Establishing an Integrated Secure Wireless Sensor Network System: A New Approach

Kalpana Sharma[1], S.K. Ghosh[2] and M.K. Ghose[3]
[1]Department of CSE, SMIT, Sikkim
kalpanaiitkgp@yahoo.com
[2] SIT, IIT Kharagpur,
skg@iitkgp.ac.in
[3] Department of CSE,SMIT, Sikkim
mkghose@smu.edu.in

ABSTRACT
Wireless sensor networks (WSNs) are gaining a lot of popularity these days due to their application in a number of areas. WSN's provide an easily implementable and cheaper solution for many real world problems like data gathering, surveillance, monitoring and control etc. However they are also used in a number of applications where security is a prime concern like military operations or other sensitive projects, whereby if the network is compromised then the outcomes can be disastrous. A lot of security schemes have been proposed which address different layers of protocol stack but none of them are fully integrated. In this paper a new approach is presented to establish a secure wireless sensor network. The proposed integrated approach addresses concerns like energy, and various security parameters like authenticity, confidentiality, integrity and requires lesser processing power.

KEYWORDS
Wireless sensor Network, Security, Clustering, localization, Hierarchical Clustering

1. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration pressure, motion etc [1]. Unfortunately Wireless sensor networks are more susceptible to attacks than wired networks [2]. A lot of security techniques have been proposed to ensure the security parameters in WSN. These techniques are somewhat disjoint and do not address the security of WSN as a whole. These techniques address individual layers and are targeted to tackle general security threats. However these techniques lack a common integrated framework that addresses the security concern of the whole WSN right from the time of deployment of nodes till data transmission.

In this paper an attempt has been made to develop mechanisms for secure WSN.Three different units have been focussed. First of all the problem of localization of sensor nodes is considered in unit I. This unit focuses on localization of sensor nodes. Unit II deals with clustering and finally the unit III describes the encryption techniques used. All these units together form the integrated framework for WSN security.

The rest of this paper is organized as follows. In section 2 background pertaining to the proposed work is highlighted. Section 3 gives an overview of the whole approach. In section 4 localization algorithms have been proposed. Section 5 describes the techniques for assigning cluster heads. Section 6 gives a detailed description of the encryption algorithm that has been proposed and devised for encrypting data in link-layer. Finally section 7 shows the results.

2 BACKGROUNDS

Wireless sensor networks (WSN's) are quite useful in many applications since they provide a cost effective solution to many real life problems. They are susceptible to a variety of attacks, including node capture, physical tampering, and denial of service, prompting a range of fundamental research challenges [2]. Security allows WSNs to be used with confidence and maintains integrity of data. Without security, the use of WSN is any application domain would result in undesirable consequences. Thus security must be addressed in such critical sensor applications. It turns out that providing security in wireless sensor networks is pivotal due to the

fact that sensor nodes are inherently limited by resources such as power, bandwidth, computation, and storage [9]. Although a lot of progress has been made for the past few years, but most of these security solutions only assures a sense of security in one layer whereas the security of the network can be ruptured any of the layers as well like network layer, physical layer etc.Thus to secure a wireless sensor it is essential to address various security concerns such as confidentially, integrity, authentication etc. A lot of work has already been carried in the field of localization, clustering and encryption separately [1]. This section will give an overview of some of these contributions, though it may be noted that that none of these contributions attempt to integrate these modules to achieve a complete integrated security framework. This paper attempts to go a step further by integrating these disjoint yet related modules to achieve the target of securing WSN in a different way.

2.1 A large number of localization algorithms have proposed by many researchers, some of them are for static networks [5] and some of them are for dynamic. But there are few algorithms which work for both static as well dynamic networks [16].One of the localization algorithms that use Virtual Coordinate assignment protocol (VCap) which works according as virtual coordinate system based on hop distances [4]. Other localization algorithm is based on the directional antenna in which every node in sensor network is configured with directional antenna and few sensor nodes have GPS receiver [17].

2.2 As far as algorithms for clustering techniques [18] are concerned, most of these clustering algorithms consider one or more properties of their neighbouring nodes like energy consumption as in HEED [15] or remaining battery power as in [18]. In [21] an equation is formed taking into consideration the four factors viz. the node degree, distance summation to all its neighbouring nodes, mobility and remaining battery power respectively. In [7] a two level clustering model for sensor networks is proposed. In this model sensor clusters around strategic locations and header nodes are distributed so that their location has flexibility. In [10] clusters are formed based on the received signal strength and the Cluster Heads (CH) are used as routers to the base-station (BS). All the data processing such as data fusion and aggregation are local to the cluster. LEACH [14] forms clusters by using a distributed algorithm, where nodes make autonomous decisions without any centralized control. In [12], the authors have proposed a clustering algorithm that aims at maximizing the lifetime of the network by determining optimal cluster size and optimal assignment of nodes to cluster heads. The main aim of hierarchical routing is to efficiently maintain the energy consumption [11] of sensor nodes by involving them in multi-hop communication within a particular cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink. Cluster formation is typically based on the energy reserve of sensors and sensor's proximity to the cluster head [13, 6].

2.3 Till date a lot of research has been carried out on WSN security issues. Security issues, a lot of research going on in this particular area. Security mechanisms in WSN are developed in view of certain constraints [8]. Among these, some are pre-defined security strategies; whereas some are direct consequences of the hardware limitations of sensor nodes. Some of the security issues for WSN are as follows

2.3.1. Energy efficiency: The requirement for energy efficiency suggests that in most cases computation is favoured over communication, as communication is three orders of magnitude more expensive than computation [9]. The requirement also suggests that security should never be overdone - on the contrary, tolerance is generally preferred to overaggressive prevention [15]. More computationally intensive algorithms can not be used to incorporate security due to energy considerations [18].

2.3.2. No public-key cryptography: Public-key algorithms remain prohibitively expensive on sensor nodes both in terms of storage and energy [19]. No security schemes should rely on public-key cryptography. However it has been shown that authentication and key exchange protocols using optimized software implementations of public-key-cryptography is very much viable for smaller networks.

2.3.3. Physically tamperable: Even if a few of the nodes go down, the network survives. The concept of resilience, or equivalently, redundancy-based defence is widely demonstrated [22].

2.3.4. Multiple layers of defence: Security becomes an important concern because attacks can occur on different layers of a networking stack. So it is evident that a multiple layer of defence is required, i.e. a separate defence for each layer [23].

3. OVERVIEW OF THE APPROACH

In this work an integrated security system is proposed. It is well known that it is not possible to have any cost effective solution to address all the security issues of all the layers of the protocol stack. Researchers have always attempted to implement security of individual layers to prove overall system security. Here for the ease of implementation of security issues like integrity, Data Link Layer (DLL) is considered. . To start with the real-time data capturing (of the location of each node) was done using GPS (Global Positioning System) and then a sensor network is established using those GPS driven coordinates. This is followed by neighbour discovery of each node and thus establishing the authentic coordinates of each node. For neighbour discovery hierarchical clustering is performed. Once the communication platform was established as 'hierarchical clusters', the proposed algorithm for Data encryption is used to achieve security requirements like confidentiality and integrity in DLL. The proposed encryption algorithm requires lesser memory and has lesser complexity than contemporary schemes.

As stated earlier in order to achieve the proposed integrated security framework (ISF), three major modules have been proposed as shown in figure 1.

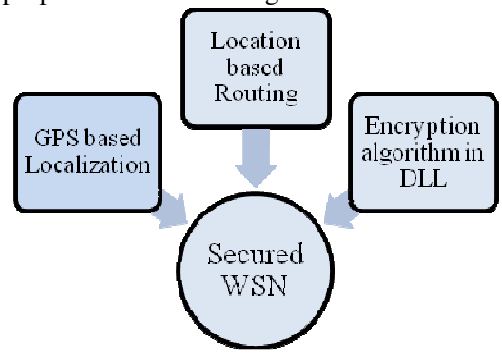

Fig. 1: Schema of Integrated Security Framework

The three modules comprises of localization module, a secure routing module, and finally a new encryption technique.

3.1 Localization algorithm: After deployment of the node the localization of the nodes are done. Here localization is the process of detection of the location of nodes and for finding optimal routes in geographic routing. In this paper 'Bi-beacon localization' is proposed which is implemented using C-language. A detail pertaining to the localization scheme used in this work is described in section 4.

3.2 Clustering algorithm: Sensor has a shorter range of communication, and hence they need to communicate with some intermediate nodes to make the data available at the base station. The hierarchical organization of the nodes in the sensor network gives an inherent scalability to the proposed scheme and keeps the energy under control because of its hierarchical nature. The nodes also need to know that to which node they have to communicate. So there must be an encryption and authentication process for the communication to take place between the nodes and the base station. Details are discussed in section 5.

3.3 Security algorithm in Data Link Layer (DLL): The proposed encryption algorithm for DLL ensures data confidentiality and integrity as this algorithm doesn't require key maintenance and key refreshment. Section 6 describes the proposed algorithm in detail.

Each module mentioned through subsections 3.1 to 3.3 contributes towards achieving one or the other security goals of this security framework.The localization scheme uses two GPS receivers. It ensures the authenticity of the nodes in the network and thus leads to authenticated broadcasts. Based upon this localization the coordinates of all the sensor nodes are established and this data is used for hierarchical based clustering and routing scheme. This technique ensures secure transmission of data to most suitable and secure node. Finally to achieve integrity, confidentiality and freshness, an energy efficient new encryption algorithm is used which has lesser complexity.

4. GPS BASED LOCALIZATION SCHEME

Localization can be defined as the process of finding location of the nodes [3] or it can also be stated as the problem of individual sensor's awareness of their position relative to a coordinate system common to the entire sensor network [4]. Localization can be of various types global, absolute, relative or directional.

For ISF absolute positioning is used and certain assumptions are made for simplicity. GARMIN eTrex vista HCx GPS receiver is used for data capturing. The following assumptions are made for simplicity. It is to be noted that this algorithm can be generalised to support more number of nodes.

- There are two nodes in which GPS receiver is embedded.
- The two special nodes are (i) Base station and (ii) Any movable sensor node called Beacon node.
- Each node is under the range (receiving and sending) of Base station.
- Only one Beacon node is mobile else other nodes are stationary i.e. Network is static.
- X and Y co-ordinates are the latitude and longitude of the specific sensor node.
- The approximate boundary of the surveillance field is known. Further it is assumed that the deployment area is flat with no irregularities elevated positions of sensor nodes are not considered.

The algorithm for 'localization unit' is described below.

Algorithm: Find_location

Step0. Begin.

Step1. All nodes are randomly deployed in the surveillance field.

Step2. Beacon node is traversed in the surveillance field.

2.1. Beacons sends message packet to all its neighbouring nodes and receives acknowledgement packet.

Step3. Beacons calculate the time duration of the communication and then using the well known mathematical formula of Distance = speed *Time, distance between node and Beacon is calculated.

Step4. Step 3 is repeated till all the nodes are traversed.

Step5. Since it is assumed that each node is under the range of the base station, the base station also knows the distance of each and every node from itself.

Step6. Using the Euclidian distance calculating formula $(X1-X2)^2+ (Y1-Y2)^2=D^2$ the exact position of the nodes can be found out (Mathematical proof is provided in section 3.1).

Step7. End.

Note: It is to be noted that the distance calculated may not be the shortest distance. To find the shortest distance the algorithm has to be augmented with any of the 'shortest distance' algorithms which are out of the scope of this work at this point.

4.1 MATHEMATICAL PROOF

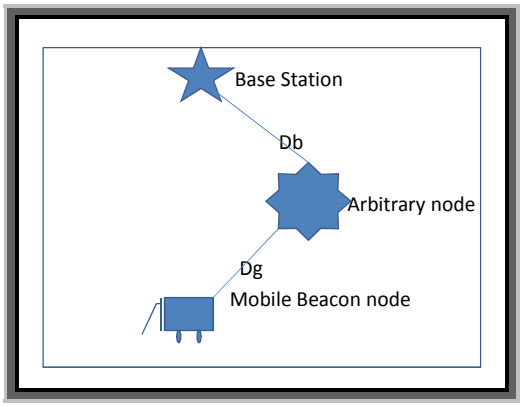

Fig 2: Arrangement of Nodes for calculation of the coordinates

Let us consider the Coordinates of Base Station to be (Xb, Yb) as shown in figure 2 and it has a GPS so its latitude and longitude is known. Similarly the Coordinates of Beacon node is (Xg, Yg) and it also has GPS, so its latitude and longitude is known. Considering the coordinates of any arbitrary node as (X, Y) their values now can be calculated easily.
Now the time difference between base station and node say Tb is known, so using Distance =Speed * Time
=>Distance = Speed of light * Tb = Db [Speed of light is known and is 3.0*108 m/sec] -- (1)
Let the time difference between beacon and Node be Tg
So using Distance =Speed * Time
=>Distance = Speed of light * Tg = Dg [Speed of light is known and is 3.0*108 m/sec] -- (2)
Now using the Euclidian distance formula i.e (X1-X2)2+(Y1-Y2)2=D2 and putting the value of distance from equation (1) in above equation distance formula deduces to
(Xb-X)2+(Yb-Y)2 = Db2
=> Xb2+X2-2*X*Xb +Yb2+Y-2*Yb*Y=Db2
=>(Xb2+Yb2) + (X2+Y2) – 2*Xb*X -2*Yb*Y = Db2
=>(X2+Y2) – 2*Xb*X -2*Yb*Y = Db2 - (Xb2+Yb2)
Now the values of Db2, Xb2, Yb2 are known thus [Db2 - (Xb2+Yb2)] = K (say)
So the above equation reduces to (X2+Y2) – 2*Xb*X -2*Yb*Y = K ---------- (3)

Again putting the value of distance from equation (2) in above equation (Xg-X)2+(Yg-Y)2 = Dg2
Similarly solving the equation as like above equation, (X2+Y2) – 2*Xg*X -2*Yg*Y = C (say) ---------- (4)
Where C = [Dg2 - (Xg2+Yb2)]
Adding Equation 3 and 4 we get
2*(X2+Y2) -2*X(Xg +Xb) -2*Y(Yg + Yb) = K+C .....(5)
The values of Xg, Xb, Yg, Yb are known so 2*(Xg +Xb) =A (say) and 2*(Yg + Yb) = B(say) and K+ C = N
Now the above equation reduces to
=> 2*(X2+Y2) –A*X –B*Y = N..... (6)

Subtracting Equation 3 and 4 we get
D*X + E*Y = M Where D,E and M are known constants
=>X=(M-E*Y)/D..... (7)
Putting the value of (7) in (6) an equation with only one variable is formed that can be solved easily. The equation is
2*[{(M – E*Y)/D}2 + Y2] –A*{(M – E*Y)/D} – B*Y = N
Where M, E, D, B, A and N are known constants.
Thus the value of Y can be found and hence value of X also.
The following figure 3 shows that each node is under the coverage area of Beacon node and the base station.

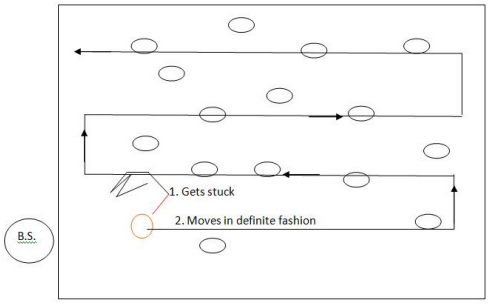

Fig 3: The ways of Beacon-traversal

It is shown in figure 3 that there are two ways of beacon-traversal viz. the mobile node gets stuck in a loop and it moves horizontally till it reaches deployment boundary then vertically and again horizontally. Unit of traversal is equal to the range of the node.
The trajectory of the Beacon is also shown and it completely covers the whole deployment area. Now each time the beacon moves in the deployment area it sends the hello message packet to all its neighbours and then after some response time it receives the acknowledgement message. Thus the time of communication is calculated as described in the above mathematical explanation and thus this step is repeated till all the nodes are traversed and its distance from the base station and the beacon node is calculated. Now with the help of the calculated distances and the known coordinates of beacon and the base station the coordinate of the nodes are calculated.
Once the localization is done, the coordinates of all the sensor nodes are found out. This ensures that all the nodes in the network are authentic thus protecting the WSN from the adversary.

5. HIERARCHICAL BASED CLUTERING & ROUTING ALGORITHM

When the sensors are deployed in an area, the nodes start forming a network for fulfilling their purpose of their deployment. They start forming a sub network in the networks. In order to implement this module well known TinyOS platform having Avrora simulator [19, 20] is used.
Since implementation of clustering algorithm is done for the minimization of communication so as to minimize energy loss in the communication. It is obvious that the number of cluster is directly related with the energy utilization in the network. So, one way to minimize the energy utilization is to minimize the cluster head. The formation of the clusters has been divided into two phases, Group Selection Phase (GSP) and Cluster Head Selection Phase (CHPS).

5.1 Categorization of nodes viz. GPS

The algorithm which is used for categorization of the node is described in this section.

Data Structures:

//b_level_id is a variable holding value 0 and is broadcasted in the packet by base station.
//n_level_id is a variable of every node which is initially initialized with -1 and later holds the level id of the node

Begin:

Base Station broadcasts a message containing b_level_id

```
If(n_level_id==-1)
{
        n_level_id=b_level_id
}
Else
{
        b_level_id++;
        broadcast the packet again
}
```

According to this proposed algorithm there is level-id which acts as a variable holding value 0 and is broadcasted to all the nodes in the packet by base station. Also there is another variable level-id of every node which is initially initialized with -1 and later holds the level id of the node. The base stations broadcasts node id as the messages to all the nodes and thus receives acknowledgement and communication begins.
Once the categorisation of nodes is completed, the task of routing is carried on separately by the Data-Cluster –Head (DCH) and Routing-Cluster-Head (RCH) as shown in figure 4. The DCH is responsible for processing data related tasks like aggregation, calculating median etc, whereas the RCH takes care of communication part i.e. sending the data to base station.

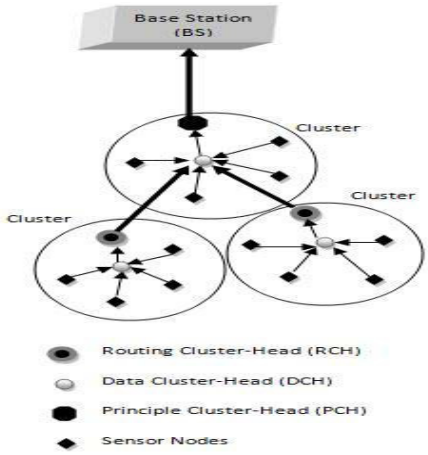

Fig 4: Clustering for RCH & DCH selection

In this algorithm the assignment of DCH is based on the median of distance. This helps to locate a node which is optimally close to all the nodes in a given cluster. The RCH is then determined based on the basis of remaining battery-life of all nodes (this information is communicated by all the nodes to DCH).

The algorithm for DCH & RCH selection is stated in subsection 5.2 below.

5.2 Assigning cluster heads viz.CHSP

Algorithm: Form_ cluster_heads

Data Structures:

//energy[i] holds the energy of the ^{i}th node

//distance[i] holds the distance of ^{i}th node from the BS.

Begin:

Step 1: Every node sends its level id and sector id to the base station through continuous broadcasting done by every node the message they received.

Step 2: For every sector id

2.1 For every four consecutive levels find the centre of distance by taking average of the distance of node from the BS.

2.2 Find the node which is nearest to that node and make it data cluster head.

Step 3: Every node then sends its own remaining energy to the data cluster head formed.

Step 4: Data cluster head then sends the information of routing cluster head to the one which is appointed the routing cluster head.

End

There is no communication from base station and nodes in the formation of routing cluster head because the location of nodes is calculated from the base station by using localization technique [16] .But there should be a communication from nodes to base station for finding data cluster head. Data cluster head are formed by taking the average of distance from the nodes which will give the distance of the densely populated region.

The node which is near to that region will be elected as data cluster head. After that every node in that region sends its remaining energy to the data cluster head which later selects the node for being the routing cluster head on the basis of maximum energy available.

In this technique two cluster heads have been used in a cluster which will obviously reduce the energy loss and also lessen the frequency time for the selection of new cluster head which is done more frequently on the cluster structure if there is only one cluster head in a cluster [18].

6. ENCRYPTION ALGORITHM IN DLL

Till now the deployment of the nodes have been done and a network is formed , then the localization algorithm is applied to find out the coordinates of all nodes, after that the task of DCH and RCH assignment is done. Then the encryption of the data in data link layer is done to provide integrity and maintain the confidentiality of the data being transmitted. The proposed algorithm is given in following steps.

6.1 Encryption algorithm

Step 0. Start

Step 1. Append an "X" at the end of the message string if number of characters in message is not even.

Step 2. Make pairs of the characters and treat each pair as a block (2 bytes) for encryption.

Step 3. Replace the characters in the pairs by their corresponding Unicode value.

Step 4. Express the Unicode values in the following format, suppose 'a' and 'b' are the Unicode values of two characters in a pair.Express them as the following equation using partial fraction:

$1/(x-a)*(x-b)=A/(x-a) + B/(x-b)$.....(1)

⇨ $1= B(x-a)+ A(x-b)$;

x not= a, and x not=b..... .....(2)

Put x=a to find the value of A

Put x=b to find the value of B

Step 5. Either of these values A OR B can serve as an encrypted cipher for the corresponding pair.

Step 6. Transmit the character A for this pair (equivalently Character B can be transmitted)

Step 7.The last byte of the encrypted message will be a time interval't' that will indicate after what time the message containing the keys will be transmitted.

Step 8. After that time interval't' the key message will be sent, the key message is simply the string of plaintext Unicode of the leftmost character in each pair

Step 9. At the receiver side the node can calculate the value of the 'a' and 'b' by the given values 'A' and the key (which is simply plaintext Unicode of the leftmost character in the pair)

Step 10.Repeat the same process for all the pairs.

Step 11. Stop

6.2 Explanation with Example.

Proof: Suppose the message string to be sent is "fbdge".An extra "X" is appended to make number of characters even i.e. "fbdgex" and make pairs as "fb --dg-- ex".Suppose Unicode of 'b' is 4.and Unicode of 'f' is 6.

Express them in the form $1/(x-6)*(x-4) =A/(x-6) +B/(x-4)$..... (1)

⇨ $1=A(x-4) +B(x-6)$

Putting x=6 gives A=1/2

And putting x=4 gives B=-1/2

Thus only A needs to be transferred for the pair "fb".Even if the adversary finds intercepts "A" and hence calculates "B" there is no way to find out Unicode 'a' and 'b' (i.e. 6 and 4) from the equation $1/(x-a)*(x-b) = A/(x-a) +B/(x-b)$ by putting A=1/4 and B=-1/4. This is so because of the equation (2) in the proposed algorithm. In equation (2) the terms (x-a)*(x-b) were cancelled from either side or at the same time, assumed that 'x' is not equal to 'a' or 'b'. But in the very next step we put x=a and x=b to find out 'A' and 'B'. The concept can further be realized by extending the argument that 1/0, 5/0,145/0, 34354546/0.... All of them are "infinity". It means given two terms, "infinity" and the denominator there is no way to find out the numerator. Thus, it is a one-way scheme in which one can find 'A' and 'B' from 'a' and 'b' but not the reverse. This is the strength of the algorithm. Moreover, it utilizes the concept of delaying the disclosure of key which was suggested in the paper [19].

This encryption algorithm utilizes the concept of randomness based on the data sensed by the sensor nodes. In a sense it generates one time pad which is almost random.

This algorithm eliminates the need of key management techniques like key storage, refreshing the key or key-generation.

This algorithm is energy efficient and has linear complexity; however it needs an extra byte per message string. However this trade-off is insignificant compared to its utility which is mostly due to lesser memory usage, lesser requirement of processing power and one-way nature.

7. CONCLUSIONS

The proposed localization algorithm uses only two GPS receivers and works on WSN of any shapes and sizes. The use of only two GPS receivers makes it cost effective and easy to deploy. It also provides the absolute positioning of the sensor node in the surveillance area. A straightforward and robust algorithm is proposed that requires only a single round of node movement to localize all the neighbour nodes. This algorithm only requires constant storage per one-hop neighbour during localization. An attempt is also made to reduce the energy consumption by the sensor nodes through the proposed clustering algorithm by minimizing the number of cluster heads. The encryption algorithm that is proposed in this work is memory efficient, uses less power and less processing time. However it is not resistant against brute force attacks though it is difficult to make out the true meaning of data. Thus this approach gives an integrated framework for establishing a secured wireless sensor network.

However the whole approach is inherently limited by certain assumptions namely consideration of only static network and the localization algorithm does not support dynamic network. Also for the DLL Encryption algorithm an extra byte was transferred for each message that was to be encrypted. The proposed algorithm is also not tolerant to brute-force technique.

Despite these few drawbacks, this approach is a straightforward and energy-efficient technique to establish a secure WSN that eliminates the need of conventional key management techniques.

ACKNOWLEDGMENTS

We are thankful to our B.Tech students namely Dipak, Piyush & Bikas for helping us in data collection using GPS as well as in implementing the concepts and coming up with new ideas to augment our idea.

REFERENCES

[1] Römer, Kay; Friedemann Mattern, (December 2004) "The Design Space of Wireless Sensor Networks",IEEE Wireless Communications 11 (6): 54–61.

[2]Adrian Perrig, John Stankovic, and David Wagner, (2004) “Security in wireless sensor networks”, Commun.ACM, 47(6):53-57.

[3] Dileep Kumar, Dr. Shirshu Varma, (December 2009) “An Efficient Localization Based on Directional Antenna for Wireless Sensor Networks (WSN’s)”International Journal of Computer & Electrical Engineering,Volume 1, number 5.

[4] L. Hu and D. Evans, (2004)”Localization for mobile sensor networks”, Proceedings of MOBICOM 2004, pp 45–57.

[5] J. Caffery and G. Stber,(2000)”Overview of radiolocation in CDMA cellular systems”IEEE Personal Communications Magazine, 7(5):28-34.

[6] A.R. Masoum, A.H. Jahangir,Z. Taghikhani, and R. Azarderakhsh, (2008) ”A new multi level clustering model to increase lifetime in wireless sensor networks”, Proceedings of the Second International Conference on Sensor Technologies and Applications, pp 185-190.

[7] Haowen Chan Adrian Perrig Dawn Song, (2006)” Secure Hierarchical in Network Aggregation in Sensor Networks”, Proceedings of the 13th ACM conference on Computer and communications security, Pp: 278 – 287.

[8] K. Akkaya, M. Younis,(2005) “A survey on routing protocols for wireless sensor networks”, Journal of Ad Hoc Networks 3 (2005) pp 325–349.

[9] C.F. Chiasserini, I. Chlamtac, P. Monti, A. Nucci,(2002) “Energy efficient design of wireless ad hoc networks, Proceedings of the Second International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; and Mobile and Wireless Communications, Pp: 376 – 386.

[10] M. Chatterjee, S.K. Das, D. Turgut, (2002) "WCA: a weighted clustering algorithm for mobile ad hoc networks", Journal of Cluster Computing 5 (2) pp 193–204.
[11] A.D. Amis, R. Prakash, (2000) "Load-balancing clusters in wireless ad hoc networks", Proceedings of ASSET 2000, Richardson, TX, pp 25 – 32.
[12] S. Lindsey, C. Raghavendra, K. Sivalingam,(2001) "Data gathering in sensor networks using energy*delay metric" , Proceedings of 15th International Parallel and Distributed Processing Symposium, , pp. 2001–2008.
[13] S. Bandyopadhyay, E. Coyle,(2003) "An energy efficient hierarchical clustering algorithm for wireless sensor networks", Proceedings of IEEE Infocom, San Francisco, CA pp 6 – 28.
[14] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.
[15] O. Younis, S. Fahmy, (2004) "HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks", IEEE Transactions on Mobile Computing 3 (4) 366–379.
[16] Mihail L. Sichitiu and Vaidyanathan Ramadurai, (2004) "Localization of Wireless Sensor Networks with a Mobile Beacon", Proceedings of the First IEEE Conference on Mobile Ad-hoc and Sensor Systems (MASS 2004), (Fort Lauderdale, FL), pp 174—183.
[17] Hüseyin Akcan, Vassil Kriakov, Hervé Brönnimann and Alex Delis (2006) "GPS Free Node Localization in Mobile Wireless Sensor Networks", Proceedings of the 5th ACM International Workshop on Data Engineering for Wireless and Mobile Access (MobiDE'06), in conjunction with SIGMOD, Chicago, IL, USA, pp 35-42.
[18] Wireless sensor networks-Architecture and protocols-CRC press.
[19 TinyOS Manual, www.tinyos.net
[20] AVR Simulation and Analysis Framework, www. *compilers.cs.ucla.edu/avrora/*
[21] Younis, M., Youssef, M., and Arisha, K., (2002) "Energy-aware routing in cluster-based sensor networks" Proceedings of 10th IEEE International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunications Systems, pp. 129 – 136.
[22] H. Chan, A. Perrig, and D. Song,(2003) "Random key predistribution schemes for sensor networks," Proceedings of the 2003 IEEE Symposium on Security and Privacy,IEEE Computer Society, 2003,pp 197 - 204.
[23] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz,(2005) "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.