Addressing Secure Data Routing Scheme for Heterogeneous Sensor Networks

Pardeep Kumar[1], Md. Iftekhar Salam[2], Sang-Gon Lee[3], HoonJae Lee[4]
[1,2]Department of Ubiquitous-IT, Graduate School of Design & IT
[3]Division of Computer & Information Engineering
[4]Division of Information Network Engineering, School of Internet Engineering
Dongseo University, Busan, 617-716, South Korea

Pardeepkumar@dit.dongseo.ac.kr, iftekharsalam@yahoo.com, nok60@dongseo.ac.kr, hjlee@dongseo.ac.kr

***Abstract*- In wireless sensor networks (WSNs); routing protocols are one of the main issues in existing research. These protocols make the best use of limited resources, particularly the energy efficiency and effectiveness of data dissemination. Few of them discuss security issues in homogenous sensor networks which consume much power, have poor performance limits and less scalability. In order to attain the high performance, we have chosen heterogeneous sensor networks (HSNs) model. In this paper, we are addressing secure data routing (SDR) scheme based on cryptography for heterogeneous sensor networks. We have incorporated following mechanism in SDR scheme: 1) symmetric-session based key system is proposed, which change session key after session expire; 2) efficient secure data routing scheme is proposed; 3) cluster-head selection technique is discussed. This is a novel scheme for non-secure sensor network application. In addition, we devote special attention to facilitate the secure routing against some popular attacks, such as: sinkhole, wormhole, sybil and selective forwarding attacks.**

Keywords: secure data routing, stream cipher, heterogeneous sensor networks

I. INTRODUCTION

Wireless sensor network is an emerging technology in existing research. Sensors bringing information to human's life, to make life more comfortable. WSNs have become popular solutions to many challenging domestic, commercial, military, healthcare, environmental and agricultural applications [1]. These sensor nodes collectively monitor the area and generates substantial amount of data, which is transmitted to base-station with the help of one node to another node via radio frequency signals and routing algorithms.

Routing is a critical function in sensor networks. Many protocols and algorithms have been proposed for wireless sensor network routing, such as direct-diffusion, energy-efficient and geographic routing etc. Generally, these schemes are focused on making WSNs more feasible, useful, and to increase network life time. However, most of routing protocols do not consider security issues during the protocol design phase and some protocol addresses security only, but no implementation.

In fact, providing security in sensor network is not an easy task as compare to traditional networks. Wireless sensor networks are very resource hungry, having low power, less memory, and limited computation. Unlike traditional networks, sensor networks are always deployed in hostile and unattended environment to execute their task. It seems WSNs routing are more vulnerable to attacks, which are more difficult to launch on wired networks.

Moreover, multihop routing schemes also has many vulnerable characteristics. Therefore, WSNs faces many threats and also more prone to attacks. Thus, secure routing has emerged as one of the most important issues for sensor networks.

So far, few security researches have been developed for sensor networks called SPINS [2], TinySec [3], MiniSec [4], INSENS [5] and Dragon-MAC [6, 7]. These schemes can prevent only from some outside attacks but no mechanism for inside attacks such as: selective forwarding, sybil, wormhole, sinkhole and other attacks.

So, to attain high secure routing for sensor networks, security must be considered at the designing time of routing protocol. Secure routing ensures wireless sensor network is secure for data communications.

Generally, wireless sensor network are composed of homogeneous and heterogeneous sensors. A homogeneous sensor networks, where all nodes have same configurations, in terms of energy supply, computation, memory, reliability and communications. Furthermore, a large scale of homogeneous sensor network requires high hardware cost and also suffers from poor performance and scalability. Performance of homogeneous sensor networks are demonstrated theoretically [8] and simulation analysis [9].

While on other hand, heterogeneous sensor networks are deployed with small number of high-end sensors having higher communication and computation capabilities, in addition to large number of low-end sensors. For example, a sensor network deployed with MICA2 [16] or T-MOTE [17] technology and as well as more powerful PDA (Personal Digital Assistants). Several recent advanced researches had adopted heterogeneous sensors for better performance and scalability [10]-[13]. Furthermore, a performance comparison between homogeneous and heterogeneous sensor networks is shows that heterogeneous sensors have significant improvement on homogeneous sensors [14, 15].

So in this paper, we have taken up above resource challenges, performance issues with homogeneous sensor networks and

addressing new secure data routing scheme (SDR) for heterogeneous sensor networks. The contribution of our work includes: 1) symmetric-session based key scheme proposed for secure data communication; 2) a novel efficient secure routing scheme proposed for heterogeneous sensor networks; 3) efficient cluster-head selection techniques is discussed.
The rest of the paper is organized as follows: In section II, discuss the data routing network model for HSNs, and section III detailed discussion of proposed secure data routing (SDR) scheme. In section IV, analysis of SDR scheme and section V, conclusion and future work.

II. DATA ROUTING NETWORK MODEL FOR HSNs

A heterogeneous wireless sensor network consists of a base station and a number of sensor nodes which are grouped into clusters. Our HSNs network model is composed of: 1) low-capability sensor nodes (SN); 2) small number of special purpose high-capability sensor nodes for cluster-head (CH) and, 3) base station (BS) that have unlimited resources as shown in fig 1. We have assumed that, low-capability sensor nodes and special purpose high- capability sensor nodes are uniformly and randomly deployed in the network field. As shown in fig 1, where small circles are low-capability sensor nodes and black rectangles are high-capability cluster-head that have more power supply, longer transmission range, higher data transfer rates than low-capability sensor nodes. SN communicates with cluster-head which is represented by dark solid black lines and cluster-head communicates with other CHs or base station by red dotted lines.

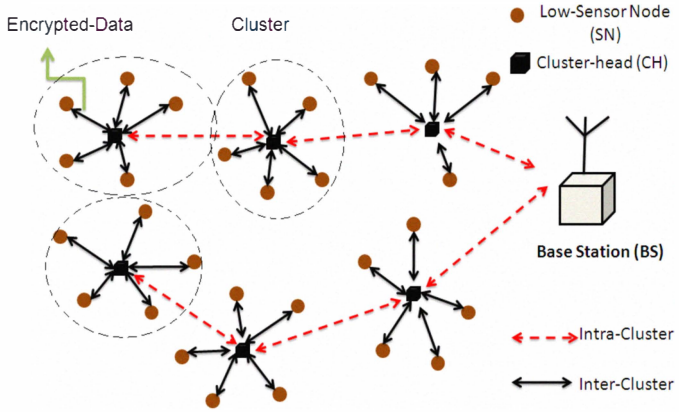

Fig. 1. Data routing network model HSNs

We have made the following assumptions for network model:

- All node's locations are static, i.e., mobility is not supported.
- The CH can directly reach to each node in its cluster.
- Sensor nodes communicate with the CH within their cluster via one or multihop.
- Due to cost constraints low-sensor are not equipped with tamper-proof hardware. It may happen, if low sensor is compromised by an adversary, then he/she can get all information from nodes.
- It is assumed that each CH is equipped with tamper-proof hardware.
- The BS is considered as trusted party.

III PROPOSED SECURE DATA ROUTING (SDR)

This section have two following parts: 1) tasks of different sensor nodes and 2) addressing the details of secure data routing scheme based on symmetric key cryptography for heterogeneous sensor networks. Our new SDR is incorporated with following: *A)* a symmetric-session based key scheme is used, which change new session key after session expires; *B)* secure routing scheme which route data from SN-to-CH, CH-to-CH and CH-to-BS; *C)* cluster-head selection techniques. SDR notations are shown in Table- I.

TABLE I
SDR NOTATIONS

Notation	Description
BS, CH, SN	Base-station, Cluster-head, Sensor node
CH_id	Cluster-head Id
S_id	Sensor id
S_{key}	Session Key
NS_{key}, CS_{key}	New Session key, Current session key
F()	Pseudorandom number function
E () , D()	Encryption and Decryption function
Pkt_i	Packet with i^{th} index
CH_{ctr} , BS_{ctr}	Cluster-head and base station counter
R	Random numbers
||	Concatenation operator
PP-MAC	PingPong Message Authentication Code

1). Tasks of different sensor nodes:
We have divided tasks of different nodes as following:

Task of Sensor Node (SN)

- Every sensor nodes encrypt the data packets. For data encryption PingPong-128 [18] stream cipher is used.
- Then encrypted data is transmitted to CH node.
- Received packets at CH node and update session key based on packets (*pkt*).

Task of Cluster-head (CH)

- At the CH, a counter (*ctr*) and its own ID is appended to all received data packets from all sensors.
- Aggregate the received data packets by applying the redundancy factors such as: MIN, MAX, AVG function and route aggregated data packets to the base station.
- Receives new session key from BS and sends this key to all its CHs and all clusters' sensor nodes.

Task of Base-station (BS)

- All received data packets will be decrypted and integrity will be checked for every packets.
- Base station generates new session keys and sends to CH whenever its session key is expired.

2). This part is discussed the details of secure data routing scheme based on symmetric key cryptography for heterogeneous sensor networks:

A). Symmetric-session based key scheme

A numbers of key establishment schemes based on pre-distribution have been explored recently [19]-[21]. Furthermore, a comparison of symmetric-key and public-key is shows that symmetric key based schemes are computationally efficient [22] for sensor networks. So we are proposing a symmetric-session based key scheme for heterogeneous sensor networks. In our scheme, base station (BS) is used as trusted party for key setup. Every sensor and cluster-head have unique sensor id (*S_id*) and cluster-head id (*CH_id*), respectively. Initially, it is assumed that base station and all sensor nodes share symmetric session key (S_{key}) to secure their communication. The symmetric session key is updated regularly. Initially, a PingPong-123 stream cipher is used to encrypt the sensors packet[1] (Pkt_i), and then encrypted data is transmitted to cluster-head (CH), which makes more secure data communication. After completing current session, BS will generate a new session key (NS_{key}) using pseudorandom function (*f*). New session key and current session key (CS_{key}) is send to corresponding CH. A new session key (NS_{key}) is broadcast to the corresponding CH sensors to encrypt the data for a new session. By doing so, session key has updated dynamically for every new session, as shown in fig 2.

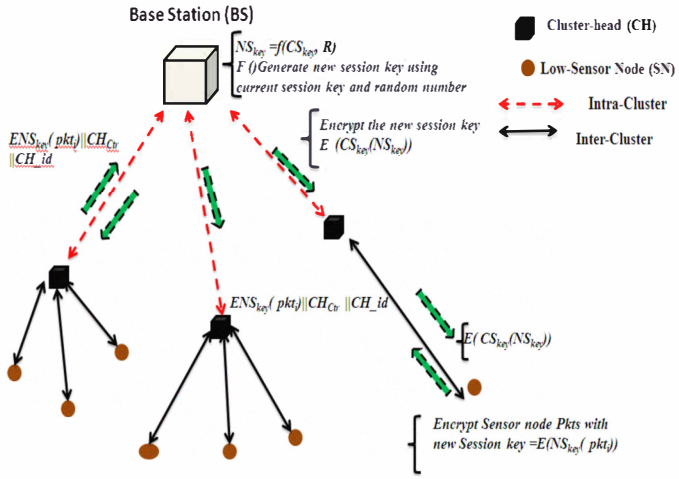

Fig. 2. Encryption and session key transmission

A PingPong-MAC[2] (PP-MAC) scheme is computed to provide entity authentication by the use of dynamically changing user specific session keys. These session keys are produced by BS (Base station) and send to CH (cluster-head) and CH again broadcast to its own (SN) sensor nodes.

1. PingPong-128 stream cipher

A PingPong-128 [18] stream cipher is proposed by HoonJae Lee and Kevin Chen. PingPong family is based on summation generator stream cipher with addition of mutual clocked control structure. This algorithm is designed with both security and efficiency in mind to satisfy the need for lightweight algorithms. PingPong is highly secure algorithm, dedicated to hardware environment and easy to implement in software. PingPong-128 is a bit based stream cipher. This stream cipher is constructed on two mutually clocking LFSRs and a single memory bit. PingPong-128 accept key as 128-bits and 128-bits initialization vector to feed the internal states. It generates an output block of 128 pseudo-random bits from a combination of the internal states, for every iteration. PingPong-128 has 257-bits of internal state. For the detailed specification, refer to [18].

B). Secure data routing scheme

In order to design secure data routing scheme, we have divided SDR scheme into three phases:

1). Sensor Node to Cluster-Head

Routing from sensor node to cluster-head is also referred to as intra-cluster routing. An i^{th} sensor node (SN_i) encrypts the i^{th} packet (Pkt_i) by using the session key (S_{key}), which is assigned at the deployment time network. Then encrypted packets are sending to cluster-head (CH_i).

$$\begin{cases} SN_i \longrightarrow CH_i \\ CH_i = ES_{key}(Pkt) \end{cases}$$

2). Cluster-Head to Cluster-Head (CH-to-CH)

Routing within cluster-head to cluster-head is also referred to as inter-cluster routing. CH-to-CH routing performed followings:

a) Cluster-head concatenates the received encrypted packets (*pkt*) from its own sensor nodes and other cluster-heads on the path to the base station.
b) Increment the value of cluster-head counter (CH_{ctr}) by one and appends it to concatenated packet (Pkt_i).
c) Cluster-head also concatenates its own id (*CH_id*) and send it to next cluster-head on the path to the base station.

$$\begin{cases} CH_i \longrightarrow CH_n \\ CH_n = ES_{key}(pkt) \,||CH_{ctr}||CH\_id \end{cases}$$

3). Cluster-Head to Base station (CH-to-BS)

CH-to-BS is following same communication as CH-to-CH. Finally, base station has received concatenated encrypted packets from the cluster-head.

$$\begin{cases} CH_n \longrightarrow BS \\ BS = ES_{key}(pkt) \,||CH_{ctr}||CH\_id \end{cases}$$

[1]Packet and data used interchangeably.
[2]MAC represent as Message Authentication Code

After receiving the encrypted packets, BS will perform following action on encrypted packets, to extract original data: BS decrypts the encrypted packets by using current decryption session key DSkey.

$$\{ DS_{key}(ES_{key}(pkt) \,||CH_{ctr}||CH\_id \;)$$

If ($CH_{ctr} \geq BS_{ctr}$), by means data is authentic:
i.e. original packets will be extracted by applying current decryption session key:
$DS_{key}(pkt') \longrightarrow$ original Packets (pkt).
If ($CH_{ctr} \leq BS_{ctr}$), then BS either discard the packet (pkt) or again send a retransmission request to the CH.

a) To check the counter (ctr) value, BS extracts CH_id from pkt. To check the valid CH_id of cluster-head, BS compares the appended CH_{ctr} with the least value of BS_{ctr} value.
b) Verify CH_id in the packets.
c) BS increment its ctr value by one, after expiry of current session and new session key is generated by using the pseudorandom function (f) and current session key.
d) The new session key is a function of current session and random number R.
i.e. $NS_{key} = f(CS_{key}, R)$, where R is random number.
e) As shown in fig 2, BS will update new session key for next session as follows:
BS encrypt the new session key (NS_{key}) by using CS_{key} and send to corresponding CH. CH broadcast new session key NS_{key} to its own sensor nodes and sensor nodes updates its session keys, with new session key.

C). Cluster-Head (CH) Selection Scheme

Generally, a heterogeneous sensor network have three types of sensors: low-power sensor node (SN), small number of special purpose high-capability sensor nodes for cluster head (CH) and, base station (BS) that have unlimited resources. In heterogeneous sensor network CHs are very important for many applications and effective selection of CH can increase the energy- efficiency, network lifetime and scalability of sensor network. Each cluster has a cluster-head and establishes its own area. This CH collects the data from their area and transmits to base station (BS), as final destination. For the selection of CH, we have made some assumptions:

- The whole sensor network is divided into several clusters and each cluster has its CH.
- The selection criteria for CHs are weighted by the initial energy of node.
- In our scheme, CH is some resource rich nodes, which are permanently selected as a CH. Furthermore, static CH concepts always reduce the energy consumption.

Cluster-head is selected based on two parameters, when they are deployed in networks; 1) weight of cluster-head, and 2) minimum reach-ability power of sensors.

1). Weight of cluster-head (CH): it is the sum of average distance from CH to neighbor CH, distance from CH to BS and battery power of the CH.

$$\{ W_c = P_c + D_c$$

Where W_c= Weight; P_c is power and D_c is Distances.

An average distance is calculated based on strength of the broadcasted message, which is broadcasted by CH to BS at the time of deployment of networks.

$$\{ WD_c = (P_{tx}/P_rx)\,(\lambda/4\pi)^2$$

Where P_{tx} is transmission power of sending node, P_{rx} is remaining power after receiving power at sensor node and λ is wavelength and d corresponds to the transmission distance.

2). Minimum reachability power (MRP): A minimum reachability power is required for each sensor node within a cluster area (a) to communicate effectively with CH. Sensor nodes calculate average on MRP based on strength of the CH message which is broadcasted by CH and based on average MPR each sensor node choose its CH. Furthermore, the CH which has single hop or least distance closer to the BS is selected as CH.

IV. ANALYSIS OF SDR (Secure Data Routing) Scheme

In this section, we have analyzed the SDR scheme. By applying symmetric PingPong-128[18] stream cipher, we achieve data confidentiality, data authentication and data integrity. The security configuration is discussed below.

A.) Confidentiality: data confidentiality is a service, in which data is used by only authorized users. In sensor networks, data should not be leaked to neighboring node because sensor deals with very sensitive data. In order to provide the security, the data should be encrypted with secret key. Secret key is intended to recipient only; hence confidentiality is achieved by applying of PingPong-128 stream cipher.

B.) Entity Authentication: Authentication service is associated to identification. Entity authentication function is important for many applications and for administrative task. Authentication allows to receiver, to verify that the data is really sent by authenticated sender or not. In node-to-node communication entity authentication can be achieved through symmetric mechanism: a message authentication code (PingPong-MAC) is computed on secret shared key for all communicated data.

C.) Data Integrity: data integrity is a service, which addresses the illegal alteration of data. To conformation of data integrity, one must have the ability to identify data manipulation by illegal parties.

SDR scheme can defend against typical attacks on the sensor network routing. Attacks on sensor networks have been presented in several papers [23]-[25]. Most of the popular network layer attacks against sensor network fall into following categories sybil [23], sinkhole and wormhole [24],

and selective forwarding attacks [25]. A brief introduction of these attacks can also be found in [26].

D.) Secure against the Sybil Attack: In Sybil attack, a malicious node presents multiple fake identities to other neighboring nodes in the network. By the use of entity authentication, it ensures that one node cannot pretend to be other, i.e., when a sensor node *i* send a packet to another node *j*, *i* must compute MAC using the MAC key (*km*) between *i* and *j*. Since the MAC key (*km*) is only known by *i* and *j*, no adversary node can pretend to be node *i* (unless *i* is captured and the keys in *i* are obtained by the adversary). Thus, the Sybil attack does not work.

E.) Secure against the Wormhole and Sink-hole Attacks: SDR routing having three parts: SN-to-CH routing, CH-to-CH, and CH-to-BS routing. For SN-to-CH routing, low-sensor only transmits data to its CH node and this is determined by the cluster head. For CH-to-CH routing, locations are static for the CH-to-CH and the packets are forwarded only by appending the own ID of cluster head to next CH. Other nodes should not participate in routing. An adversary is not able to route in SDR, and hence, SDR is resistant to wormhole attack and sink-hole attack.

F.) Secure against the Selective Forwarding Attack: CH nodes are the tamper-proof hardware, hence CH cannot be compromised, and the selective forwarding attack cannot be applied on CH. However, selective forwarding attack may attack on low-sensor. Furthermore, malicious nodes can refuse to forward the certain packets and simply drop them. For example, a powerful adversary always serves as a relay node in a cluster, and he/she can selectively forward some packets while dropping other packets. The packet index (pkt_i) field is used to defend this attack. The packet index field is used to identify the particular packet. If a node selectively drops a packet, this will be detected by the up-stream sender.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a novel and secure data routing scheme for heterogeneous sensor network. It is noticed that a well-planned secure routing mechanism must be designed for successful deployment of secure sensor network. In this respect we have addressed secure data routing scheme (SDR) based on symmetric key cryptography for heterogeneous sensor networks, which enforces the fact that if a data routing scheme is secure then people trust on it.

Now, continued research into the suitability and efficient secure data routing scheme will be carried out through both real-time implementation and simulation. Still more work and efforts are required in secure data routing scheme for heterogeneous sensor networks.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramamiam and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communication Magazine*, August 2002, pp. 102-114.

[2] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", Procd of 7th Annual International Conference on Mobile Computing and Networks (MOBICOM 2001), Rome, Italy July 2001.

[3] C. Karloff, N. Sastry and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), Baltimore, MD, November 2004.

[4] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A Secure Sensor Network Communication Architecture" IPSN'07, April 2007, Cambridge, Massachusetts, USA.

[5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing in wireless sensor networks," Technical Report CU-CS-939-02, University of Colorado, Deptt. Of Computer Science.

[6] P. Kumar and H. J. Lee, "A Secure Data Mechanism for Ubiquitous Sensor Network with Dragon Cipher", IEEE 5th International Joint Conference on INC, IMS and IDC, 2009.

[7] S. Y. Lim, C. C. Pu, H. T. Lim, and H. J. Lee, "Dragon-MAC: Securing Wireless Sensor Networks with Authenticated Encryption", 2007. [http://eprint.iacr.org/2007/204.pdf].

[8] P. Gupta and P. R. Kumar, "The Capacity of Wireless Network," *IEEE Trans. of Inform. Theory*, vol. 46 pp. 388-404, 2000.

[9] K. Xu, X. Hong, and M. Gerla, " An adhoc network with mobile backbones," *in proc. IEEE ICC*, apr ,pp. 3138-3143.2002.

[10] Md. A. Razzaque, M. M. Alam, Md. M-O Rashid, and C.S Hong, "Multi-Constrained Qos geographic routing for heterogeneous traffic in sensor network," *IEICE Trans. commun.* Vol. E91-B, No.8, pp. 2589-2601, Aug 2008.

[11] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, y. Liu, and S. Singh, "Exploiting Heterogeneity in sensor networks," *in proc. of IEEE infocom 2005.*

[12] V. Paruchuri, A. Durresi, "Energy aware routing protocol for heterogeneous wireless sensor network," *16th international workshop on database and expert system application (DEXA'05)*, 2005.

[13] K.J. Kaur, X. Du, and K. Nygard, "Enhanced routing in heterogeneous sensor networks," *in proc. of IEEE computation world'09*, 2009.

[14] V. Mhatre and C. Rosenberg, "Homogeneous and Heterogeneous clustered sensor network: a comparative study," *in proc of IEEE ICC'04*, 2004.

[15] P. Samundiswary, P. Priyadarshini and P. Dananjayan, "Performance analysis of homogeneous and heterogeneous sensor networks," *MASAUM journal of computing*, vol.1, no. 3, Oct. 2009.

[16] http://blog.xbow.com/xblog/mica2_mote/.

[17]http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf

[18] H. J. Lee and K. Chen, "A New Stream Cipher for Ubiquitous Application," ICCIT, 2007, South Korea.

[19] X. Du, M. Guizani, Y. Xiao, and H-H Chen, "Two tier secure routing protocol for heterogeneous sensor networks," *IEEE trans. on wireless communications,* vol 6, no.9, Sep. 2007 pp. 3395-3401.

[20] F. Kausar, M. Q. Saeed, and A. Masood, "Key management and secure routing in heterogeneous sensor networks," IEEE international conf. on wireless and mobile computing, networking and communication, 2008, pp. 549-554.

[21] X. Cao, G. Chen, and B. Yu, "Providing resource oriented security solution for heterogeneous clustered sensor networks," *IEEE inter. conf. on mobile adhoc and sensor networks,* 2006, pp. 729-734.

[22] H. Wang, B. Sheng, C. C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: a case study of user access control," *Proc. of the 28th International Conference on Distributed Computing Systems*, 2008.

[23] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis and defenses," *ISPN,04*, 2004.

[24] A. A. Pirzada and C. McDonald, "Circumventing sinkhole and wormhole in wireless sensor network," *IWWAN* 2005.

[25] B. Yu and B. Xiao, "Detecting Selective forwarding attacks in wireless sensor networks," *IPDPS'06*, 2006.

[26] C. Karlof, and D. Wagner, "Secure routing in wireless sensor network: attacks and countermeasures", *ELSEVIER, Adhoc networks*,1 (2003) 293-315.