure Routing in Wireless Sensor Network: Attacks adn Countermeasures. *IEEE* , 113-127.
38. Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. *Second ACM conference on embedded networked sensor systems (SensSys 2004)*, (pp. 162–175).
39. Kausar, F., Saeed, M. Q., & Masood, A. (2008). Key Management and Secure Routing in Heterogeneous Sensor Networks. *IEEE International Conference on Wireless and Mobile Computing, Networking and Communication* (pp. 549-554). IEEE Computer Society.
40. Khalil, I., Bagchi, S., & Shroff, N. B. (2005). LITEWORP: A lightweight countermeasure for wormhole attack in multihop wireless networks. *International conference on depandable systems and networks* (pp. 1 - 10). IEEE.
41. Kizza, J. (2009). *A Guide to Computer Network Security.* Springer.
42. Krawczyk, H., Bellare, M., & Canetti, R. (1997). *HMAC: Keyed-Hashing for Message Authentication, RFC 2014.*
43. Lai, B., Kim, S., & Verbauwhede, I. (2002). Scalable session key construction protocol for wireless sensor networks. *IEEE workshop on Large Scale RealTime and Embedded Systems LARTES.*
44. Lan, Y., Zhibin, Z., Fuxiang, G., & Ge, Y. (2006). The Research on Certainty-Based Secure Routing Protocol in Wireless Sensor Networks., (pp. 1-5).
45. Law, Y. W., Doumen, J., & Hartel, P. (2004). Benchmarking Block Ciphers for Wireless Sensor Networks (Extended Abstract). *IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, (pp. 447-456).
46. Lee, G., Kim, D.-k., & Seo, J. (2008). An approach to mitigate wormhole attack in wireless ad hoc network. *International conference on information security and assurance*, (pp. 220 - 225).
47. Lee, J., & Stinson, D. R. (2005). Deterministic Key Predistribution Schemes for Distributed Sensor Networks. In *Selected Areas in Cryptography* (pp. 294-307). Springer.

48. Lee, S.-B., & Choi, Y.-H. (2006). A Secure althernate path routing in sensor netwroks. *ScienceDirect computer communication* , 153-165.
49. Li, G., He, J., & Fu, Y. (2006). A Hexagon-Based key Pre-distribution Scheme in Sensor Networks. *International Conference on Parallel Processing Workshop.*
50. Li, P., Zhang, J., & Lin, Y.-p. (2005). Curve-base routing algorithm for sensor networks. *International conference on computer networks and mobile computing.*
51. Li, P., Zhang, J., & Lin, Y.-p. (2006). Multipath-Based Secure Routing Algorithm for Sensor Network. *6th world conference on Intelligent Control and Automation* . Dalian, China: IEEE.
52. Liu, D., & Ning, P. (2003). Establishing pairwise keys in distributed sensor networks. *10th ACM conference on Computer and communications security* , (pp. 52 - 61).
53. Luna, J., Dikaiakos, M. D., Kyprianou, T., Bilas, A., & Marazakis, M. (2008). Data Privacy Considerations in Intensive Care Grids. *HealthGrid.*
54. Madria, S., & Yin, J. (2009). SeRWA: A secure routing protocol against wormhole attack. *Ad Hoc Networks 7* , 1051-1063.
55. Matsui, M. (1997). New Block Encryption Algorithm MISTY. *Fast Software Encryption Workshop* (pp. 54-68). Springer.
56. Modirkhazeni, A., & Ithnin, N. (2011). Secure Hierarchal Routing Protocols in WSN; A Security Survey Analysis. University Technology Malaysia.
57. Modirkhazeni, A., Ithnin, N., & Ibrahim, O. (2010). Secure Multipath routing protocol in wireless sensor network; A security survey analysis. *2th international conference on network applications, protocols and services.* Alor Setar: IEEE Explore.
58. Muruganathan, S. D., Ma., D., Bhasin, R., & Fapojuwo, A. (2005). A Centerilzed Energy-Efficient Routing Protocol for Wireless Sensor Networks. *IEEE Communication Magazine Vol 43* .
59. Papadimitratos, P., Poturalski, M., Schaller, P., Lafourcade, P., Basin, D., Capkun, S., *et al*. (2008). Secure neighborhood discovery: a fundamental element for mobile ad hoc networking. *IEEE Communications Magazine* , 132 - 139 .
60. Paul Walters, J., Liang, Z., Shi, W., & Chaudhary, V. (2006). Wireless Sensor Network Security: A Survey. *Security in Distributed, Grid, and Pervasive Computing* .

61. Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. *Second IEEE workshop on Mobile Computing Systems and Applications*, (pp. 90 - 100).
62. Poon, C. C., Zhang, Y.-T., & Bao, S.-D. (2006). A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health. *IEEE Communications Magazine* , 73-81.
63. Poovendran, R., & Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks . *Wireless Networks* , 27-59.
64. Poturalski, M., Papadimitratos, P., & Hubaux, J.-P. (2008). Secure neighbor discovery in wireless networks: formal investigation of possibility. *2008 ACM symposium on Information, computer and communications security* . New York: ACM.
65. Prasannajit B, V., Anupama, S., Vindhykumari, K., Subhashini, S. R., & Vinitha, G. (2010). An Approach towards Detection of Wormhole Attack in Sensor Networks. *WASE International Conference on Information Engineering*, (pp. 283 - 389).
66. Qian, L., Song, N., & Li, X. (2007). Detection of wormhole attack in multipath routed wireless ad hoc networks; statistical analysis approach. *30*.
67. Rasheed, A., & Mahapatra, R. (2009). Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks in Wireless Sensor Networks. *2009 IEEE 28th International Performance Computing and Communications Conference (IPCCC)* (pp. 216 - 222). Scottsdale, AZ : IEEE Explorer.
68. Rehana, J. (2009). Security of Wireless Sensor Networks. *Seminar on Internetworking.*
69. Rivest, R. L. (1995). *The RC5 Encryption Algorithm* .
70. Rivest, R. L., Robshaw, M. J., Yin, Y., & Sidney, R. (1998). *The RC6 Block Cipher.* submitted to NIST as a candidate for the AES.
71. Rogers, E. M. (1996). *Diffusion of Innovations.* Free Press.
72. Rosenberg, A. I. (2008). *A Taxonomy-based Approach to Design of Large-scale Sensor network.* Springer.
73. Sabbah, E., & Kang, K.-D. (2009). Security in Wireless Sensor Networks. In *Guide to Wireless Sensor Networks* (pp. 491-512). Springer.
74. Sabbah, E., & Kang, K.-D. (2009). Security in Wireless Sensor Networks. In *Guide to Wireless Sensor Networks* (pp. 491-512). Springer.

75. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. *10th IEEE International Conference on* , (pp. 78 - 87).
76. Seys, E. (2004). *Lightweight Cryphtography Enabling Secure Wireless Sensor Network, Security Issues in Mobile and Wireless Heterogenouse Networks.*
77. Shi, E., & Perrig, A. (2004). Designing secure sensor networks . *IEEE Wireless Communications* , 38-43.
78. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., & Srivastava, M. B. (2002). On Communication Security inWireless Ad-Hoc Sensor Networks. *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, (pp. 139 - 144).
79. Srinath, R., Reddy, A. V., & R.Srinvasan. (2007). AC: Cluster Based Secure Routing Protocol for WSN. *Third International Conference in Networking and Services.* IEEE.
80. Sun, K., Ning, P., & Wang, C. (2006). Secure and resilient clock synchronization in wireless sensor networks. *IEEE Journal on Selected Areas in Communications* , 395 - 408 .
81. Tang, L., & Li, Q. (2009). S-SPIN: A Provably Secure Routing Protocol for Wireless Sensor Network. *IEEE International Conference on Communication Software and Network* (pp. 620-624). IEEE.
82. Verdonel, R., Dardari, D., Mazzini, G., & Conti, A. (2008). *Wireless Sensor and Actuator Networks.*
83. Wang, W., Bhargava, B., Lu, Y., & XiaoxinWu. (2006). Defending against wormhole attacks in mobile ad hoc networks. *Wireless Communications & Mobile Computing* .
84. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A Survey of Security Issues in Wireless Sensor Networks. *IEEE Communications Surveys and Tutorials* .
85. Wen, S., Du, R., & Zhang, H. (2006). A Segment transmission secure routing protocol for wireless sensor network . (pp. 1579-1582). IEEE.
86. yao, X., & Zheng, X. (2008). A Secure Routing Scheme Based on Multi-objective optimization in Wireless Sensor Network. *2008 International Conference on Computational Intelligence and Security*. IEEE Computer Society.

87. Yin, C., Huang, S., Su, P., & Gao, C. (2003). Secure Routing for Large-Scale Wireless Sensor Network. *ICCT2003* (pp. 1282-1286). IEEE.
88. Yin, J., & Madria, S. K. (2006). A hierarchical secure routing protocol against black hole attack in sensor networks. *IEEE Intenational Conference on Sensor Networks and trustworthy computing.*
89. Yin, J., & Madria, S. (2006). SecRout: A Secure Routing Protocol for Sensor Network. *20th International Conference on Advanced information networking and applications.* IEEE.
90. Zhang, K., Wang, C., & Wang, C. (2008). A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management. (pp. 1-5). IEEE Computer Society.
91. Zhao, Z., Wei, B., Dong, X., Yao, L., & Gao, F. (2010). Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis. *WASE International Conference on Information Engineering* (pp. 251 - 254). IEEE.
92. Zhou, J., Li, C., Coa, Q., & Shen, Y. (2008). An Intrusion-tolerant Secure Routing Protocol with key exchanges for Wireless Sensor Network. *International Conference on Information and Automation* (pp. 1547-1552). Zhangiajie: IEEE.
93. Zia, T., & Zomaya, A. Y. (2009). Security Issues and Countermeasures in Wireless Sensor Networks. In *Algorithms and protocols for wireless sensor networks.* John Wiley & Sons, Inc.