International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183810

A Survey on Hierarchical Cluster Based Secure Routing Protocols and Key Management Schemes in Wireless Sensor Networks

Yugashree Bhadane, Pooja Kadam
Department of Information Technology, Dhole Patil College of Engineering,Pune, Maharashtra, India

ABSTRACT

Now days, wireless technology is one of the center of attention for users and researchers. Wireless network is a network having large number of sensor nodes and hence called as "Wireless Sensor Network (WSN)". WSN monitors and senses the environment of targeted area. The sensor nodes in WSN transmit data to the base station depending on the application. These sensor nodes communicate with each other and routing is selected on the basis of routing protocols which are application specific. Based on network structure, routing protocols in WSN can be divided into two categories: flat routing, hierarchical or cluster based routing, location based routing. Out of these, hierarchical or cluster based routing is becoming an active branch of routing technology in WSN. To allow base station to receive unaltered or original data, routing protocol should be energy-efficient and secure. To fulfill this, Hierarchical or Cluster base routing protocol for WSN is the most energy-efficient among other routing protocols. Hence, in this paper, we present a survey on different hierarchical clustered routing techniques for WSN. We also present the key management schemes to provide security in WSN. Further we study and compare secure hierarchical routing protocols based on various criteria.

Keywords : Wireless Sensor Network (WSN), Routing, Hierarchical Cluster Based Routing, Key Management

I. INTRODUCTION

Current technological advances in microelectronic mechanical systems (MEMS) and wireless communication technologies have empower the development of small, low-cost, low-power, and multifunctional smart sensor nodes in a wireless sensor network (WSN). WSNs have been widely considered as one of the most important technologies for the twenty-first century [1],[2]. These smart sensor nodes are positioned in a physical area and networked through internet and wireless links, which provide novel opportunities for a variety of civilian and military applications, for example, battle field surveillance, environmental monitoring, and industry process control [3]. The development of wireless sensor networks was originally influenced by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, which include environment and habitat monitoring, healthcare applications, home automation and traffic control.

Generally a Wireless Sensor Network (WSN) is consists of a large number of wireless sensor nodes with low processing power and less energy consumption for monitoring a specific environment. These sensor nodes are small in size, but are equipped with radio receivers, power components to allow sensing, embedded microprocessors, computing, communication, and actuation. These components

are consolidated on a single/multiple boards, and packaged in a few cubic inches. The large number of such sensor nodes and their random placement in space offers great redundancy in data transmission. Therefore WSN are generally adaptive networks that use data aggregation and hierarchy to reduce energy consumption.

However this new technology poses many design goals, [4] that up until recently, have not been considered feasible for these applications.

Fig. 1 and Fig. 2 show the communication architecture of WSN. The sensor node is the principal component of a WSN. It is typically dispersed in a *sensor field* as shown in Fig. 1. Each of these dispersed sensor nodes has the capabilities to collect data and route data back to the *sink*. Data are sent back to the sink using a multi-hop infrastructure less architecture as shown in Fig. 1. The sink may interface with the *task manager node* through Internet and satellite. The layout of the sensor network as described by Fig. 1 is influenced by many factors, including scalability, hardware constraints, production costs, fault tolerance, operating environment, power consumption, sensor network topology and transmission media.

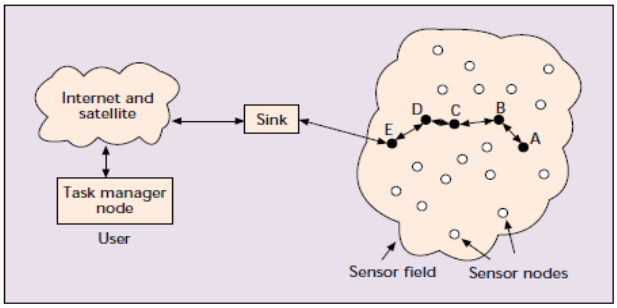

Figure 1 : Sensor nodes dispersed in a sensor field

A sensor node has following basic components, as shown in Fig. 2: a transceiver unit a sensing unit, a processing unit, and a power unit. They can have some additional application-dependent components also, such as a location finding system, power generator,
and mobilizer. Sensing unit is made up of two subunits: sensors and analog-to-digital converters (ADCs). ADC converts analog signals produced by the sensor to the digital signals and then fed into the processing unit. The processing unit, along with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to move out the allotted sensing tasks. A transceiver join the node to the network. The power unit is one of the most dominant component of a sensor node. Power units can be maintained by power scavenging units such as solar cells. Application-dependent subunits are also there. Most of the sensor network routing methods and sensing tasks need knowledge of location with high accuracy. Thus, we can say that a sensor node has a location finding system.

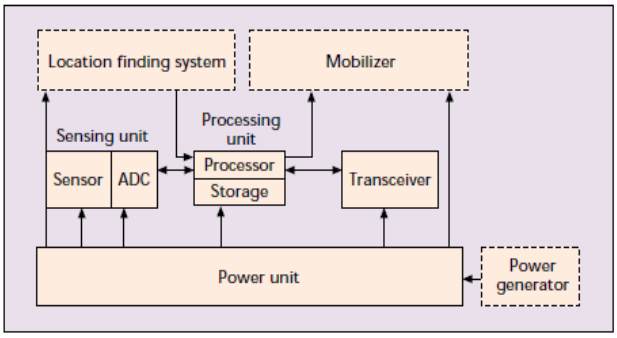

Figure 2 : The components of a sensor node.

Considering the network structure, routing protocols are categorized into 3 main groups:-

1. Flat
2. Hierarchical and cluster based
3. Location based

Among these three groups, especially hierarchical and cluster based routing protocols have substantial savings in total energy consumption of the WSN. Hierarchical and cluster based routing protocols creates clusters and a head node is assigned to each cluster. Each group has a head node which acts as a leader having responsibilities like collection and aggregation of data from their respective clusters and

transmitting the aggregated data to the base station. Such data aggregation in the head nodes greatly reduces energy consumption in the network by shrinking the total data messages to be sent to BS. If the less the energy consumption, the more the network life time. The key idea of developing cluster-based routing protocols is to minimize the network traffic toward the sink. Compared to flat network topologies for large-scale WSNs cluster-based protocols exhibit better energy consumption and performance. Fig. 3 shows the view of clustering.

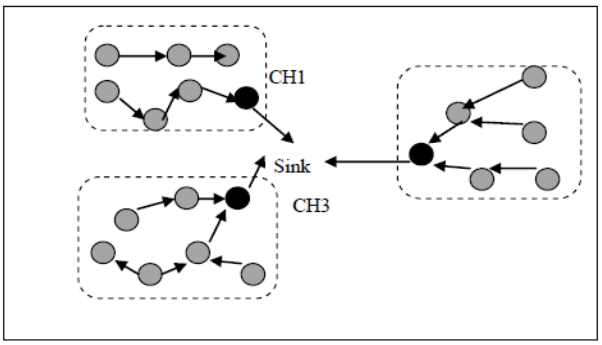

Figure 3 : Clustering

The remaining paper is organized as follows: Section II presents the literature survey over the related work. Finally, the section III concludes the review paper and gives the future directions to work ahead.

II. LITERATURE SURVEY

In this section, we have discussed previous research papers related to hierarchical cluster based routing protocols and the key management techniques in WSN. We are divided a literature survey in three categories:

1. Hierarchical Routing Protocols
2. Secure Hierarchical Routing Protocols
3. Key Management Schemes for WSN

A. Hierarchical Routing Protocols

Before knowing the Secure Hierarchical Routing Protocols, it is important to know the hierarchical routing protocols. Hierarchical or cluster-based routing, initially proposed for wired network to intensify scalability and efficiency. In WSNs, Hierarchical routing schemes are used to intensify energy-efficiency and hence extend the network lifetime. Data aggregation by cluster head, collision avoidance, uniform energy dissipation, lower latency, fair allocation of channel and reservation-based scheduling are some features of hierarchical topology routing protocol[5].

W. R. Heinzelman et al. [6] presented a Low energy adaptive clustering hierarchy (LEACH) protocol. It is one of the very first hierarchical routing protocol. LEACH involves distributed clustering and uses randomize rotation of cluster heads to evenly disperse the energy load in the network. It determines a threshold value to choose the cluster head. LEACH protocol is very helpful and functional for the applications, where continuous monitoring is required.

V. Loscri et al. [7] suggested a TL-LEACH which is an extension of the LEACH, where TL stands for Two-Level. It makes use of two level of clustering where primary cluster head(CH) communicate with secondary CH in order to send the data, for desirable throughput. TL-LEACH makes clusters based on minimum distance of nodes to their corresponding CH, EECS (Energy Efficient Clustering Scheme by M. Ye et al. [8] extends this by dynamic sizing of clusters based on cluster distance from the base station. CH election is dependent on the residual energy of the node.

S. Lindsey et al. [9] presented a Power-efficient Gathering in Sensor Information System (PEGASIS). It is a near-optimal chain-based protocol. Nodes in a PEGASIS need to communicate to its nearest neighbor and propagates to the base-station. Different from LEACH, PEGASIS avoids cluster formation and makes use of only one node in a chain to transmit to the base-station [5]. Like this, it

increases the lifetime of the network and permit only local communication for less bandwidth consumption in communication.

Furthermore to reduce the energy consumption of PEGASIS, S. Jung et al. [10] has been proposed a Concentric Clustering Scheme (CCS). CCS divides the whole network in co-centric circular tracks and each track presents a cluster. Depending on the distance from the base-station, track level has been assign to each track. Data communication is done through tracks. TSC protocol by N. Gautam[11], is the enhance version of CCS, it further divides tracks into sectors.

A. Manjeshwar et al. [12] has been presented a Threshold sensitive Energy Efficient sensor Network protocol (TEEN). TEEN is a data-centric protocol designed for time critical application. In this, the transmission of the sensed data is depends on the threshold values, called Hard Threshold (HT) and Soft Threshold (ST), which is broadcasted by CH. APTEEN by A. Manjeshwar et al. [13], is the enhance version of TEEN. The goal of TEEN is to capture both periodic data and time critical data. APTEEN assists three different query types: historical query, one-time query and persistent query [14].

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

B. Secure Hierarchical Routing Protocols

In order to secure the WSN, many hierarchical routing protocols work have been proposed. In this section we have discussed those techniques,

M. Bohge et al. [15] proposed a secure hierarchical routing protocol by using three tier ad hoc network topology. It used TESLA certificates for authentication. The message authentication code in the framework protects complete data against malicious modification as well as information forgery. Still, it cannot prevent intruders from coming inside the network and sending packets. Also, it cannot protect network against eavesdropping.

a. SRPSN

M. Tubaishat et al. [16] presented an energy-efficient level-based hierarchical routing technique. In this, a secure route from the source to sink node is build to safeguard WSN from different attacks. SRPSN uses symmetric key cryptography and proposed a group key management scheme. The drawback associated with this protocol is, while changing the CH it requires to compute inter-cluster and intra-cluster key once again, which is a complicated task.

b. LHA-SP

B. Parno et al. [17] proposed the first work which focused on securing heterogeneous hierarchical WSNs with arbitrary number of levels. It uses the symmetric key scheme and prevents outsider attackers to taking activity, tempering with or injecting message into the networks and prevents eavesdropping on communication between legitimate nodes. Authentication and confidentiality is preserve by shared pairwise key. It deals with orphan node problem.

c. F-LEACH

L. B. Oliveria et al. [18] proposed a FLEACH, it is a protocol for securing node to node communication in LEACH-based network. It uses random key pre-distribution scheme with symmetric key cryptography to increase security in LEACH. FLEACH provides confidentiality, integrity, freshness and authenticity to node-to-node

communication. But it is susceptible to node capturing attack.

d. SLEACH

A. C. Ferreira et al. [19] proposed the first modified secure version of LEACH called SLEACH, which provides security using clustered communication protocol for homogeneous wireless sensor networks. SLEACH safeguard against selective forwarding, sinkhole and HELLO flooding attacks. It prevents attackers to send bogus sensor data to the CH and CH to forward bogus message. Still, SLEACH cannot prevent to crowd the time slot schedule of a cluster, causing DoS attack or simply lowering the throughput of the CH and cannot guarantee data confidentiality. The solution is predestined to protect outsider attack only.

e. SHEER

J. Ibriq et al.[20] proposed a secure hierarchical energy efficient routing protocol (SHEER). It provides secure communication at the network layer. It makes use of the probabilistic broadcast mechanism and three-level hierarchical clustering architecture to refine the network energy performance and enhance its lifetime. To secure the routing SHEER implements symmetric key cryptography and HIKES (a secure key transmission protocol). The performance is compared with the secure LEACH using HIKES.

f. Authentication Confidentiality based Protocol.

R. Srinath et al. [21] proposed a protocol based on LEACH protocol; named as Authentication Confidentiality cluster based secure routing protocol. It uses both public key and private key cryptography. The protocol deals with interior adversary or compromised node. It is not efficient for the WSNs because of the high computational requirement (i. e. use of public key cryptography).

g. NHRPA

C. Hong-bing et al. [22] proposed a routing protocol that can adopt suitable routing technology for the nodes according to the distance of node to the base station, residual energy of the nodes and density of the nodes distribution. It does not uses any cryptography method in the routing protocol, so the overhead is less. But it is restricted only to deals with the node compromise attack.

h. Sec-LEACH

L. B. Oliveira et al. [23] proposed a Sec-LEACH protocol which provides an efficient solution for securing communications in LEACH. Sec LEACH uses random-key predistribution and μTESLA to enable secure hierarchical WSN with dynamic cluster formation. It applied random key distribution to LEACH, and introduced symmetric key and one way hash chain which provide freshness and confidentiality. In terms of security, Sec-LEACH provides authenticity, integrity, confidentiality and freshness to communications [35].

i. SS-LEACH

Di Wu et al. [24] introduced a secure hierarchical protocol called SS-LEACH, which is the secure version of LEACH. SSLEACH refines the method of electing cluster heads and builds dynamic stochastic multi-paths cluster heads chains to communicate to the base station, Like this way it improve the energy-efficiency and hence extends the lifetime of the network. SS-LEACH uses the key pre-distribution and self-localization technique to safeguard the basic LEACH protocol. It prevent weak node to take part in the network and conserve the secrecy of the packet. It evades selective forwarding, HELLO flooding and Sybil attack.

j. RLEACH

Secure solution for LEACH has been introduced by K. Zhang et al. [25] called RLEACH, in which clusters are formed dynamically as well as

periodically. They used improved random pair-wise key scheme to overcome the RLEACH orphan node problem. To provide security in the LEACH Hierarchical routing protocol RLEACH uses the one way hash chain, symmetric and asymmetric cryptography. RLEACH opposes to many attack like sinkhole, spoofed, selective forwarding, alter and replayed information, HELLO flooding, wormhole and Sybil attack.

k. ESMR

J. Chen [26] proposed an Efficient Security Model of Routing protocol (ESMR). It is the security solution for the LEACH. ESMR uses only public key cryptography technique. Test result shows that the ESMR is not as good as LEACH in attacker environment, but it becomes better when the number of attacker increases. The drawback of this protocol is, it only deals with out-sider attack and excessive computation burden is there due to the use of public key cryptography.

l. SRPBCG

Z. Quan et al. [27] presented a routing protocol called secure routing protocol cluster-gene-based for WSNs(SRPBCG). The election of CH is same as LEACH. This scheme the manages trust and reputation locally and authenticates identity of node with minimal overhead and time delay. SRPBCG scheme uses biological authentication mechanism which is a very effective authentication method. 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 is more in this protocol.

Fig. 4 shows the analysis of secure routing protocols based on the 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	✓	✓		✓	

Figure 4 : Secure Routing Protocols analysis based on security goals

C. Key Management Schemes for WSN

Key management techniques that have been surveyed so far can be categorized as follows [28, 29]:

a. Random key Pre-distribution scheme

Peer Intermediaries for Key Establishment (PIKE) [30] is an example of Random-key pre-distribution schemes. PIKE makes use of probabilistic techniques to establish pair wise keys between neighboring nodes in the network. In this scheme, each node has to store a large number of keys.

b. Master-key-based scheme

The nodes in this scheme share unique symmetric keys with the Base station. These keys are assigned before the network is deployed. This includes a significant pre-deployment overhead which is not scalable. Security Protocols for Sensor Networks (SPINS) [31], Localized Encryption and Authentication Protocol (LEAP) [32], are the examples of this scheme.

c. BS based scheme

Ibriq et al. [33] proposed a Hierarchical Key Establishment Scheme (HIKES). It is an example of BS based scheme. In BS based scheme, the base station acts as the intermediate trust authority and allows randomly selected sensors to act as local trust authorities. The nodes authenticate the cluster members and issue all secret keys on behalf of the base station. Hierarchical key establishment scheme

uses a partial key scheme that enables any sensor node selected as a CH to generate all the cryptographic keys required to authenticate other sensors within its cluster. The main problem with this scheme is the storage overhead of the partial key table in every node.

The notion of 'Secure Triple-Key Management Scheme' is proposed in [34]. The main drawback of the scheme is that it is the pre-development key management scheme.

III. CONCLUSION

The better performance of the network in terms of energy efficiency, security, resiliency and lifetime depends on the selection of protocol. So the secure, robust and efficient routing protocol is the basic requirement of WSN. Due to the insufficient energy resources of sensors, energy efficiency is one of the main challenges in the design of protocols for WSN. The key objective behind the protocol design is to keep the sensors operating for as long as possible, thus increasing the network lifetime. This paper provides a survey and summarizes recent research works focused mainly on the hierarchical cluster-based routing protocols for WSNs. Also, we have surveyed the key management schemes for providing security in WSN. Based on the topology, the protocol and routing strategies can be applied. The factors affecting the cluster head communication and cluster formation are open issues for future research. Moreover, the process of data aggregation and fusion between the clusters is also an interesting problem to explore. The information provided in this paper would be useful for the researchers to work in this area.

IV.ACKNOWLEDGEMENT

We are thankful all who give their valuable guidance to us.

V. REFERENCES

[1]. 21 ideas for the 21st century., Business Week, Aug. 30 1999, pp. 78-167.

[2]. Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[3]. CY. Chong and S.P. Kumar, "Sensor Networks: Evolution, opportunities, and Challenges", Proceedings of the IEEE, vol. 91, no. 8, Aug. 2003, pp. 1247-1256.

[4]. I F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Surveyon Sensor Networks," IEEE Communications Magazine, vol. 40, no. 8,pp. 102-114, Aug 2002.

[5]. 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.

[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]. V Loscri, 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.

[8]. 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.

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

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. M. Bohge andW. 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.

[16]. 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.

[17]. 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.

[18]. 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.

[19]. A. C. Ferreira, M. A. Vilaca, 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.

[20]. 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-U? 6, Singapore, October 2006.

[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]. 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.

[23]. L. B. Oliveira, A. Ferreira, M. A. Vilaca, 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.

[24]. 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.

[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.

[26]. 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.

[27]. 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.

[28]. Zhou, Y., and Fang, Y. (2007), 'A two-layer key establishment scheme for WSN'. IEEE trans. Mobile Computing, Volume 6, No. 9, pp: 1009-1020.

[29]. Zhou, Y., Fang, Y., and Zhang, Y. (2008), 'A survey of Securing Wireless Sensor network'. IEEE communication surveys, Volume 10, No. 3, pp: 6-28.

[30]. Chan, H.,and Perrig, A., (2005), 'PIKE: Peer Intermediaries for Key Establishment in Sensor Networks'. In Proceedings of IEEE Infocom, Miami, Florida, pp: 524-535.

[31]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J.D.Tygar. Spins: Security protocols for sensor networks. Wireless Networks, 8:521 - 534, 2002.

[32]. Zhu, S., Setia, S., Jajodia, S. (2003) 'LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks', CCS '03, Washington D.C., USA, 27 - 31 October 2003, New York, USA: ACM Press, 62-72.

[33]. Ibriq, J., and Mahgoub, I. (2007), 'A Hierarchical Key Establishment Scheme for Wireless Sensor Networks'. 21st International Conference on Advanced Networking and Applications, pp: 210-219.

[34]. T.A Zia and A.Y. Zomaya, 'A Secure Triple-Key Management Scheme for wireless sensor networks', in the proceedings of INFOCOM 2006,25th IEEE International Conference on Computer Communications, Barcelona, pp1-2 ,23-29 April 2006

[35]. Naser Alajmi. Ac: Wireless Sensor Networks Attacks and Solutions. In International Journal of Computer Science and Information Security, page 45, Bridgeport, USA, Volume 12, No. 7, July 2014.