A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks

Suraj Sharma and Sanjay Kumar Jena
Department of Computer Science and Engineering
National Institute of Technology Rourkela, Odisha, India
suraj.atnitrkl@gmail.com, skjena@nitrkl.ac.in

ABSTRACT

WSNs usually deployed in the targeted area to monitor or sense the environment and depending upon the application sensor node transmit the data to the base station. To relay the data intermediate nodes communicate together, select appropriate routing path and transmit data towards the base station. Routing path selection depends on the routing protocol of the network. Base station should receive unaltered and fresh data. To fulfill this requirement, routing protocol should be energy-efficient and secure. Hierarchical or cluster-base routing protocol for WSNs is the most energy-efficient among other routing protocols. In this paper, we study different hierarchical routing technique for WSNs. Further we analyze and compare secure hierarchical routing protocols based on various criteria.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: *Data communications, Security and protection*; C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Routing protocols.*

General Terms

Security.

Keywords

Wireless sensor network, Hierarchical (cluster-based) routing protocol, Routing security.

1. INTRODUCTION

The growth of micro devices, small memory chip and wireless communication technology invented the tiny sensor device called sensor node. Sensor node constrained with the limited battery power, small memory, less computation and communication capability. These sensor nodes are responsible for sensing the data from the environment and sending the processed data to the base station though intermediate sensor nodes. These self-configurable sensor nodes form a multi hop and collaborative network called Wireless Sensor Network. In the near future WSNs will become very popular and reliable for remote monitoring and sensing technology. There is a wide verity of application area ranges from forest fire monitoring to building security monitoring, health field to battle filed, animal habitat monitoring and nuclear firm monitoring are the challenging application of the WSNs.

Main task of the sensor node is to sense data and send it to the base station in multi hop environment for this routing path is essential. For computing the routing path from the source node to the base station there is huge number of proposed routing protocols exist. Routing protocols in WSNs mainly classified in two categories[1]: *Network Structure* and *Protocol Operation*. *Network Structure* is further classified into Flat, Hierarchical and Location based routing. *Protocol Operation* is further classified into Negotiation, Multi-path, Query, QoS and Coherent based routing. All these routing protocols are very useful for routing path computation, but it highly affect the WSNs performance. So the development of the routing protocol should be for balancing the load among the sensor nodes and prolonging the network lifetime.

Nowadays researchers are working towards the energy efficient routing protocol. Hierarchical routing protocols are the most energy efficient among rest of the protocols for WSNs. In hierarchical routing protocol, network is divided into clusters and cluster head is assigned to each cluster. These cluster heads are higher energy nodes, which aggregate, process and transmit the information to the BS, while the lower energy nodes used to sense the targeted area and send the data to CH. Hierarchical routing is an efficient way to reduce the total energy consumption of the network. Data aggregation and processing in the CH greatly reduce total number of sent messages to the BS. Actually, the goal of developing hierarchical routing protocol is to minimize the network traffic towards the base station.

Generally, security issue in Hierarchical routing protocol have not given much attention, since most of the routing protocol in WSNs have not been developed with security in mind. Many hierarchical routing protocols have been developed, where energy efficiency is the main goal. In many applications like military and battle field, data is important and have to maintain secrecy in data communication between sensor nodes and BS. In this paper we discuss, analyze and list the advantages and drawback of secure Hierarchical Routing Protocol techniques proposed till now.

The rest of the paper is organised as follows. Section 2 describes some basic hierarchical routing protocols. Security

ICCCS'11 February 12-14, 2011, Rourkela, Odisha, India

goals in WSNs are listed in section 3. Section 4 introduces different possible attacks on routing protocol. In section 5 verious secure routing protocols is covered. In section 6, we does analysis on different secure routing protocols. We concludes the paper in section 7.

2. HIERARCHICAL ROUTING PROTOCOLS

Hierarchical or cluster-based routing, originally proposed for wired network to enhance scalability and efficiency. In WSNs, Hierarchical routing techniques is used to enhance energy-efficiency and hence prolong the network lifetime. Reservation-based scheduling, collision avoidance, data aggregation by cluster head, uniform energy dissipation, fair allocation of channel and lower latency are some characteristics of hierarchical topology routing protocol[1].

Low energy adaptive clustering hierarchy (LEACH)[6] is one of the very first hierarchical routing protocol. LEACH includes distributed clustering and utilizes randomize rotation of cluster heads to evenly distribute the energy load in the network. It calculates a threshold value to elect the cluster head. LEACH protocol is very useful for the applications, where constant monitoring is required. TL-LEACH[12] is the extension of the LEACH, where TL stands for Two-Level. It utilizes two level of clustering where primary CH communicate with secondary CH in order to send the data, for better throughput. TL-LEACH form clusters based on minimum distance of nodes to their corresponding CH, EECS[24] extends this by dynamic sizing of clusters based on cluster distance from the base station. CH election is based on the residual energy of the node.

Power-efficient gathering in Sensor Information System (PEGASIS)[11] is a near-optimal chain-based protocol. In PEGASIS, nodes need to communicate to its nearest neighbor and they propagate to the base-station. Unlike LEACH, PEGASIS avoids cluster formation and uses only one node in a chain to transmit to the base-station[1]. In this way it increase the lifetime of the network and allow only local communication for less bandwidth consumption in communication. Further reduce the energy consumption of PEGASIS, CCS[9] has been proposed. In CCS, the whole network is divided in co-centric circular tracks and each track presents a cluster. Track level has been assign to each track, depends upon the distance from the base-station. Data communication is done through tracks. TSC[5] protocol is the enhance version of CCS, by further dividing tracks into sectors.

Threshold sensitive energy efficient sensor network protocol (TEEN)[14], is a data-centric protocol designed for time-critical application. In TEEN, the transmission of the sensed data is depends upon threshold values, called Hard Threshold (HT) and Soft Threshold (ST), which is broadcasted by CH. APTEEN[15] is the enhances version of TEEN and goal is to capturing both periodic data and time critical data. APTEEN supports three different query types: historical, one-time and persistent query[13].

Further to reduce the energy consumption and prolong the lifetime of the network many hierarchical routing protocols have been proposed.

3. SECURITY GOALS IN WSNS

In an ideal world, we ensure the security goal if every eligible node receives all the messages intended to it. In the presence of resourceful adversary, security goals guarantee the confidentiality, integrity, authenticity, availability and freshness of data.

- **Confidentiality:** Data should not leak by the sensor nodes to other network. While communicating the data in the network, no one can understood except intended recipient[20]. The standard way to keep the sensitive data secret is to use the cryptography technique, hence achieve the confidentiality.
- **Integrity:** Data should reach to the intended receiver without any alteration in the data. Data loss or damage can even occur due to the communication environment. The integrity mechanism should ensure that no adversary can manipulate the communicated data[20]. Integrity of the data can be maintain by the techniques like message digest and MAC.
- **Authenticity:** Authentication is necessary for maintaining the network, coordinating with the sensor node and sending or receiving the information. An adversary can easily inject the messages in the network, so receiver should ensure that the received message is originated by the correct source[20]. Informally, data authenticity allows a receiver to verify that the data really sent by the authorized user. Authenticity can be maintained by the cryptography mechanism like MAC.
- **Availability:** Availability ensures that the services of a network should be available always even in presence of an internal or external attacks such as a denial of service attack (DoS). Different mechanisms have been proposed by the researches to achieve this goal[20].
- **Freshness:** Freshness implies that receiver receives the recent and fresh data and ensures that no adversary can replay the old data. This requirement is especially important when the WSN nodes use sharedkeys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN[20]. To achieve the freshness the mechanism like nonce or time stamp should add to each data packet.

4. ATTACKS ON ROUTING PROTOCOL

Many sensor network routing protocols were very simple and not developed as security in mind, so the adversary can launch various attacks in the network. Mainly network layer protocol (i.e. routing protocol) suffers from many attacks [10] like; spoofing or altering the route information, selective forwarding, sinkhole attack, wormhole attack, Sybil attack, HELLO flood attack etc.

4.1 Spoofing, Altering or Replaying the route information

An adversary can launch the routing information corruption by spoofing, altering or replying the routing information. By this an adversary can attracts or redirects the traffic, increases the latency, generate routing loops or creates false error[10] etc.

4.2 Selective forwarding attack

In the selective forwarding attack, malicious node may refuse to forward certain packet and simply drop it. If an

Table 1: Secure Routing Protocols analysis based on security goals

Secure Routing Protocol	Confidentiality	Integrity	Freshness	Authenticity	Availability
M. Bohge et al.		✓		✓	
SRPSN	✓	✓		✓	
LHA-SP	✓			✓	
F-LEACH	✓	✓	✓	✓	
SLEACH		✓		✓	
SHEER	✓	✓	✓	✓	
R. Srinath et al.	✓	✓		✓	
NHRPA					
Sec-LEACH	✓	✓	✓	✓	
SS-LEACH	✓			✓	
RLEACH	✓	✓		✓	
ESMR	✓				
SRPBCG	✓	✓		✓	

Table 2: Secure routing protocols comparison based on prevention of security attacks

Secure Protocol	Alter/Replay	Selective	Sinkhole	Sybil	Wormhole	HELLO	Outsider	Node Compromise
M. Bohge et al.	✓							✓
SRPSN	✓	✓					✓	
LHA-SP							✓	
F-LEACH	✓			✓		✓		
SLEACH	✓	✓	✓			✓	✓	
SHEER	✓	✓		✓		✓	✓	
R. Srinath et al.	✓					✓	✓	✓
NHRPA								✓
Sec-LEACH	✓	✓		✓		✓		
SS-LEACH	✓	✓		✓		✓		✓
RLEACH	✓	✓	✓	✓	✓	✓		
ESMR							✓	
SRPBCG	✓						✓	✓

adversary drops the entire received packet, it behaves like a blackhole attack[10]. An adversary explicitly includes on the path of data flow to perform selective forwarding.

4.3 Sinkhole and Wormhole attack

Basically, in the both sinkhole and wormhole attacks[10]; the adversary tries to attract all the traffic from a particular area through a compromised node. Sinkhole attack mainly works by making a compromised node look attractive to the neighbor nodes to route the data packet and generally spoof, modify or drop the packet. In this way, sinkhole attack give birth to many attacks like; selective forwarding, blackhole, tempering the routing information etc.

An adversary launch wormhole with two distant malicious nodes and try to attract the traffic by showing one hop distance to the sink. Wormhole attack is very difficult to detect because it uses out-of-bound channel to route packets [10].

4.4 Sybil attack

In this attack [10], a single node presents multiple identities to the other node in the network. It tries to mislead the node in neighbor detection, route formation and topology maintenance. The Sybil attack is a significant threat to many geographic and multipath routing protocols.

4.5 HELLO flood attack

In the HELLO flood attack[10], an adversary rebroadcast overheard packet with enough power to be received by every node in the network. The protocols that generally use the local topology like neighbor information for route creation and topology maintenance get affected by this attack.

5. SECURE HIERARCHICAL ROUTING PROTOCOLS

Many previous Hierarchical routing protocols assume a safe and secure environment where all sensor nodes cooperate with no attack present. But the real world environment is totally opposite, there are many attacks that affects the performance of routing protocol. Attacker use different kinds of technique to launch attack and damage or harm the data and the network. In order to secure the hierarchical routing protocol many works have been proposed. In this section we discuss those techniques, analyze them and list out the advantages and disadvantages associated with each secure hierarchical routing protocol.

5.1 M. Bohge et al.

Secure hierarchical routing protocol by using three tier ad hoc network topology has been proposed[2]. It used TESLA certificates for authentication. The use of massage authentication code in the framework protects all data against malicious modification and information forgery. It presented an authentication framework for an application driven hierar-

Table 3: Evaluation of secure routing protocols based on security mechanism used

Secure Protocol	AsymmetricKey	Symmetrickey	PairwiseKey	KeyPredist.	OnewayHASHchain	MAC
M. Bohge et al.	✓					✓
SRPSN		✓		✓		
LHA-SP		✓	✓			
F-LEACH		✓		✓		
SLEACH		✓				✓
SHEER		✓		✓		
R. Srinath et al.	✓	✓				
NHRPA						
Sec-LEACH		✓		✓	✓	
SS-LEACH		✓		✓		
RLEACH	✓	✓	✓		✓	
ESMR	✓			✓		
SRPBCG						

chical ad hoc sensor network and deals with compromised nodes. But it cannot prevent intruders from coming into the network and sending packets and cannot protect against eavesdropping.

5.2 SRPSN

In SRPSN[22] an energy-efficient level-based hierarchical routing technique proposed. They have designed a secure routing protocol for WSNs to safe guard from different attacks by building a secure route from the source to sink node. They used the symmetric key cryptography and proposed a group key management scheme, which contains group communication policies, group membership requirements and an algorithm for generating a distributed group key for secure communication. Every node contributing its partial key to generate a group key. One drawback associated with this protocol is that, while changing the CH all group key i.e. inter-cluster and intra-cluster key should have to compute once again, which is a cumbersome task.

5.3 LHA-SP

LHA-SP[18]is the first work focusing on securing heterogeneous hierarchical WSNs with arbitrary number of levels. It uses the symmetric key scheme and took following assumption: an adversary will take a certain amount of time to compromise the group key or temper with a node and this amount of time exceeds, that require setup the network. It prevents intruders (outsider attacker) to taking activity, tempering with or injecting message into the networks and prevents eavesdropping on communication between legitimate nodes. Authentication and confidentiality is maintained by shared pairwise key. It deals with orphan node problem.

5.4 F-LEACH

L. B. Oliveria et al.[17] propoesed FLEACH, a protocol for securing node to node communication in LEACH-based network. It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. FLEACH provides authenticity, integrity, confidentiality and freshness to node-to-node communication. But it is valnerable to node capturing attack.

5.5 SLEACH

This is the first modified secure version of LEACH called SLEACH[4], which investigated the problem of adding security to cluster-based communication protocol for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources. SLEACH provides security in LEACH by using the building block of SPINS (Security Protocol for Sensor Network), symmetric-key methods and MAC (Message Authentication Code). SLEACH protects against selective forwarding, sinkhole and HELLO flooding attacks. It prevents intruder to send bogus sensor data to the CH and CH to forward bogus message. But SLEACH cannot prevent to crowd the time slot schedule of a cluster, causing DoS attack or simply lowering the throughput of the CH and does not guarantee data confidentiality. The solution is meant to protect only outsider attack.

5.6 SHEER

J. Ibriq et al.[8] proposed a secure hierarchical energy-efficient routing protocol(SHEER) which provides secure communication at the network layer. It uses the probabilistic broadcast mechanism and three-level hierarchical clustering architecture to improve the network energy performance and increase its lifetime. To sucure the routing SHEER implements HIKES a secure key transmission protocol and symmetric key cryptography. They have compared the performance with the secure LEACH using HIKES.

5.7 R. Srinath et al.

This protocol is based on LEACH protocol; named Authentication Confidentiality cluster based secure routing protocol[21]. It uses both public key (in digital signature) and private key cryptography. This protocol deals with interior adversary or compromised node. Because of the high computational requirement (use of public key cryptography), it is not efficient for the WSNs.

5.8 NHRPA

The proposed routing protocol[7] can adopt suitable routing technology for the nodes according to the distance of node to the BS, density of the nodes distribution and residual energy of the nodes. NHRPA compared with Directed Diffusion (DD), LEACH and PEGASIS in terms of the energy usage, packet latency and security in the presence of node compromised attacks, results show that the proposed routing algorithm is more efficient for WSNs. It does not use any cryptography technique in the routing protocol, so the overhead is less. But it only deals with the node compromise

Table 4: Analysis of secure routing protocols based on fundamental aspect

Secure Protocol	Basic Protocol	Deal with orphan node	Energy Efficiency
M. Bohge et al.			Medium
SRPSN			Good
LHA-SP		✓	Medium
F-LEACH	LEACH		Medium
SLEACH	LEACH		Medium
SHEER			Good
R. Srinath et al.	LEACH		Medium
NHRPA			Good
Sec-LEACH	LEACH		Medium
SS-LEACH	LEACH		Good
RLEACH	LEACH	✓	Medium
ESMR			Medium
SRPBCG			Medium

attack.

5.9 Sec-LEACH

Sec-LEACH [16] provides an efficient solution for securing communications in LEACH. It used random-key predistribution and μTESLA for secure hierarchical WSN with dynamic cluster formation. Sec-LEACH applied random key distribution to LEACH, and introduced symmetric key and one way hash chain to provide confidentiality and freshness. Sec-LEACH provides authenticity, integrity, confidentiality and freshness to communications.

5.10 SS-LEACH

Di Wu et al.[23] introduced a secure hierarchical protocol called SS-LEACH, which is the secure version of LEACH. SS-LEACH improves the method of electing cluster heads and forms dynamic stochastic multi-paths cluster heads chains to communicate to the base station, In this way it improve the energy-efficiency and hence prolong the lifetime of the network. It used the key pre-distribution and self-localization technique to secure the basic LEACH protocol. It prevent compromised node to take part in the network and preserve the secrecy of the packet. It avoids selective forwarding, HELLO flooding and Sybil attack.

5.11 RLEACH

Secure solution for LEACH has been introduced called RLEACH[25] in which cluster are formed dynamically and periodically. In RLEACH the orphan node problem is raised due to random pair-wise key scheme so they have used improved random pair-wise key scheme to overcome. RLEACH has been used the one way hash chain, symmetric and asymmetric cryptography to provide security in the LEACH Hierarchical routing protocol. RLEACH resists to many attack like spoofed, alter and replayed information, sinkhole, wormhole, selective forwarding, HELLO flooding and Sybil attack.

5.12 ESMR

Proposed model is the security solution for the LEACH called efficient security model of routing protocol (ESMR)[3], which use only public key cryptography technique. Simulation result shows that the performance of ESMR is not as good as LEACH in no attacker environment, but it becomes better and better with the number of attacker increases. This protocol only deals with out-sider attack and computation burden is high due to the use of public key cryptography.

5.13 SRPBCG

Z. Quan et al.[19] proposed a routing protocol called secure routing protocol cluster-gene-based for WSNs(SRPBCG). The selection of CH is same as LEACH. Objective of the scheme is to manage trust and reputation locally and to authenticate identity of node with minimal overhead and time delay. Biological authentication mechanism has been used which is a very effective authentication method, biological 'gene' as encryption key is very secure and effective key distribution scheme, which require only few memory and communication overhead. It only deals with the adversary's attack and compromised nodes. Security of protocol is inconsiderately, when forming a cluster and transmitting the message. Computation and communication burden are more in this protocol.

6. ANALYSIS

In the previous section, we have seen various secure cluster-based routing protocols. Table 1. describes several security goals achieved by different secure hierarchical protocols; F-LEACH, SHEER and Sec-LEACH routing protocol maintain the most whereas NHRPA and ESMR gain the least. WSNs routing protocols are vulnerable of various attacks. The secure protocols which prevented routing protocol attacks are listed in Table 2. Depends upon the comparison we can say that SLEACH, SHEER, Sec-LEACH, SS-LEACH and RLEACH are more secure than rest of the secure protocols. To add security in the routing protocol, we have to take help from the various security mechanisms. Use of different security mechanism by the various secure routing protocols is listed in Table 3. This evaluation is very helpful for the researchers, who want to implement secure hierarchical routing protocol. To impose the security into the existing protocol sometime increases the complexity of the protocol and decreases the lifetime of the network. Energy efficiency analyses for different secure routing protocols are in Table 4.

7. CONCLUSION

Routing protocol affects the performance of the network in the form of energy efficiency, security, resiliency and lifetime. So that secure, robust and efficient routing protocol is the basic requirement. In this paper, we have studied and analyzed a number of secure and energy efficient hierarchical routing

protocols for WSN. The information provided in the paper would be beneficial for the researchers to work in this area.

Acknowledgment: The authors are indebted to Information Security Education and Awareness (ISEA) Project, MCIT, Department of Information Technology, Govt. of India, for sponsoring this research and development activity.

8. REFERENCES

[1] J. N. Al-karaki and A. E. Kamal. Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, 11(6):6–28, December 2004.

[2] M. Bohge and W. Trappe. An authentication framework for hierarchical ad hoc sensor networks. In *Proceedings of the 2nd ACM workshop on Wireless security (WiSe '03)*, pages 79–87, New York, NY, USA, 2003. ACM.

[3] J. Chen, H. Zhang, and J. Hu. An efficiency security model of routing protocol in wireless sensor networks. In *Proc. of the 2008 Second Asia International Conference on Modelling and Simulation*, pages 59–64, Washington, DC, USA, 2008. IEEE Computer Society.

[4] A. C. Ferreira, M. A. Vilaça, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro. On the security of cluster-based communication protocols for wireless sensor networks. In *Proc. 4th IEEE International Conference on Networking (ICNŠ05), volume 3420 of Lecture Notes in Computer Science*, pages 449–458, 2005.

[5] N. Gautam, W. Lee, and J. Pyun. Track-sector clustering for energy efficient routing in wireless sensor networks. In *Proc. of the 2009 Ninth IEEE International Conference on Computer and Information Technology*, volume 2, pages 116–121. IEEE Computer Society, 2009.

[6] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proc. of the 33rd Hawaii International Conference on System Sciences (HICSS '00)*, page 8020, Washington, DC, USA, January 2000. IEEE Computer Society.

[7] C. Hong-bing, Y. Geng, and H. Su-jun. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. *The Journal of China Universities of Posts and Telecommunications*, 15(3):75–81, September 2008.

[8] J. Ibriq and I. Mahgoub. A secure hierarchical routing protocol for wireless sensor networks. In *In: Proc. 10th IEEE International Conference on Communication Systems*, pages 1–Ű6, Singapore, October 2006.

[9] S. Jung, Y. Han, and T. M. Chung. The concentric clustering scheme for efficient energy consumption in the pegasis. In *Proc. 9th International Conference on Advanced Communication Technology*, volume 1, pages 260–265, February 2007.

[10] C. Karlof and D. Wagner. Secure routing in sensor networks:attacks and countermeasures. *Ad Hoc Networks*, 1:293–315, May 2003.

[11] S. Lindsey and C. S. Raghavendra. Pegasis: Power-efficient gathering in sensor information systems. In *IEEE Aerospace Conference Proceedings*, pages 1125–1130, 2002.

[12] V. Loscrì, G. Morabito, and S. Marano. A two-levels hierarchy for low-energy adaptative clustering hierarchy (tl-leach). In *Proc. VTC2005*, pages 1809–1813, Dallas (USA), September 2005.

[13] J. J. Lotf, M. Hosseinzadeh, and R. M. Albuliev. Hierarchical routing in wireless sensor networks: a survey. In *2nd International Conference on Computer Engineering and Technology*, volume 3, pages 650–654, April 2010.

[14] A. Manjeshwar and D. P. Agrawal. Teen: a routing protocol for enhanced efficiency in wireless sensor networks. In *Proc. 15th International In Parallel and Distributed Processing Symposium*, volume 3, pages 2009–2015. IEEE Computer Society, April 2001.

[15] A. Manjeshwar and D. P. Agrawal. Apteen: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In *Proc. of the 16th International Parallel and Distributed Processing Symposium (IPDPS '02)*, page 48, Washington, DC, USA, 2002. IEEE Computer Society.

[16] L. B. Oliveira, A. Ferreira, M. A. Vilaça, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro. Secleach-on the security of clustered sensor networks. *Signal Processing*, 87(12):2882–2895, December 2007.

[17] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro. Secleach - a random key distribution solution for securing clustered sensor networks. In *Proc. of the Fifth IEEE International Symposium on Network Computing and Applications*, pages 145–154, Washington, DC, USA, 2006. IEEE Computer Society.

[18] B. Parno, M. Luk, E. Gaustad, and A. Perrig. Lha-sp: secure protocols for hierarchical wireless sensor networks. In *Proc. of 9th IFIP/IEEE International Symposium on Integrated Network Management*, pages 31–44, May 2005.

[19] Z. Quan and J. Li. Secure routing protocol cluster-gene-based for wireless sensor networks. In *Proc. The 1st International Conference on Information Science and Engineering (ICISE2009)*, pages 4098–4102, December 2009.

[20] J. Sen. A survey on wireless sensor network security. *International Journal of Communication Networks and Information Security (IJCNIS)*, 1(2):59–82, August 2009.

[21] R. Srinath, A. V. Reddy, and R. Srinivasan. Ac: Cluster based secure routing protocol for wsn. In *Proc. of the Third International Conference on Networking and Services*, page 45, Washington, DC, USA, 2007. IEEE Computer Society.

[22] M. Tubaishat, J. Yin, B. Panja, and S. Madria. A secure hierarchical model for sensor network. *ACM SIGMOD Record*, 33(1):7–13, March 2004.

[23] D. Wu, G. Hu, and G. Ni. Research and improve on secure routing protocols in wireless sensor networks. In *4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008)*, pages 853–856, May 2008.

[24] M. Ye, C. Li, G. Chen, and J. Wu. Eecs: An energy efficient clustering scheme in wireless sensor networks. In *Proc. of the IEEE International Performance Computing and Communications Conference*, pages 535–540, 2005.

[25] K. Zhang, C. Wang, and C. Wang. A secure routing protocol for cluster-based wireless sensor networks using group key management. In *Proc. 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*, pages 1–5, October 2008.