ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Algorithm and Architecture for Control of Wireless Sensor Networks

G.Kalpana, T.Bhuvaneswari, S.Ravi
Research Scholar Dr.M.G.R Educational and Research Institute University, Govt. Arts and Science College Ponneri, Dr.M.G.R Educational & Research Institute University

Abstract - Sensor nodes in a Wireless Sensor Network (WSN) organize themselves into a cooperative network and perform the three basic functions of sensing, computations and communications. Energy constraints of the sensors pose a major challenge and have become an extensive research in WSN. An event driven secure topology discovery algorithm for a WSN is proposed where individual nodes are responsible for sending update messages to the base station when they detect a topological change in their own descendent sub tree. The collision between neighbour nodes has been minimized Denial of Service (DOS) threats and countered and hence the lifetime of the nodes been prolonged thereby improving the robustness of WSN.

Index Terms: **Optimization Algorithm, Secure Topology Discovery, WSN**

I. INTRODUCTION

Multiple sensor nodes deployed densely in a common neighborhood to sense an event and subsequently transmit sensed information to a remote processing unit or base station, has been the recent focus of research [17]. These tiny sensor nodes (fabricated using micro-electro-mechanical systems (MEMS) technology) perform sensing, data processing, and communication and leverage the idea of sensor networks based on collaborative effort (unlike traditional networks) [2]. These numerous sensors can deliver crucial information in real-time from environments and processes, where data collection is impossible previously with wired sensors. Major beneficiaries of wireless sensor networks (WSNs) include environmental monitoring, monitoring of quality of good (especially perishable items), climate monitoring, monitoring the health status of building structure, medical, public safety, transportation, military etc [3]. Their emergence has enabled observation of the physical world at an unprecedented level of granularity. However, these WSNs have extreme energy constraints (as the power unit of a sensor node in most applications is supported by scavenging unit such as solar cells) and need to integrate general purpose computing with heterogeneous sensing and perform wireless communication [3]. Also, wireless networks are subject to various kinds of attacks and wireless communication links can be eavesdropped on without noticeable effort and communication protocols on all layers are vulnerable to specific attacks and injection of false messages (in contrast to wire-line networks) [22]. Emerging applications of WSNs demand an inherently increasing degree of dynamics of their topology (due to mobility and joining/leaving devices), and deploying security mechanisms becomes difficult [27]. Also, there exist limited resources of end systems, bandwidth restrictions and possible asymmetrical communication links [1].

In this context, this research work focuses on algorithms that include energy – efficient routing protocols along with the management and diagnosis of dynamically changing network topologies and collision detection. The issues addressed in this work assists in maintaining network integrity and maximize its lifespan [18]. Topology management and control has been the main focus of this research, since it helps to achieve the global objective of extending the network lifetime (in addition to improving network performance). The proposed solution exploits a cluster overlay, where the cluster head nodes form a distributed service registry which results in visiting only the cluster head nodes [4,5]. This results in minimizing the communication costs during discovery of services and maintenance of a functional distributed service registry. The algorithms presented in this work, makes decisions based on 1-hop neighborhood information and can avoid chain reactions and help in constructing a set of sparsely distributed cluster heads [4]. These sparsely distributed cluster heads allows for uniform energy consumption and greater spatial reuse, which results in greater throughput [14]. The proposed algorithm is able to tackle the denial of service attacks present in a WSN [19]. The performance and trade-offs between the proposed secure topology (cluster based) algorithm and the traditional solutions are also presented.

II. LITERATURE REVIEW

Gang Xiong and Shalinee Kishore [13] propose a novel discrete-time second-order distributed consensus time synchronization (SO-DCTS) algorithm for wireless sensor networks. The consensus properties and convergence rates of the SO-DCTS algorithm are analyzed for both directed and undirected networks. Additionally, the convergence region and optimal convergence rate of the SO-DCTS algorithm are determined for undirected

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013
networks and this convergence rate is shown to be superior to that of the discrete time first order distributed consensus time synchronization (FODCTS) algorithm under careful algorithm design. Furthermore, the asymptotic expectation and mean square synchronization error are investigated for the SO-DCTS algorithm when there is Gaussian delay between network nodes. Finally, simulation results are provided to verify these analytical results.

Routing is an important issue in any type of networks. Multiple-hop based routing in sensor networks suffer performance downgrade from too many hops with the increase of the size of sensor nodes, as well as various attacks. A number of approaches have been proposed for routing in sensor networks, but they lack of sufficient support for secure routing in large-scale sensor networks. Feilong Tang. et. al., [11] propose a scalable and secure routing protocol that can work energy-efficiently and resist most of attacks. By hierarchical and long-distance mesh routing, their protocol significantly reduces average number of hops for data transmission. Lightweight security mechanism enables the routing protocol to survive from most attacks against sensor networks.

Previous architectures of pervasive computing are customized for specific types of applications. Daqiang Zhang et. al., [8] proposes a new architecture named iShadow, which facilitates the design and implementation of generic applications in pervasive computing environment. iShadow gracefully integrates physical spaces and human attention, and provides fundamental and flexible support to construct pervasive applications rapidly. Significant differences of iShadow from previous works are lightweight user-shadow model, scalable resource discovery and potent context inference mechanism. The prototypes demonstrated shows that the iShadow architecture is robust, feasible and effective for pervasive applications.

Wireless mesh sensor network (WMSN) merges advantages of wireless mesh networks and wireless sensor networks, especially on scalability, robustness and balanced energy dissipation. Routing in WMSNs faces with more challenges than that in traditional sensor networks on account of multiple sink nodes and the mobility of nodes. Work proposed by Minyi Guo, et.al., [12] focuses on two challenging problems. Firstly, they propose a reliable architecture of WMSNs by deploying multiple mobile mesh nodes in each sensor network to collect sensed data, which improves the scalability and performance of WMSNs. Also, they design a routing protocol characteristic to WMSNs. The routing protocol aims at maximizing the lifetime of sensor networks by reducing total energy consumption of a sensor network, as well as balancing energy usage among sensor nodes.

Deployment of sensor networks is concerned with setting up an operational wireless sensor network in a real-world setting. Unfortunately, deployment is a labor-intensive and cumbersome task as environmental influences often degrade performance or trigger bugs in the sensor network that could not be observed during lab tests. In this context, Ringwald .M. and Romer K. [22] study existing sensor networks to identify and classify typical problems that have been encountered during deployment. They further investigate whether and how the existence of these problems can be detected by means of passive inspection, where messages exchanged in the sensor network are overheard and analyzed such that modification of the sensor network is not required. They also show how passive inspection can be implemented in a practical tool.

III. OBJECTIVES OF THE PRESENT WORK

The primary objective of this research work is

1. To focus on issues concerning the generation, maintenance and retrieval of the topology of sensor networks. This is highly essential since post-deployment the topology of a WSN is susceptible to frequent change [29].
2. To propose a secure topology discovery algorithm for a WSN that is event driven where individual nodes are responsible for sending update messages to the base station when they detect a topological change in their own descendent sub tree. This is in contrast to other reported methods [6,9] which uses a demand driven based approach, where the topology of the sensor network can be extracted.
3. To optimize the routing table and effectively route the data in the network layer and to design a power aware Medium Access Control (MAC) protocol (where the environment is noisy and sensor nodes can be mobile) [7, 21, 28]. This is possible using self organizing nodes into a logical communication network structure using which data can be routed, hop by hop, from source to destination.
4. To minimize collision with neighbors during broadcast and to effectively detect the aberrant nodes and eliminate them (robustness) [15].
5. To effectively counteract the Denial of Service (DOS) threats [19] and hence, prolong the lifetime and improve robustness of wireless sensor networks.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

IV. METHODOLOGY

We select schedule – based medium access as the most appropriate channel sharing method for wireless sensor networks. In schedule based medium access, each node uses its receiving and transmitting functionality according a schedule. As such, the medium can be shared conflict free and high peek loads can be sustained without inducing energy-wasting collisions [21]. These are requirements for wireless sensor networks.

We combined schedule-based medium access control with backbone creation that identifies redundant wireless sensors. These redundant wireless sensor nodes (i.e. passive nodes) are not required in multi-hop forwarding and can thus save energy by following a sleep pattern. This backbone maintains connected and dominating structures that keep the overall network operational. Many time slots per frame are required in dense networks and consequently message delay is significant. However when using the backbone creation, the number of required timeslots can inherently be reduced, because many nodes realize their redundancy, give up their time slot and become passive. With an eye to limited capabilities of wireless sensor node, proposed medium access is kept simple. Time is organized into time slots, which are grouped into frames. Each frame has a fixed length of a (integer) number of time slots. Each node takes control of (at least) one time slot and a node is allowed to transmit packets during this time slot. During time slots of other nodes, a node receives packets when it is addressed. Otherwise, the node switches its transceiver to low-power mode in order to conserve energy [15].

Nodes lack sufficient memory to obtain and maintain a global view of the network. Thus, operation is required to be localized. We develop a mechanism that allows nodes to decide which time slots can be used without causing interference to other nodes, based upon local information only. Nodes autonomously select (randomly) a time slot when it is not used in a two hop radius and this allows for medium to be spatially reused, which is beneficial for transport capacity of the network [20].

A secure topology discovery algorithm using the information about the network state in terms of the number of active nodes present and the connectivity (reachability) map of the system is proposed. Its performance is studied for different types of node distributions. The approach divides the network into clusters and decentralization is achieved using threshold cryptography and a network secret that is distributed over a number of nodes. The constructed topology has desirable properties such that the performance of the proposed algorithms is highly efficient and optimized in terms of the resources they consume. The proposed work is tested for its effectiveness by performing sample data transfer under various random deployment of sensors (like Gaussian, Poisson, Rayleigh and exponential), all capable of a transmission range of ‘r’ meters and located in a rectangular area of specified dimensions. The proposed algorithm design is validated by performing different experiments and by varying several system parameters. Comparative studies with conventional schemes are also presented and the improvement achieved due to the use of the present work, is clearly established in the thesis.

V. SECURE TOPOLOGY DISCOVERY ALGORITHM

The secure topology discovery algorithm proposed in this work belongs to the class of prevention type security. The malicious nodes are prevented from joining the graph. This is implemented by providing a secret key to all sensor nodes and all the route information messages are encrypted. Perimeter security is the application chosen to illustrate the proposed security protocol. The following assumptions are made:

A. ASSUMPTIONS

1. The base station is computationally robust, having the requisite processor speed, memory and power to support the cryptographic and routing requirements of the sensor network.
2. The base station is part of a trusted computing environment.
3. The communication paradigm is either base station-sensor or sensor-base station.
4. The radio range of a sensor is 150 meters and sensing range of the sensor is 10m.
5. An address space of 10 bits is used to accommodate the network.

B. SINGLE COLLECTION AND AUTHENTICATION POINT (BASE STATION) MODEL

Each sensor communicates either directly or indirectly with a base station and in turn the base station correlates and aggregates information from each sensor. Accordingly, the base station will need to verify the authenticity of the sensor and the integrity of the communication. This can be achieved by using threshold cryptography. To implement cryptography effectively, the cryptographic keys need to be managed properly. The necessary keys needs to be distributed before predeployment of nodes in such a way that any two or more nodes that need to communicate securely can establish a session key. Then, the session keys need to refreshed from time to time to prevent known attacks. Finally, in case any nodes are found to be compromised, the key ring of the compromised keys might need to be replaced [27].

Effective key management ensures that wireless sensor networks, (1) become tamper proof; (2) can operate unattended; (3) need no fixed infrastructure and preconfigured topology; (4) communicate in an open medium;

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

and (5) can operate even in severe hardware and resource constraints [10,25]. In this security protocol the j^{th} sensor shares a unique 64 bit key with the base station. The 64 bit key is used since there exist a tradeoff between severe hardware constraints, utilized energy and over aggressive prevention. The protocol provides for a multi-hop scenario where the range of a base station is extended by employing nodes that are adjacent to the base station to serve as intermediaries for non-adjacent nodes. Figure 1 depicts an example of such a sensor network topology.

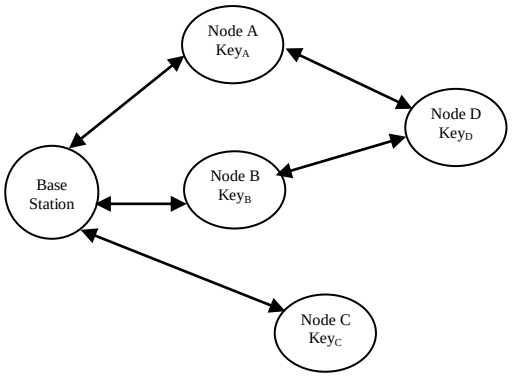


Fig 1: Example Network Topology

The format of all communication (sensor nodes and the base station) consists of a preamble, header and payload. The preamble is empty if the communication originates from the base station and is directed to a sensor; otherwise it contains the address of the sending node. The header contains the recipient's address, nonce and a command and is encrypted under key K_j, which is shared between the base station and node j. The payload contains data exchanged between the node and the base station. The header is tied with the pay load. The payload is encrypted under the shared key of the destination node, which may be different from the key used to encrypt the header. This difference comes into play when the communication needs to be relayed by an intermediate node. This tying of payload in the header make it to robust attacks, such as, an attacker using the header from one message and attaching the payload to another message (Worm hole Attack). This is due to the encryption of the payload being different from that of the header. Table 1 depicts the communication format. To provide a trade of between message latency and network lifetime, the size of the packet is assumed to be 40 bytes.

Table 1: Message Format

Addr_1()	Key$_j${Addr_2(j), DTG, Command, **K$_{yj}$ {data}**}
Preamble	Header tied with payload

In Table 1,

1. Addr_1 is empty if the communication is from the base station to a sensor. Addr_1 contains the address of the sending node if the communication is directed from sensor to the base station. The inclusion of Addr_1 enables the base station to immediately select the correct key; instead of trying keys until it locates the correct one which will be expensive.
2. Addr_2 contains the address of the destination node if the communication is from the base station to a node. If the communication is from a node to the base station Addr_2 will contain the address of the sending node.
3. DTG is the date-time-group and is used to prevent replay attacks.
4. COMMAND is a command to the sensor.

C. DISCOVERY ALGORITHM

The proposed secure topology discovery algorithm is heavily bent on using the neighborhood concept because of the fact that, that node which manages to respond to HELLO message first sent by base station, due to the inherent timeout parameter in the adhoc network, the base station assumes that the node is best reached directly. The base station is deployed with a unique ID and symmetric encryption key of each node in the micro sensor network. Similarly, each node is deployed with the unique key that it shares with the base station and its clock is synchronized with the base station's clock [24,26]. Without precise synchronization, nodes have to use long guard intervals and timeouts to ensure that receivers are ready when transmitters start transmitting, wasting valuable energy. The more accurate the synchronization is, the smaller tolerated timing differences can be and the lesser the energy-wastage and a long lived network. The local clocks of the sensor nodes needs to be synchronized and can achieved by using a good synchronization scheme such as tree clock synchronization.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

D.ADJACENT NODE DISCOVERY

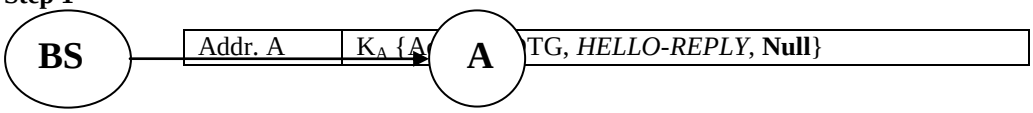
A node is called an adjacent node if it is within the broadcast range of the base station. To discover the node as an adjacent node or not, the following steps are performed.

1. The base station sends a HELLO message to each node.
2. If the node replies with a HELLO REPLY, then the node is adjacent to the base station and base station adds that node to its route table.

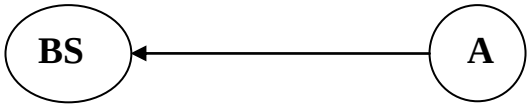
Table 2: Adjacent node discovery algorithm

NULL	K_A {Addr. A, DTG, *HELLO*, **Null**}
Preamble	Header tied with pay load

Step 1



Step 2



If the base station does not know which the adjacent nodes are, the only way is to try all K_j which seems expensive. However, this can be made optimal by using the already available algorithms (Bellman-Ford algorithm) for quickly identifying K_A.

E. NON ADJACENT NODE DISCOVERY

A non adjacent node is the one which is not reachable directly by the base station. To discover the non adjacent node, the base station uses the adjacent node. The adjacent nodes which are used to reach the non adjacent node are noted as the route to reach the non adjacent node.

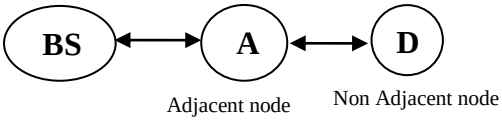
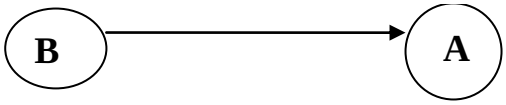


Fig 2: Network model

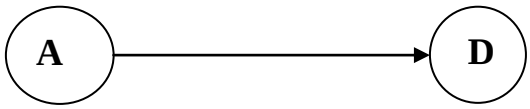
Table 3: Non-adjacent node Discovery Algorithm

Step 1 $\Psi = K_A$ {Addr. A, DTG, RELAY}



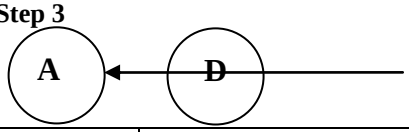
NULL	K_A {Addr. A, DTG, *RELAY*, **K_D {Addr. D, DTG, HELLO}**}
Preamble	Header tied with pay load

Step 2



Addr.A	K_D {Addr. D, DTG, *HELLO*, **K_A {Addr. A, DTG, *RELAY* }**}
Preamble	Header tied with pay load

Step 3

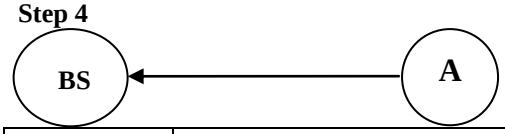


Addr. D	K_A {Addr. A, DTG, *RELAY*, **K_D {Addr.D, DTG, *HELLO-REPLY*}**}

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Preamble	Header tied with pay load

Step 4



Addr, A	K_D {Addr. D, DTG, *HELLO-REPLY*, ***Null***}

Preamble	Header tied with pay load

The implementation procedure is given below.

1. The base station sends a message containing the RELAY command and a payload, to be forwarded to the non-adjacent node, to each of the adjacent nodes (Table 3. Step 1).
2. The relaying (adjacent) node adds the original header to the payload and transmits the new message to the non-adjacent node which contains the HELLO command (Table 3. Step 2).
3. To respond to the HELLO message, the non-adjacent node constructs a HELLO-REPLY message encrypting it under the key it shares with the base station and places it in the payload. The message is transmitted adding the base station's address to the preamble and the? to the payload (Table 3. Step 3).
4. In turn, the adjacent node receives the transmission, decrypts the header and upon seeing the RELAY command, adds the preamble to the payload and transmits it to the base station. The cost for each node to decrypt the header is independent (Table 3. Step 4).
5. The base station after receiving the HELLO-REPLY adds the adjacent node as one of the route to reach the non-adjacent node.

F.CIPHER UPDATING

Cipher updating is the process by which the non-adjacent nodes are given a payload to enable communication with the base station. The primary route is the cipher given to the non-adjacent nodes. The Cipher contains the address of the primary route node, a nonce and COMMAND encrypted by the key of the primary route node.

G. OPTIMIZATION ALGORITHM ROUTE TABLE

After performing the secure topology discovery, the base station contains a route table. A route table is a constituent of nodes and their route to reach these nodes. If the node is an adjacent node then the route to the node is mentioned as direct else the different adjacent route nodes are mentioned. This route table is called as raw route table since there are many redundant routes to reach a non adjacent node. The purpose of route table optimization is to assign impartial load to all adjacent nodes.

H. ROUTE TABLE OPTIMIZATION ALGORITHM

The optimization algorithm for non adjacent nodes involves the following steps:

1. Calculate the load for each adjacent node.
2. Chose minimum load adjacent node as the route.
3. Steps 1 and 2 are repeated till all the non-adjacent nodes are assigned routes.

I. LOAD CALCULATION

Load is calculated based on the number of past assigned confirmed nodes (they are given higher weightage since confirmed) and the number of future possible assignment of nodes. For an adjacent node the load calculation is done using the formula

Load = mP + nQ

Where 'P' is the number of past assigned non-adjacent nodes to the adjacent node and 'Q' is the number of future possible assignment of non-adjacent nodes to the adjacent node and 'm' and 'n' are the weight for P and Q respectively.

J. OPTIMAL WEIGHTS

Optimal weight should be chosen to obtain an optimized route table. In this algorithm, the optimal weight is chosen by trail and error method. The optimized route table is compared for different weights and the weights which results in best route table are chosen as the optimal weights.

VI. RESULTS AND DISCUSSION

The results obtained by applying the proposed algorithms are presented for an example scenario shown in Figure 3. The raw route table obtained after secure topology discovery is given in Table 4. The raw route table is a constituent of nodes and their route to reach nodes. The connection table shown in table 5 gives information about the non adjacent nodes alone along with their connection with the adjacent nodes. The load calculation is shown in Table 6. After applying the route table optimization algorithm, the optimized route table with primary

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

route is shown in Table 7. The primary route is use to reconstruct a unique topology with one to one napping and secondary route is used to know about the adjacency nodes that are uniquely attached to source nodes

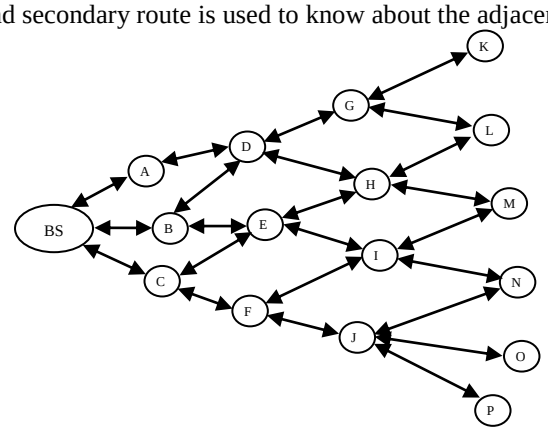


Fig 3: An Example Scenario

TABLE 4: Raw Route Table for the sample scenario

Node	Route 1	Route 2	Route 3
A	Direct		
B	Direct		
C	Direct		
D	A	B	
E	B	C	
F	C		
G	D		
H	D	E	
I	E	F	
J	F		
K	G		
L	G	H	
M	H	I	
N	I	J	
O	J		
P	J		

TABLE 5: Examples of connection table

	A	B	C	G	H	I	J
D	1	1	0	1	1	0	0
E	0	1	1	0	1	1	0
F	0	0	1	0	0	1	1
K	0	0	0	1	0	0	0
L	0	0	0	1	1	0	0
M	0	0	0	0	1	1	0
N	0	0	0	0	0	1	1
O	0	0	0	0	0	0	1
P	0	0	0	0	0	0	1

TABLE 6: Load Calculation

Node	Route 1	Route 2
A	Direct	
B	Direct	
C	Direct	
D	A	B
E	B	C
F	C	
G	D	
H	D	E
I	E	F

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

J	F	
K	G	
L	G	H
M	H	I
N	I	J
O	J	
P	J	

TABLE 7: Optimized Route Table

Node	Primary route
A	Direct
B	Direct
C	Direct
D	A
E	B
F	C
G	D
H	D
I	E
J	F
K	G
L	G
M	H
N	I
O	J
P	J

A.DISCUSSION

To check the validity of the algorithms proposed in this work, different test inputs were given and the results were analyzed. Different test inputs are used to know the best distribution for a particular application. Typically the sensor node positions are determined by the field conditions of what is being observed such as health/status monitoring of bridges which can be decided offline i.e. apriori. It is assumed that 12 mA of current was drawn to transmit a message and 10 mA to receive the message [20]. The secure topology discovery algorithm was validated with known placement of nodes and also random distributions like Poisson, Rayleigh and Exponential. The base station was located at the centre and 24 sensor nodes are randomly distributed (following distributions like Poisson, Rayleigh and Exponential) around the base station. A known placement of nodes (uniform distribution of nodes) considered for study is shown in Figure 4. Similarly, Figures 5, 6 and 7 shows the Exponential, Poisson and Rayleigh distribution respectively of sensor nodes. The actual field is depicted in terms of the X and Y coordinates of the nodes.

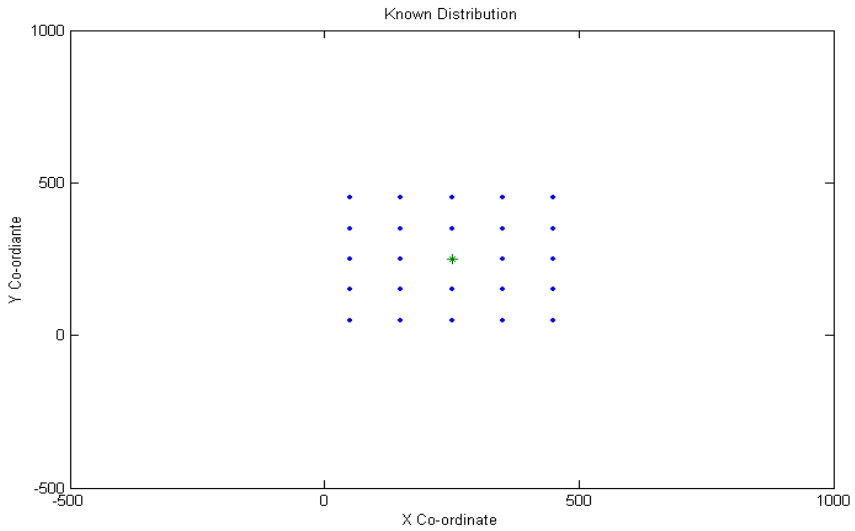


Fig 4: Known Placement of nodes

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

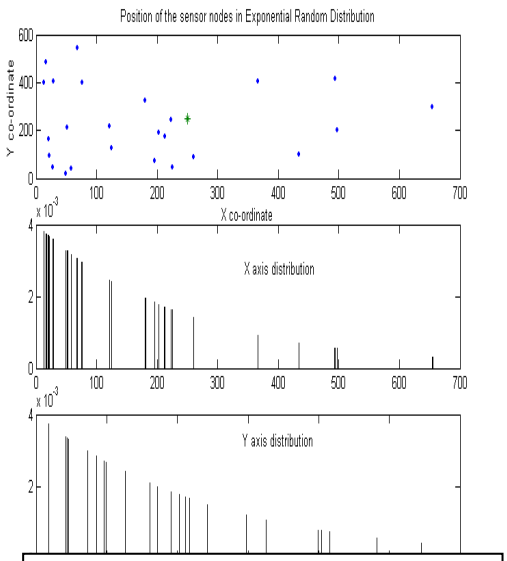


Fig 5. Exponential Distribution of Sensor Node

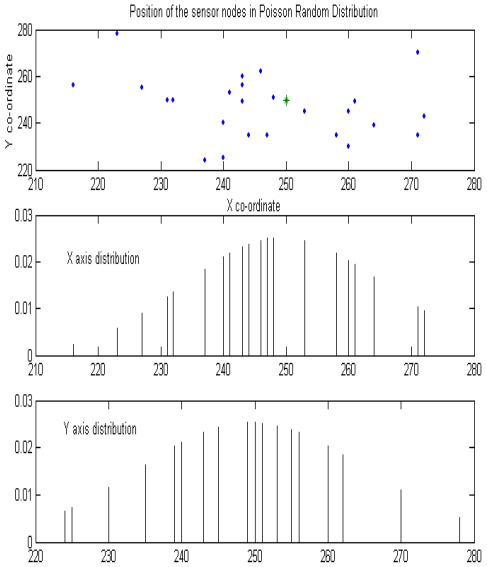


Fig 6. Poison Distribution of Sensor Node

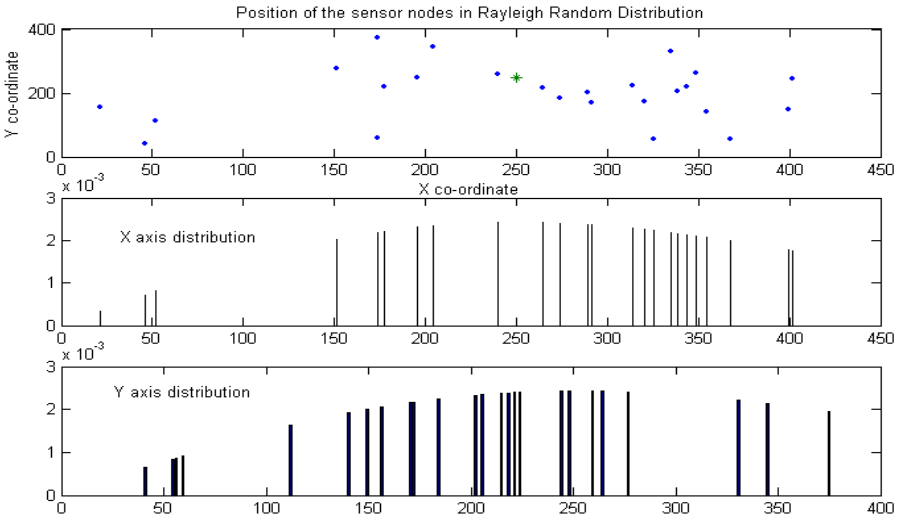


Fig 7: Rayleigh Distribution of Sensor Nodes

Figure 8 gives the energy spent in transmission and reception to discover the given topology using the proposed secure topology discovery algorithm. The energy spent for reception is lesser than the energy spent for transmission. This is intuitive as the number of messages received greatly overweighs those transmitted.

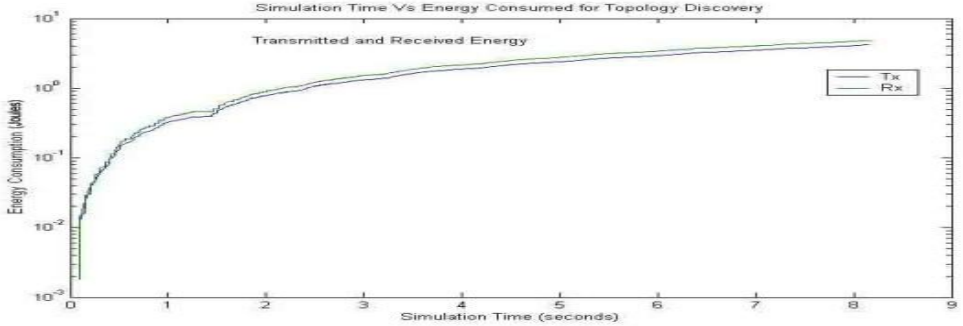


Fig 8: Energy Consumption for Topology Discovery

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Figure 9a and 9b shows the energy spent in transmission and reception respectively for different types of node distributions and we see the Poisson's distribution consumes extremely low energy for transmission and reception.

9a. Energy spent in transmission **9 b. Energy spent in reception**

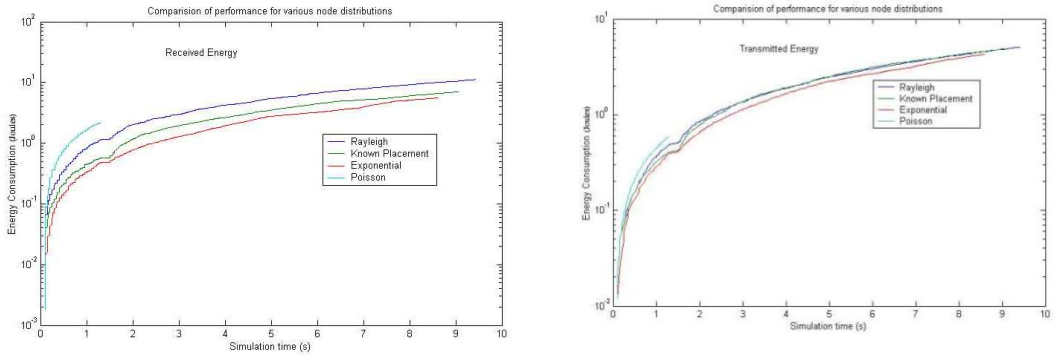


Fig 9: Energy Spent For Different Nodes Placement

The implementation results for route table optimization algorithm for a sample node distribution is presented.

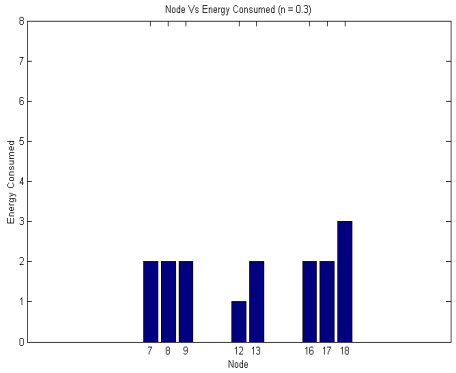


Fig 10: Load on nodes for n = 0.3

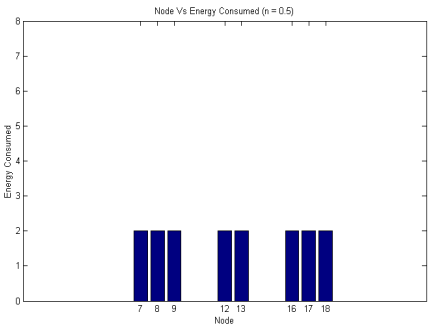


Fig 11: Load on nodes for n = 0.5

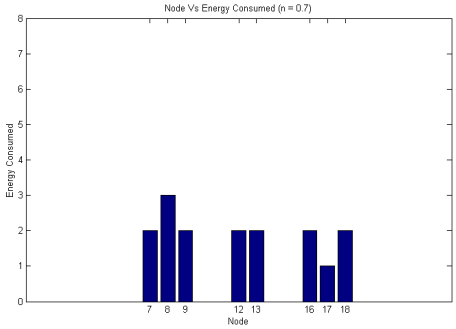


Fig 12: Load On Nodes for N = 0.7

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Figures 10, 11 and 12 shows the load distribution for Poisson's distribution of nodes. By simulation the optimal weights for Poisson's distribution of nodes are found to be m=1 and n=0.5. Even though the optimality of weights is shown for Poisson's distribution of network, the proposed algorithm is generic and can be applicable for any network configuration. A comparison of these plots proves that the value of weight n = 0.5 results in equal share of load to the nodes. The comparison plots for throughput fluctuation are plotted in Figure 13 and we see that the throughput is more for even distribution of nodes.

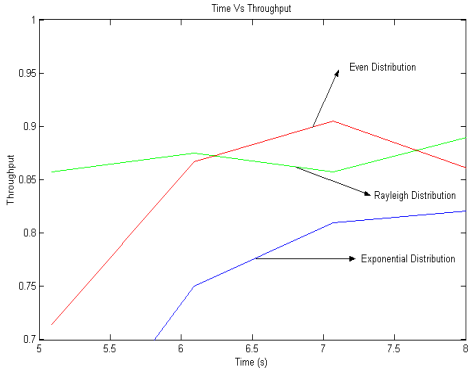


Fig 13: Comparison of Throughput Fluctuation for Different Node Placement

Table 8 shows the connection table. After applying the optimization algorithm, primary route table of Table 9 and secondary route table of Table 10 are obtained. Table 8, 9, 10 should have been 24x24, but coloums and rows are skipped just to indicate that sparse (unused) elements are not reflected for brevity.

Table 8: Connection table

	1	**2**	**5**	**7**	**10**	**11**	**13**	**14**	**15**	**16**	**17**	**19**	**20**	**21**	**24**
3	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*1*	*1*	*0*	*1*	*0*	*1*
4	*1*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*1*	*0*	*0*	*0*	*0*	*1*	*0*
6	*1*	*0*	*0*	*1*	*0*	*0*	*1*	*0*	*1*	*0*	*0*	*1*	*0*	*1*	*0*
8	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*1*	*0*
9	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*1*	*0*	*0*	*0*	*1*
12	*1*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*0*
18	*1*	*1*	*0*	*1*	*0*	*0*	*1*	*0*	*1*	*0*	*0*	*1*	*0*	*1*	*0*
22	*0*	*0*	*1*	*0*	*0*	*1*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*1*
23	*1*	*1*	*0*	*1*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*1*	*0*

Table 9: Primary route Table

	1	**2**	**5**	**7**	**10**	**11**	**13**	**14**	**15**	**16**	**17**	**19**	**20**	**21**	**24**
3	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*
4	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
6	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*
8	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
9	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*
12	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*
18	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
22	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
23	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*

Table 10: Secondary route Table

	1	**2**	**5**	**7**	**10**	**11**	**13**	**14**	**15**	**16**	**17**	**19**	**20**	**21**	**24**
3	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*
4	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*
6	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
8	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*
9	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*
12	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*
18	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
22	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
23	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Table 11: Optimized route Table

Node	Primary Route	Secondary Route
1	*D*	
2	*D*	
3	*20*	*16*
4	*13*	*15*
5	*D*	
6	*15*	*1*
7	*D*	
8	*7*	*19*
9	*16*	*17*
10	*D*	
11	*D*	
12	*17*	*20*
13	*D*	
14	*D*	
15	*D*	
16	*D*	
17	*D*	
18	*1*	*2*
19	*D*	
20	*D*	
21	*D*	
22	*5*	*11*
23	*2*	*7*
24	*D*	

VII. CONCLUSION

The proposed work is the development of architecture for secure communication in mobile wireless networks. The approach divides the network into clusters and implements a decentralized certification authority. Decentralization is achieved using threshold cryptography and a network secret that is distributed over a number of nodes. While this basic idea has been proposed earlier partially, its application on clustered network is a novelty of the work. The work address issues of authorization, access control and a multilevel security model and helps to adapt to the complexity of mobile end systems. It also effectively counteract the denial of service (DoS) threats and hence, can prolong the life time and improve robustness of wireless sensor network. To check the validity of algorithms proposed in this thesis, different test inputs are given and the results are analyzed. The algorithm was validated with uniform distribution of nodes and also random distributions like Gaussian, Poisson, Rayleigh and Exponential. Studies related to energy spent in transmission and reception to discover the given topology using the proposed algorithm is done along with throughput fluctuations. Results obtained show that the schemes proposed in this work, result in significant dependability improvement for a wireless sensor network. The proposed work shall enable a wireless sensor network to consume extremely low power, operate in high volumetric densities and be dispensable. It is ideally suited to most of the applications that share similar features such as difficult to access because of geographical location where the network has been deployed, the large scale of deployment, high mobility and prone to failure. It also ensures that the wireless sensor network be autonomous and operate unattended, be adaptive to the environment and choose an optimal number of communicating sensing nodes since too many sensors can generate bottlenecks in the communication infrastructure when they all compete for bandwidth.

REFERENCES

[1] Akyildiz. I.F, Su W, Sankarasubramaniyam Y, Cairci E, “Wireless sensor networks: A survey,” computer networks 38, pp 393-422, 2002.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

[2] Akyildiz I.F, Su. W, Sankarasubramaniam Y, and Cayirci E, "A survey on sensor networks", IEEE Communication magazine, vol. 40 Issue: 8, pp. 102-114, August 2002.

[3] Akyildiz. I.F, Varun. M.C, Akan. O.B and Su. W, "Wireless sensor networks: A survey REVISITED," computer networks Journal Elsevier, 2006.

[4] Amis. A.D, Prakash. R, Huyuh. D, and Vuong. T, "Max-Min D-Cluster formation in wireless Ad-hoc network," Proceeding of IEEE INFOCOM, pp 32-41, 2000.

[5] Basagni. S, "Finding a maximal weighted independent in wireless networks," Telecommunication systems, special issue on mobile computing and wireless networks, 18 (1/3): 155-168, 2001.

[6] Budhaditya Deb, Sudeept Bhatnagar and Badri Nath, STREAM "sensor topology retrieval at multiple resolution," Computer Science Department, Rutgers University.

[7] Chatterjea. S, Havinga. P.J.M, and Lodewijk F.W. Van Hoesel, "A low latency, Information – centric Medium Access Protocol for wireless sensor networks," in proceedings of PRORISC, the Netherlands, November 2004.

[8] Daqiang Zhang, Hu Guan, Jingyu Zhou, Feilong Tang, Minyi Guo, "iShadow: Yet another Pervasive Computing Environment," IEEE International Symposium on Parallel and Distributed Processing with Applications, pp.261-268, 2008.

[9] Deb. B, Bhatnagar. S and Nath. B, "A Topology discovery algorithm for sensor networks with application to network management," in: Proc. Of the IEEE CAS Workshop on wireless communication and networking, Pasadena, USA, September 2002.

[10] Du. W and Deng. J and Y.S. Han, P.K. Varshney, J. Katz and A. Khalili. "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Secur., 8(2): 228-256., 2005.

[11] Feilong Tang, Minyi Guo, Minglu Li, Zhijun Wang, Zixue Cheng, "Scalable and Secure Routing for Large-Scale Sensor Networks," IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 300-305, 2008.

[12] Feilong Tang, Minyi Guo, Minglu Li, Yanqin Yang, Daqiang Zhang, Yi Wang, "Wireless Mesh Sensor Networks in Pervasive Environment: a Reliable Architecture and Routing Protocol," International Conference on Parallel Processing Workshops (ICPPW 2007), pp. 72, 2007.

[13] Gang Xiong and Shalinee Kishore "Second order distributed consensus time synchronization algorithm for wireless sensor networks," GLOBECOM, pp 292-296, December 2008.

[14] Geerlings. J, Hoeksema F.W, Havinga. P.J.M, Slump. C.H and Lade Wijk F.W. Van Hoesel, "Spatial medium reuse in wireless sensor networks," proceedings of SPSDARTS'07, March 2007.

[15] Havinga. P.J.M, Lodewijk F.W, Van Hoesel, "Collision – free time slot reuse in multi-hop wireless sensor networks," in intelligent sensors, sensor networks and information processing (ISSNIP'05) conference, Australia, 2005.

[16] Hermann. C, Dargie. W, Senceive: "A middleware for a wireless sensor network," 22nd International Conference on advanced information networking and applications, pp. 612-619, March 2008.

[17] Huang. Polly, "Sensor network, Where is it going to be?," IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy computing, pp. 271-271, June 2008.

[18] Imrich chalamtac, Mario Confi, Jennifer. J, Liu. N, "Mobile ad hoc networking: Imperatives and challenges," Ad-hoc Networks Journal, vol. 1, issue 1, pp 13-64, July 2003.

[19] Jian Yin, Madria, Sanjay Kumar, "Sybil attack detection in a hierarchical sensor network," Third International Conference on Security and privacy in communication networks, pp. 494-503, Sept. 2007.

[20] Lodewijk F.W. Van Hoesel, "Schedule based medium access control protocol for wireless sensor networks," Ph.D. thesis, University of Twente, Netherlands, ISBN 978-90-365-2497-1, June 2007.

[21] Nieberg. T, Kip. H.J, Havinga. P.J.M, "Advantages of a TDMA based, energy efficient, self organizing MAC protocol for wireless sensor networks," in IEEE VTC spring, Italy, May 2004.

[22] Ringwald. M, Romar. K, "Deployment of sensor networks: Problems and passive inspections," IEEE WISES, Madrid, Spain, June 2007.

[23] Shi. E and Perrig. A, "Designing secure sensor networks," IEEE wireless communication magazine, 11 (6) 38-43, December 2004.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

[24] Sivrikaya, Yenes. B, "Time synchronization in sensor networks: A survey," IEEE International Conference on Networks, vol. 18, issue 4, pp 45-50, July – August 2004.

[25] Xiao Chen, Drisgi. J, "An efficient key management scheme in hierarchical sensor networks," IEEE information conference on mobile Ad-hoc and sensor networks, pp 840-846, November 2005.

[26] Xiaojiang Du, Guizani, Yang Xiao, Hsiao-Hwa Chen, "Secure and efficient time synchronization in Heterogeneous sensor networks," IEEE transactions on vehicular technology, vol. 57, issue 4, pp 2387-2394, July 2008.

[27] Yi Qian, Kejie Ln, Bo Rong, Hua Zhu., "Optimal key management for secure and survival heterogeneous wireless sensor networks," IEEE Global Telecommunication conference, GLOBECOM'07, pp. 996-1000, Nov. 2007.

[28] Ye. W, Heidemann. J, and Estrin. D. "An energy efficient MAC protocol in wireless sensor networks," proceedings of IEEE INFORCOM conference, June 2000.

[29] Zhu. S, Setia. S, and Jagodia. S. LEAP+: "Efficient Security Mechanisms for large scale distributed sensor networks," ACM Trans. Sen. Netw., 2(4): 500-528, 2006.