A Reliable Security Model Irrespective of Energy Constraints in Wireless Sensor Networks

D. Prasad
Department of Computer Engineering
Maharishi Markandeshwar University,
Mullana (Ambala), Haryana, India.
dprasadvns@gmail.com

Manik Gupta
Department of Computer Engineering
Maharishi Markandeshwar University,
Mullana (Ambala), Haryana, India.
manikjmu@gmail.com

R. B. Patel
Department of Computer Science,
D.C.R.U.S.T,
Murthal (Sonepat), Haryana, India.
patel_r_b@yahoo.com

***Abstract*- Wireless Sensor Networks (WSNs) are one of the most exciting and challenging research areas. It is an emerging technology that shows various applications both for public and military purpose. In order to operate these applications successfully, it is necessary to maintain privacy and secrecy of the transmitted data.**

In this paper, we have presented a Reliable Security Model (RSM) for WSNs. To incorporate the security, we are using four keys out of which two are static and remaining two are dynamic. One of the static key is obtained by composition of Q number of keys, and other is real-time MAC ID (RTMAC). Dynamic keys are computed on fly and keep on changing each time when the network is synchronized. In RSM, the synchronization time is less than the time required to compromise any node by an adversary, so that even if some nodes get compromised, the keying materials of the node have already been changed.

Keywords*- *Wireless sensor network (WSN); Sensor Node (SN); Base Station (BS); Static Keys; Dynamic Keys; Real-Time MAC ID (RTMAC).

I. INTRODUCTION

Wireless sensor networks (WSNs) are built up of sensor nodes (SNs), which consist of sensing, computing, communication, actuation and power components that cooperatively perform the task of collecting relevant data and monitor its surrounding for some change or event to occur [1]. Thus, two types of architectures were studied for WSNs. One for SNs itself and second for network architecture required for communication among the SNs. WSNs has its own features that not only differentiate it from other wireless networks but also craft the scope of wireless application to disaster relief, military surveillance, habitat monitoring, target tracking and in many civic, medical and security applications [2, 3, 20, 21]. Some features of WSNs that impose some limitation on WSNs and were kept in mind before developing this article are as following [11]:

A. Resource constraints

SNs have limited resources, including low computational capability, small memory, low wireless communication bandwidth, and a limited power battery.

B. Traffic characteristics

In WSNs, the primary traffic is in the upstream direction from the SNs to the sink node or BS, although the BS or sink nodes may occasionally generate certain downstream traffic for the purposes of query and control. In the upstream, this is a many-to-one type of communication. Depending on specific applications, the delivery of upstream traffic may be event-driven, continuous delivery, query-driven delivery, or hybrid delivery.

C. Small message size

Messages in sensor networks usually have a small size compared with the existing networks. As a result, there is usually no concept of segmentation in most applications in WSNs.

D. Sensor Location and Redundancy of Data

Position awareness of sensor network is important, since data collection is normally based on location. Also, there may be common phenomena to collect data, so there is a high probability that this data has some redundancy. There are three criteria that drive the common design issues for large-scale sensor networks; scalability (these networks might involve thousands of nodes), energy-efficiency (in particular, wireless communication can incur significantly higher energy cost than computation), and robustness (to environmental effects and node and link failures).

E. Network Lifetime

The time for which the network is operational or, put another way, the time during which it is able to fulfill its tasks (starting from a given amount of stored energy). It is not quite clear, however, when this time ends. Possible definitions are:

1) *Time to first node death:* When does the first node in the network run out of energy or fail and stop operating?
2) *Network half-life:* When have 50% of the nodes run out of energy and stopped operating?

F. Time to partition

When does the first partition of the network in two (or more) disconnected parts occur?

G. Addressing Schemes

Due to relatively large number of SNs, it is not possible to build global addressing schemes for the deployment of a large number of SNs as overhead of identity maintenance is high.

H. Density of nodes

In WSNs, the number of nodes per unit area i.e. the density of the network – can vary considerably. Different applications will have very different node densities. Even within a given application, density can vary over time and space because nodes fail or move; the density also does not have to be homogeneous in the entire network (because of imperfect deployment) and the network should adapt to such variations**.**

I. Maintainability

As both the environment of a WSNs and the WSNs itself change (depleted batteries, failing nodes, new tasks), the system has to adapt it by monitoring its own health and status to change operational parameters or to choose different trade-offs (e.g. to increase the interval of monitoring data and reduce quality when energy resource become scarce).

J. Node Deployment

Node deployment can be random, deterministic or self-organizing. For deterministic deployed networks the routes are pre-determined, however for random deployed networks and self-organizing networks route designation have been a challenging subject.

K. Energy consideration

Since the life-time of the WSNs depends on energy resources and their consumption by sensors, the energy consideration has a great influence on route design. The power consumed during transmission is the greatest portion of energy consumption of any node. Direct communication consumes more power than multi-hop communication; however the multi-hop communication introduces extra topology management and medium access control.

L. Miscellaneous applications

WSNs may be used in different environments supporting diverse applications, from habitat monitoring and target tracking to security surveillance and so on. These applications may be focused on different sensory data and therefore impose different requirements in terms of quality of service (QoS) and reliability. Thus sensor networks are application specific.

Now days, WSNs are not used only for security or social intention but also used for commercial purposes. Extensive research is going on in almost all fields of sensor network, including sensor design, communication protocol stack design, and operating system for sensors, security and management algorithm design. The design goals of WSNs are application specific, but share some common attributes like energy efficiency, scalability, robustness, network life time, fault tolerance, self-organization and data aggregation. Out of which, energy efficiency and security are more important. In recent years, the availability of cheap and tiny micro-sensors and low power wireless communication enabled the deployment of large quantity of wireless sensor nodes, which are scattered in the interested area.

In WSNs, routing, security and networks lifetime are seemed to be incompatible. But, in RSM, the balance of energy consumption among all the sensor nodes is maintained, in order to avoid the "hot spot" problem. Besides this, the availability of never lasting energy due to wireless power provides the security model more strength.

The main emphasis while designing and developing the protocol is uniform load distribution among SNs, in order to increase the network lifetime. Many protocols existing in the literature [22-25], minimize energy consumption on routing paths. Even though these many existing approaches increase energy efficiency, but technique such as; dynamic routing where, data is forwarded to nodes with the highest residual energy, may cause problem such as, unbounded delays. However, RSM is efficient enough to solve the security and energy issues, with dynamic routing and key management techniques that is not suffered from the traditional problems of unbounded delays and easy compromise of the nodes. Beside this, the network acts more efficiently in terms of energy with the help of wireless energy provided by the BS to the deployment area.

Rest of the paper is organized as follows. Section II summarizes the related works. In Section III, System model and protocol description is presented. Implementation of System Model is discussed in Section IV. In Section V, we analyze RSM in respect to energy, security and life of the network. System Model is compared with some existing techniques in Section VI followed by the results and discussions in Section VII. Finally, we conclude RSM and discuss the scope of future work in Section VIII.

II. Related Works

Security is a big issue, when WSNs are deployed in a hostile environment. Secret keys should be used to encrypt the exchanged data between communicating parties. In the Internet or traditional wireless networks, such as, cellular networks, most security protocols are based on asymmetric cryptography, such as; RSA or Elliptic Curve Cryptography (ECC) [6, 7] are not applicable, due to the high computational complexity, high-energy consumption and increased code storage requirements. Furthermore, due to unpredictable network topology and lack of infrastructure support, trusted-server based key distribution protocols are not suitable for WSNs either [5]. Research shows that key pre-distribution mechanism could be a practical method to solve the key distribution problem in WSNs. The basic idea of key pre-distribution scheme is preloading some secret keys into SNs, before they are deployed. After the deployment, the nodes discover shared keys for secure communications. It is divided into 3 phases; i.e. Key distribution, Shared key discovery and Path-key establishment. During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range, to find another node to communicate. A secure link is established, when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. For this purpose, various keying techniques are being used. Some of the common key management schemes are as follows [8]:

A. Single Network-wide Key Establishment

In this technique, a single key is preloaded into all the nodes of the network. After deployment, every node in the network can use the same key for the message encryption and decryption. The main advantages of this technique are minimal storage requirements and avoidance of complex protocols. However, such keys provide enough space to adversaries for accessing the network. If any node is compromised in this scheme, then entire network is compromised.

B. Pair-wise Key Establishment

In pair-wise key establishment, every node in the network has to stores n-1 key pairs. This can be eradicated when we use a Trusted BS, also called centralized key distribution center (KDC), to send the session keys for the communication, between any two nodes. This scheme has small memory requirement and perfectly controlled node replication, it is resilient to node capture and possible to revoke key pairs. The drawbacks of this scheme are that it is not scalable and the base station becomes the target of attacks.

C. Dynamic Key Management

Dynamic key management system was proposed by Eltoweissy et al., also called exclusion-based system (EBS) [26]. Here, various nodes and methods are disclosed for automatically disseminating key node contact information in a network. Some of the advantages of using a dynamic key management scheme are: improved network survivability and better support for the network growth.

The issue in creating a dynamic key management system is being able to make it secure and efficient. The EBS assigns each node k keys from a key pool of size k+m. If node capture is detected, re-keying occurs throughout the network. A disadvantage to this EBS scheme is that if even a small number of nodes in the network are compromised, information about the entire network could be uncovered by an adversary.

D. Public Key Schemes

A public key scheme employs a pair of different but associated keys. One of these keys is released to the public while the other, the private key, is known only to its owner. WSNs have mostly been using symmetric key and other non-public-key encryption schemes [27]. A drawback to these schemes is that they are not much flexible, but they are computationally faster. With limited memory, computing and communication capacity, and power supply, sensor nodes cannot employ sophisticated cryptographic technologies, such as; typical public key cryptographs. The use of public key cryptography on WSNs has not been tested enough to rule it out completely.

E. Q-Composite Random Key Management

In this scheme, BS generates key sets from the key pool, for each node. SNs needs to have at least Q number of keys in common to establish a communication link, rather than only one key, which enhances the security level as compared to those schemes having single common key.

Besides the key management techniques, we have used RTMAC [28] for real time data streaming in WSNs. RTMAC is a collision free TDMA based MAC protocol which uses channel reutilization technique based on the network topology to reduce its latency. It maximizes spatial channel reuse by avoiding false blocking problem of RTS/CTS exchange based wireless MAC protocols. RT-MAC reduces contention duration for control packets to facilitate faster traveling of data packets; thus, it reduces end-to-end delay of data packet transmission and hence facilitates periodic delivery of data packets as well as fast reporting of an alarming event.

Each of the above WSN key management scheme consists of three main components [9]:

(1) key establishment (2) key refreshment (3) key revocation

Key establishment is about creating a session key between the parties that need to communicate securely with each other. Key refreshment prolongs the effective lifetime of a cryptographic key, whereas, key revocation ensures that an evicted node is no longer to able to decipher the sensitive messages that are transmitted in the network.

The reliable security model proposed in this article is scalable, secure and energy efficient. It enhances the security level of Q-composite keys scheme by changing the keying material every time, the network is synchronized. To increase the scalability and life of the network, RSM is introducing one more parameter (i.e. distance between SNs) in the Q-composite key scheme, for the establishment of communication link between SNs. Beside the energy efficient method, the model also introduces the concept of power beam [12] to supply power wirelessly to the BS as well as to the network throughout the life of the rechargeable batteries and the laser diode arrays and thus increasing the lifetime of the network almost to infinity.

Due to the recent efforts of MIT and Intel Co. [14, 15, 16], wireless electricity comes into revolutionary phase, which motivate us to think upon and work over the concept so as to make the WSN’s life never lasting. Though this concept is motivating to work upon future applications, but still it is facing problem related to the transmission range, 3 to 8 meters. So, due to this problem as well as introduction of new hardware structure to the SNs, the current technology introduced by MIT and Intel Co. limits anyone to work upon WSN. But, if one thinks about the principle of power transmission in space to the space vehicles or space based solar power satellites (SPS), as mentioned in [17, 18] or to recharge batteries of satellites in geo-stationary orbits as in [19] made us to think beyond the concept of simple wireless electricity, as discussed in [14-16]. Though the concept of SPS is capable enough to provide unlimited power to the SNs in the deployment area as well as to the flying BS over it, but a large burden of extra cost is also involved in it as includes a large number of SNs and the BS to get charged through the satellites, which are governed by any third party and hence the point of security also arises. So, it would be more cost effective and more secured, if we are able to apply the same principle from the land itself rather than space, at the deployment area by the first party itself. This can be possible with Microwave power transmission (MPT) or Laser Power Beaming.

III. System Model & Protocol Description

We have divided this RSM into two phases i.e. pre-deployment phase and post-deployment phase.

A. Pre-Deployment Phase

In the pre-deployment phase, the network is deployed with an assumption that it is free from adversarial attacks during the setup phase. The pre-deployment phase deals with the following activities:

- Delivering wireless energy to the BS and SNs in the deployment area as in [12].
- Random deployment of SNs in the deployment area from the flying BS.
- Cluster formation among the sensor nodes in the deployment area.
- Generating a strong security model for the sensor nodes at their respective cluster ends.

Initially the power is supplied to the BS and SNs in the deployment area as in [12]. In RSM, the BS is considered to be any flying object like UAVs, which remains over the top of the deployment area. Though it may change its position, but it can compute the Localization ID (LID) of the sensor nodes in the deployment area with its own reference [4] to incorporate more security with respect to the GPS system.

After the BS receives energy to the threshold level, the static sensor nodes are randomly deployed from the BS in the deployment area. On the basis of the node Localization ID (LID), the BS divides the deployment area into various clusters. After the successful completion of the deployment phase of the SNs, the power supply phase in the deployment area begins after some time, since the SNs are initially completely charged before deployment.

Besides regular power supply to the deployment area, the BS also generates key sets from the key pool, for each node. By using the concepts of Q-composite keys, the nodes needs to have at least Q number of keys in common to establish a communication link rather than only one key, which enhances the security level of the network. But, the drawback with Q-composite is that if the Q number of keys is common between two nodes, which are far away from each other, then to establish communication link between such nodes is a bad idea, because to make communication between these nodes is much energy consuming. Keeping this in mind, the security model imposes a new constraint of distance on Q-composite concept. In RSM, communication link between such nodes will be established, only if the distance between such nodes is less than or equal to some threshold value D_0. The value of D_0 is guided by the deployment area and the density of nodes within that area.

ID_1	LID $_{12}$	$RTMAC_1$	$K_{11}, K_{12}, K_{13}, \ldots\ldots\ldots, K_{1K}$
ID_2	LID $_{22}$	RTMAC $_2$	$K_{21}, K_{22}, K_{23}, \ldots\ldots\ldots, K_{2K}$
ID_3	LID $_{35}$	RTMAC $_3$	$K_{31}, K_{32}, K_{33}, \ldots\ldots\ldots, K_{3K}$
: : : ID_N	: : : LID_{N9}	: : : RTMAC $_N$	$K_{N1}, K_{N2}, K_{N3}, \ldots\ldots\ldots, K_{NK}$
Sensor ID	Location ID	RTMAC	Sensor Key Sets

Figure 1. Data structure representing node information

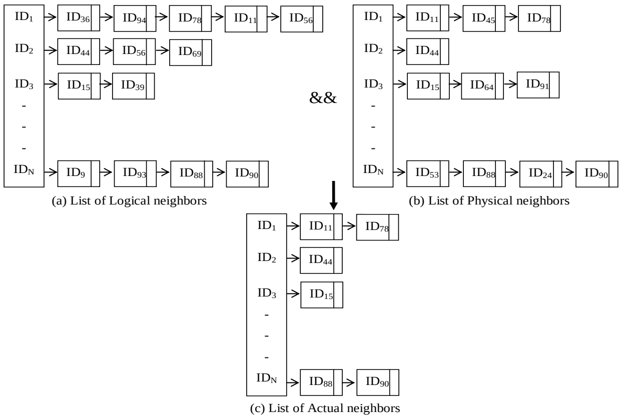
In RSM, the BS generates N key sets of K keys in each, from the key pool, for the node to be deployed in the deployment area, and maintains a list containing node ID, node Localization ID (LID), Real-time MAC ID (RTMAC) and key sets assign to the node, as shown in Figure 1. RTMAC allows sensors to go to sleep when they are not communicating and hence it conserves energy. In RSM, nodes having Q keys in common, are known as logical neighbors, nodes having distance less than or equal to D_0 between them, are known as physical neighbors and nodes satisfying both criteria, are known as actual neighbors.

1) Finding Logical Neighbor (LN): The method of finding Logical neighbors is straightforward. To find the Logical neighbors of any node, BS compare all the keys in the key set, assign to the node under consideration, with all the keys in the key sets assign to other nodes one by one, and whenever BS find any node having Q keys in common with the node under consideration, it store the ID of that node in the 'LNbr' list. The BS finds all logical neighbors for each node and stores them in list 'LNbr', as shown in Figure 2(a). If any entry in the list 'LNbr' remains empty then BS assign new key set to the corresponding nodes and repeat the process.

2) Finding Physical Neighbor (PN): To find the physical neighbors of any node, BS compute the distance of the node under consideration with all its logical neighbors and store the ID of all those node, which distance is less than or equal to D_0 in 'PNbr' list as shown in Figure 2(b).

Finding Actual Neighbor (AN): With the help of these two lists, for each nodes BS finds all those nodes, which falls within distance D_0 and having at least Q keys in common and store them in 'Nbr' list, as shown in Figure 2(c). Any empty location in list 'Nbr' indicate that the corresponding node falls far away from the remaining node, which chance is very rare, because of dense deployment, and even if it happened, we can ignore it, because such nodes are very few in numbers.

In this way, all the exhaustive operations are managed by the BS itself rather than the SNs in the deployment area. Hence, we can achieve more security even in large sized network without any loss of energy as in the conventional scheme of the Q-Composite scheme.


ID_1 → ID_{36} → ID_{94} → ID_{78} → ID_{11} → ID_{56}
ID_2 → ID_{44} → ID_{56} → ID_{69}
ID_3 → ID_{15} → ID_{39}
ID_N → ID_9 → ID_{93} → ID_{88} → ID_{90}
&&
ID_1 → ID_{11} → ID_{45} → ID_{78}
ID_2 → ID_{44}
ID_3 → ID_{15} → ID_{64} → ID_{91}
ID_N → ID_{53} → ID_{88} → ID_{24} → ID_{90}
ID_1 → ID_{11} → ID_{78}
ID_2 → ID_{44}
ID_3 → ID_{15}
ID_N → ID_{88} → ID_{90}

(a) List of Logical neighbors (b) List of Physical neighbors

(c) List of Actual neighbors

Figure 2. List of various neighbors maintained at BS.

B. Post-Deployment Phase

Once the BS obtains the actual neighbors for all nodes, it constructs two network graphs where, edges represents secure link and nodes represents sensor nodes in the network. The graphs are obtained separate for both odd as well as even RTMAC values, stored in the sensor nodes, which work on switching basis. The network graph which is active will sense the data but the inactive network will be in sleep mode to preserve energy and to provide illusion of dead network to the adversary if he was trying to capture a network, which suddenly enters into sleep mode by transferring the last sensed packet to the immediate physical neighbor, present in the alternate network. From the network graphs, the BS obtain two minimum spanning trees as shown in the Figure 3, and designate one of the node as cluster head in the active tree and set it to communicate with base station. This delegation must be on rotation basis, otherwise the energy of the node communicating continuously with the BS will be depleted soon and the whole network will be disconnected. To rotate the delegation, BS can choose any scheduling scheme; RSM introduced in this paper is using the scheme presented in GANM [10]. BS computes link keys between a node and all of its neighbors by applying some hash function, as shown in the algorithm. It also computes a timer value, as shown in the algorithm, to synchronize the network.

Here, both the trees so obtained are the representations within the same cluster units and the corresponding position nodes in odd and even networks are actually the physical neighbors (PNbr) of each other. Here, the dotted lines show the traversing of tree to rotate the delegation. It can be seen in figure 3 that when the delegation reached to the last node of the odd minimum spanning tree, it gets shifted to the even minimum spanning tree and vice-versa; thus giving illusion to any continuously observing adversary that the network becomes dead after sometime, which in fact is in sleeping mode for security and energy efficiency purpose.

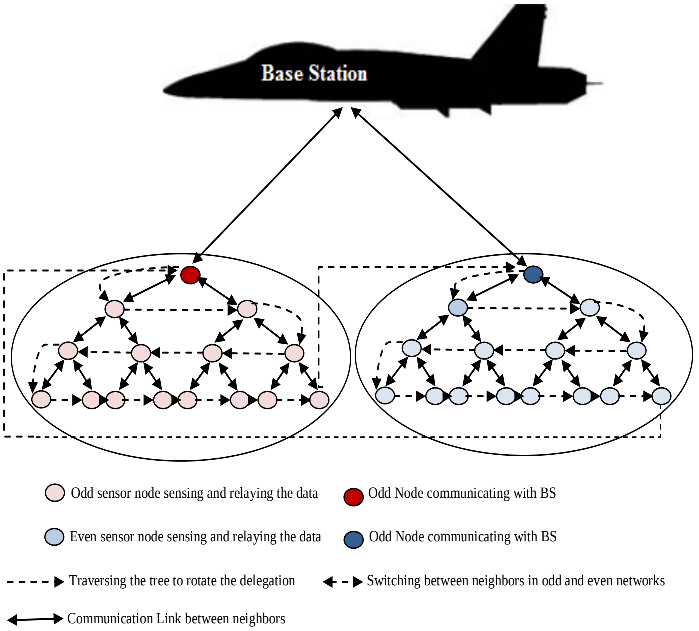

Base Station
Odd sensor node sensing and relaying the data
Odd Node communicating with BS
Even sensor node sensing and relaying the data
Odd Node communicating with BS
Traversing the tree to rotate the delegation
Switching between neighbors in odd and even networks
Communication Link between neighbors

Figure 3. Communication network of our protocol

During this process of shifting the delegation from odd to even tree or vice-versa, each of the nodes in the tree which is going to be in sleep mode will send its last sensed data packet to its corresponding physical neighbor in other tree which will now act as active tree. Since, the physical neighbor in active tree will replace the corresponding node in the tree in sleep mode hence it is assumed that it will now sense the data in approximately the same sensing limits.

Once the link keys and timer value are computed, BS constructs N packets; one for each node, containing node ID, RTMAC, set of link keys for that node and timer value, as shown:

Cluster ID	Node ID	Neighbors Link Keys	Timer Value	RTMAC

Synchronization Packet

BS broadcast these packets in the network. Nodes in the area receive only the packet meant for them, store this information within its memory, and ignore other packets. On receiving the above packet, timer within the node is triggered and the whole network gets synchronized. Once the network is synchronized, nodes within the cluster start sensing the surrounding and send the sensed data, in the following format to its parents, where, these data are aggregated and this aggregated data is forwarded to their parent; this process is continued and finally aggregated data reaches to the node communicating with BS through which data is reached to the BS.

Source ID	Neighbors Link Keys	Timer Value	Data	RTMAC

Data Packet

This whole process of resynchronization is repeated after the regular interval of time in order to enhance the security level of each cluster within the network, by generating unpredictable key values, in the least possible interval. To enhance the security level further, link keys and timer values may be encrypted before their transmission in the data packet.

IV. Implementation of System Model

In our network model, we have assumed that all sensors are distributed in an evenly randomized manner in a polygon region, and the network has the following properties:

1) There exists a unique BS, located at the top of the network with a maximum height of 1 mile due to the power constraint of power beam [13].
2) Each SN has a unique identity.
3) All sensors cannot move after being deployed.
4) Network is homogeneous i.e. all sensor nodes are equivalent, having the same energy, computing and communication capacity.
5) Location of nodes is obtained using virtual co-ordinate system as in [4].
6) The transmitter can adjust its amplifier power based on the transmission distance.
7) Each sensor node consists of photo-voltaic cells for charging the power both from the sun as well as from the beam director embedded at the BS.

A. Algorithm

List 'LNbr' is an array of pointer, in which locations are pointing to the link list of ID of logical neighbors of the node under consideration (i.e. nodes with Q keys in common, can be represented as $CKeys_{I,J}$ for nodes I and J), 'PNbr' is an array of pointer, in which locations are pointing to the link list of ID of those nodes whose physical distance is less than D_o, 'Nbr' is an array of pointer, in which locations are pointing to the nodes allowed to communicate with each other, Nbr[O] and Nbr[E] are the neighbor lists for odd and even MST respectively and 'Iso' is list of all those nodes, which are isolated from the network. Besides this, a list RTMAC[] is maintained to store the RTMAC numbers of the sensor nodes respectively.

The function SECURE_LINK(Iso[I]) is used to establish a secure link among the isolated nodes present in the list 'Iso[I]'. However, the function RESYNCHRONIZE( ) is used to resynchronize the entire network in the synchronization time, 'T_{sync}' so that, each delegate node, 'Dlgt' in the list communicates with the BS on round robin basis. The synchronization time, 'T_{sync}' must be less than the threshold time, 'T_0' (by some tolerance value ε) is the time taken by an adversary to capture any node in the network. Moreover, T_{BS} and timer[I] are the timers maintained at the Base Station and at each node in the network; acting as their respective dynamic keys.

For each cluster in the deployment area, the following algorithm will be executed concurrently, so as to find the dynamic cluster head that will act as delegate node to communicate with the BS.

```
1)While((Nbr[1])||(Nbr[2])||(Nbr[3])||...||(Nbr[E])||…||(Nbr[O])
   = NULL) repeat steps 2 to 5
2) Initialize C :=1.
3) For I:=1 to N // Here, N=O+E.
      If (Nbr[I] = NULL) add its ID to Iso[C]; C:=C+1.
4) For I:=1 to C
      Generate new key set and replace the key set in
      KSets[I] corresponding to node Iso[I] by new set.
5) Call SECURE_LINK (Iso[I]).
6) Establish two way communication links by the link key as:
      K:= HASH {$k_1$||$k_2$||……||$k_Q$}.
7) Call MINIMUM_SPANNING_TREE for the graph
   obtained in step 6.
8) Traverse the Tree constructed in step 7 and store the nodes
   in Dlgt[I].
9) Initialize E[I]:= E[1].
10) while ((E[I] <= N/2) || (O[I] <= N/2)) repeat step 11 to 15
11) Temp:= $T_{sync}$:= $T_0$ - ε
12) while(Temp > 0 )
        a) Delegate node Dlgt[I] to communicate with BS.
        b)Temp: = Temp -1.
13) Call RESYNCHRONIZE ( ).
14) I:=I+1; Temp:= $T_{sync}$
15) If (E[I] == E[N/2]) then
      Set O[I]:= O[1] and transfer latest sensed data packet to
      corresponding PNbr in Odd network tree .
    Else If (O[I]== O[N/2]) then
      Set E[I]:= E[1] and transfer latest sensed data packet to
      corresponding PNbr in Even network tree .
```

```
RESYNCHRONIZE ( )

1) Temp:= $T_{sync}$
2) while (Temp >= 0) repeat steps 3 to 6
3) If (Temp == $T_{sync}$)
     a) Generate two way communication links between each
        pair of nodes by the link key as:
        K:= ((HASH {$k_1$||$k_2$||……||$k_k$}+
        LID[Dlgt[I]])*$T_{BS}$)
     b) x:= (int | ($T_0$-HASH{n||LID[Dlgt[I]]})/2| ).
     c) Set $T_{BS}$:= x.
     d) for I:=1 to N
            Set timer[I]:= x.
4) $T_{BS}$:= $T_{BS}$ + 1.
5) timer[I]:= timer[I] + 1.
6) Temp:= Temp-1.
```

```
SECURE_LINK (Iso[I])

1)Initialize E = 0 and O = 0.
2)for I:=1 to N repeat steps 3 to 5.
3)for J:=1 to N repeat step 4 to 5.
4)If ((I!=J) && (($CKeys_{I,J}$>=Q) && (|$LID_I$-$LID_J$|<=$D_0$) &&
  (RMAC[I]%2==0)))
  a)Add the IDs of the nodes in the neighbor list (Nbr[E]).
  b) E++
5)If ((I!=J) && (($CKeys_{I,J}$>=Q) && (|$LID_I$-$LID_J$|<=$D_0$) &&
  (RMAC[I]%2!=0)))
  a)Add the IDs of the nodes in the neighbor list (Nbr[O]).
  b) O++
```

V. Analysis of the System Model

In WSN routing, energy and security are the three primary factors that should be kept in mind, before designing any protocol. It is a general myth that efficient routing, security and networks lifetime are seemed to be incompatible, but RSM trying to balance all these parameters. All these aspects are considered in development of RSM.

We are using four keys for communication; out of which two are static (i.e. ID of node and RTMAC) and remaining two are dynamic, which are computed by applying hash function; as given in the algorithm. These two dynamic keys are changed every time, when the network gets resynchronized. So, in RSM, if some node gets compromised, it will be identified in the next synchronization. RSM resynchronize entire network in the time less than T_0, where, T_0 is the time required to compromise any node by an adversary. Shorter is the value of T_0, higher is the security level of the network.

In some protocols, highest residual energy nodes are identified within the network and all data to the BS are routed through that node, which may causes problem, such as, unbounded delays. However, rather than checking nodes with highest residual energy, RSM delegate a node to communicate with BS on rotation basis, which is selected based on GANM [10], and we kept this rotation time less than T_0, so that, even if somehow an adversary is able to capture it, its effect could be minimized.

Energy is considered to be most important factor to enhance the life of the network. In RSM, wireless energy is provided to both the BS as well as to the SNs in the deployment area; moreover, communication link between two nodes is established only if the distance between these two nodes is less than D_0 and they satisfied the key criteria of Q composite keys. In RSM, all the exhaustive operations to set up the network are running at the BS, which saves energy of SNs a lot. In Q-composite scheme, there is no restriction of distance between two nodes and if communication link is established between two nodes, which are far away with each other, then much more energy is required to communicate with each other, as compared to RSM. Also, by increasing the value of Q in Q-composite scheme, more energy gets dissipated to match more number of keys, but RSM make it possible to enhance security with larger values of Q and match the keys at the BS itself rather than at the deployment area, as in regular fashion.

VI. Comparison with Existing Techniques

Table I shows the comparison of RSM with Q-Composite and Peer-to-Peer key magangement schemes which are considered as strong techniques for security existing till now.

TABLE I. COMPARISONS OF RSM, Q-COMPOSITE AND PEER-TO-PEER

Attributes	***RSM***	***Q- Composite***	***Peer-to-Peer***
Feasible Key Set Size that can be Achieved	High	Small	Single Key is involved
Feasible Value of Q	Very High	High	Not Applicable
Security Level	Very High	High	High
Number of Keys Required to Establish Communication Among Nodes	3 Keys(1 static key in composition of Q keys and 2 dynamic keys)	Only 1 Key (composition of Q keys)	1Key (static)
Suitable Network Size	Very Large	Small	Large
Energy Consumption at SNs	Low	High	Low
Dynamic Keys	Yes	No	No
Network Scalability	Yes	No	No
Key Refreshment	Yes	No	No
Hot Sink Problem	Hot sink problem can never exist as the data aggregating node/sink node gets changed dynamically after short spans.	Hot sink problem may exist here, as the upstream communication path remains constant.	Hot sink problem may exist here, as in peer to peer communication also the upstream path remains constant.
Network Setup Time	Very High	High	Less

VII. Results and Discussion

Simulation is done using Matlab as the plotting software, as well as the calculation engine to plot results for the energy consumed by SNs with the increasing threshold distance value required to identify the physical neighbors, the effect of key set size on the time taken to establish a secure link, comparison between RSM and Q-Composite random key pre distribution and finally we plot the change in total flux intensity with respect to time, considering the total flux, considering both the flux due to solar energy and power beam.

The following are the simulation parameters considered for the implementation of the developed scheme:

- Deployment area is 100m X 100 m.
- The distance between the BS and the network is taken as 125m.
- Size of message is 80 bytes.
- Free space attenuation coefficient (E_{fs}) is 10 pJ/bit/m^2.
- Multipath attenuation coefficient (E_{mp}) is 0.0013 pJ/bit/m^4.
- Electronic power (E_{elec}) is 50 nJ/bit.
- Size of node ID 4 bytes.
- Size of MAC 8 bytes.

For realistic, our simulation uses the first order radio model as the communication model. Equation (1) and (2) represent the energy dissipation, when a SN sends or receives an *l* -bit message.

$$E_{recieve} = l \times E_{elec} \quad (1)$$

$$E_{trans} = \begin{cases} l \times (E_{elec} + E_{fs} \times d^2), if d \le \sqrt{\frac{E_{fa}}{E_{mp}}} \\ l \times (E_{elec} + E_{mp} \times d^4), if d > \sqrt{\frac{E_{fs}}{E_{mp}}} \end{cases} \quad (2)$$

Figure 4 shows the establishment of secure link among the randomly deployed static sensor nodes within the deployment area.

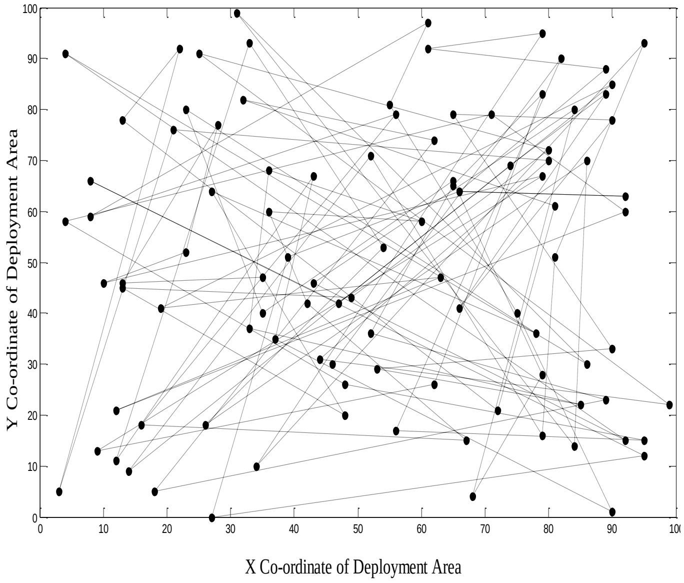


Figure 4. Deployment of SNs in the deployment area of 100m X 100m

Figure 5 shows that the times taken for the establishment of secure link decreases with the increasing key set size assigned to the sensor nodes. It is observed that the lifetime of a SNs decreases as the distance between two nodes increases as shown in Figure 6, and finally, Figure 7 shows the comparison between the traditional Q- composite random key pre-distribution technique and RSM. It can be observed that the energy consumption for the secure link establishment in Q-composite random key pre-distribution scheme gets increased with the increasing size of Q. However, in RSM, the energy consumption remains constant, since all the exhaustive tasks are managed by the BS rather than SNs itself.

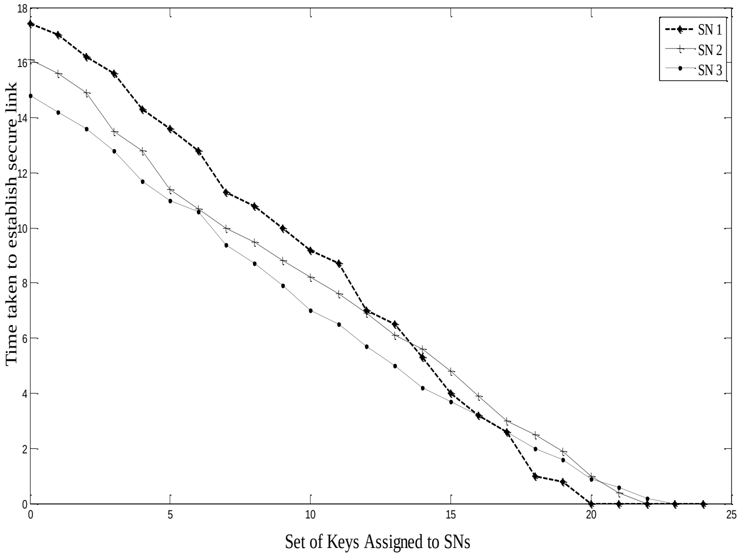


Figure 5. Effect of Key Set Size on Secure Link Establishment

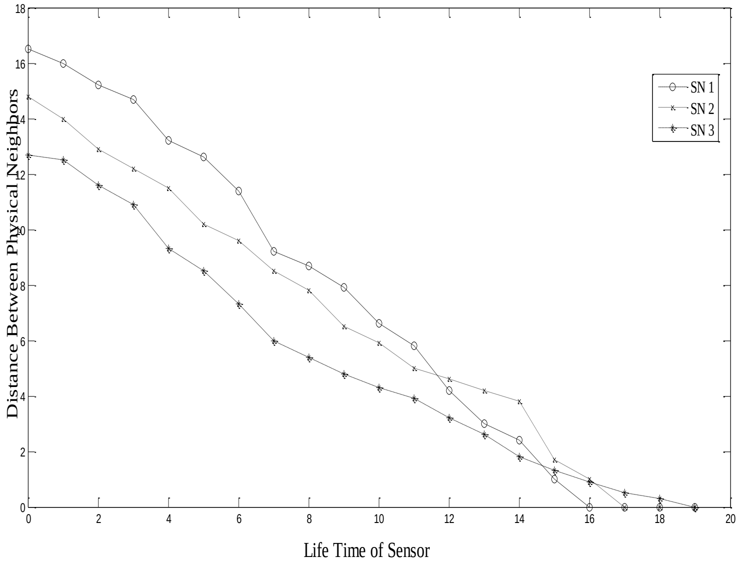


Figure 6. Effect of Distance between the Neighbors on the Lifetime of SNs

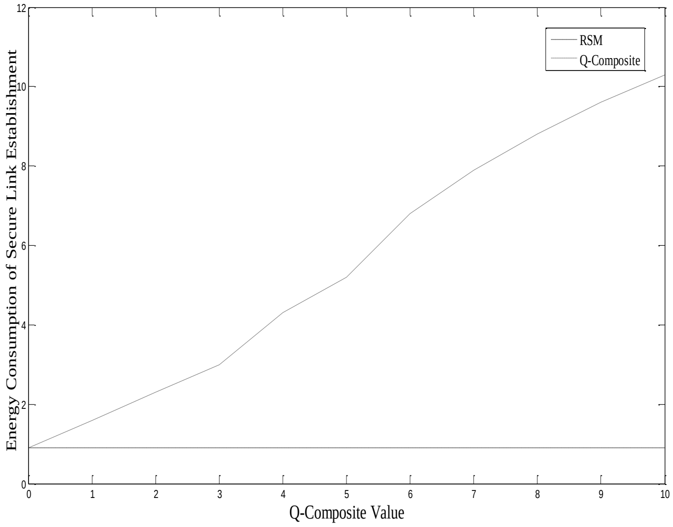


Figure 7. Comparison of Q-Composite Scheme with RSM

VIII. Conclusion and Scope of Future Work

In this article, we have presented a system model (RSM) for WSNs. The design of RSM is motivated by the observation of Q- composite scheme. To enhance the security, RSM keeps on changing keying materials every time network gets resynchronized.

Some of the advantages of RSM are as follows:

1) RSM ensures high energy at the BS end, rather than any assumption in fictions.

2) RSM provides ample amount of energy to the BS as well as to the SNs with a very low investment at the corporate end.

3) High energy by RSM may also ensure continuous sensing of data rather than periodic sensing as in general techniques of WSN.

As a future work, one can work upon some good robotics technology to introduce Mobile Sensor Nodes by taking advantage of high energy and homogeneous distribution of SNs even though they have been spread randomly from the BS as well as fault revoking can be done easily at the deployment end.

References

[1] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey”, Computer Networks Journal, Elsevier Science, Vol. 38(4):393-422, No. 4 pp 393–422, March 2002.

[2] Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler. “Wireless sensor networks for habitat monitoring”, In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[3] Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. “Lessons from a sensor network expedition”, In First European Workshop on Wireless Sensor Networks (EWSN'04), January 2004.

[4] Ajay Kr. Gautam (Member IEEE), and Amit Kr. Gautam, “Accurate Localization Technique using Virtual Coordinate System in Wireless Sensor Networks”, International Journal of Recent Trends in Engineering, Vol 2, No. 5, November 2009

[5] S. A. Camtepe and B. Yener, “Key distribution mechanisms for wireless sensor networks: a survey,” Department of Computer Science, Rensselaer Polytechnic Institute, Tech. Rep. TR-05-07, March 23 2005.

[6] J.-P.Kaps, “Cryptography for ultra-low power devices”, Ph. D. thesis, at Worcester Polytechnic Institute, 2006.

[7] Heo, J., Hong, “Efficient and authenticated key agreement mechanism in low-rate WPAN environment”, International Symposium on wireless pervasive computing, pp. 1-5, Phuket, Thailand 16 – 18 January 2006, IEEE 2006.

[8] A Survey of Key Management Schemes in Wireless Sensor Networks.Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway; Computer Communications, Special Issue On Security On Wireless Ad Hoc and Sensor Networks.

[9] Key Management Building Blocks for Wireless Sensor Networks; Yee Wei Law, Jeroen Doumen and Marimuthu Palaniswami: The University of Melbourne, Australia, University of Twente, The Netherlands.

[10] Devendra Prasad, R. B. Patel, Ajay Kr. Gautam “A Reconfigurable Group Aware Network Management Protocol for Wireless Sensor Networks”, in proceeding of the IEEE International Conference on Advance Computing(IACC), Patiala, India, 6-7 March 2009.

[11] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey”, Computer Networks Journal, Elsevier Science, Vol. 38, No. 4 ,pp 393–422, March 2002.

[12] Manik Gupta, D. Prasad, R.B. Patel, “FREEDOM: Fault Revoking and Energy Efficient Protocol for the Deployment of Mobile Sensor Nodes in Wireless Sensor Networks”, International Journal of Computer Science Engineering and Applied Research, Vol. 1, No. 1, pp 1-9, November 2010.

[13] T.J. Nugent and J.T. Kare “Laser Power for UAVs”, Laser Motive White Paper- Power Beaming for UAVs, NWEN, March 2010.

[14] http://technologyreview.com/energy/18836/page1/

[15] http://www.mit.edu/~soljacic/

[16] http://www.gizmag.com/intel-researchers-working-to-commercialise-wireless-power-sources/9858/picture/50110/

[17] W. Neil Johnson, Keith Akins, James Armstrong, Kwok Cheung, Glen Henshaw , Steven Huynh, Paul Jaffe,Matthew Long, Michael Mook, Michael Osborn, Robert Skalitzky, and Frederick Tasker, Jill Dahlburg, Michael N. Lovelette, David Huber, Mark Dorsey, Donald Gubser, Philip Jenkins, Scott Messenger, John Pasour, Robert Walters, Nathan Smith, Wayne Boncyk, Michael Brown, Robert Bartolo and Keith Williams “Space-based Solar Power: Possible Defense Applications and Opportunities for NRL Contributions” October 23, 2009.

[18] Glaser, P.E., "The Future of Power From the Sun," Intersociety Energy Conversion Engineering Conference (IECEC), IEEE publication 68C-21- Energy, 1968, pages 98-103.

[19] HerbertW.Friedman, “Near-Term Feasibility Demonstration of Laser Power Beaming” SPIE's International Symposium on Optoelectronic and Microwave Engineering Los Angeles, California January 25-27, 1994.

[20] Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton. “Resuscitation monitoring with a wireless sensor network”. In Supplement to Circulation: Journal of the American Heart Association, October 2003.

[21] G.L. Duckworth, D.C. Gilbert, and J.E. Barger. “Acoustic counter-sniper system”, In SPIE International Symposium on Enabling Technologies for Law Enforcement and Security, 1996.

[22] S. Bandyopadhyay, E. Coyle, "An energy-efficient hierarchical clustering algorithm for wireless sensor networks", in Proceedings of the IEEE INFOCOM 2003, San Francisco, IEEE Computer Press, July 2003, pp. 1713 -1723.

[23] H. O. Tan, "Power efficient data gathering and aggregation in wireless sensor networks", SIGMOD Record, 2003, 32(4): 66 -71.

[24] Y. Tang, M. Zhou, X. Zhang, "Overview of Routing Protocols in Wireless Sensor Networks", Journal of Software, 2006, 17(3):410-421

[25] O. Younis, S. Fahmy, "Distributed clustering in Ad hoc sensor networks: A hybrid, energy-efficient approach", in Proceedings of the IEEE INFOCOM 2004. Hong Kong: IEEE Computer Press, 2004, pp. 630-640.

[26] M. Eltoweissy, M. Moharrum, R. Mukkamala, “Dynamic key management in sensor networks,” IEEE Communications Magazine, Vol. 44, No. 4, April 2006, pp. 122- 130.

[27] A. S. Wander, N. Gura, H. Eberle et al., “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks,” in Proceeding of the Third IEEE International Conference on Pervasive Computing and Communications (PERCOM), 2005.

[28] Brajendra Kumar Singh, Kemal Ertugrul Tepe “Feedback based real-time MAC (RT-MAC) protocol for wireless sensor networks”, in Proceedings of the 28th IEEE conference on Global Telecommunications (GLOBECOM'09), 2009.

AUTHORS PROFILE

Devendra Prasad is an Associate Professor in the Department of Computer Science and Engineering, M.M. University, Haryana, India. Devendra Prasad is in teaching and Research & Development since 1996. He has supervised several M. Tech, and M. Phil Thesis. Devendra Prasad received his B.E. degree from Kumaon University, Nainital, India in 1995, M.Tech. Degrees from Kurukshetra University, Kurukshetra, India in 2007. He is currently enrolled as a PhD student in the Department of Computer Science and Engineering at M. M. University, Haryana, India. His research area is security, Fault tolerant and data dissemination, in wireless sensor networks.

Manik Gupta is a member of IAENG-International Association for Engineers and currently enrolled as a student of Masters of Technology in Computer Science in the Department of Computer Science, Maharishi Markandeshwar University, Mullana, Ambala, India. He had been awarded for Best Research Paper, in December, 2010. He also worked as Software Developer for one year after completing his Bachelors Engineering in Computer Science from University of Jammu. His research area is Security, Energy Efficiency, Fault Tolerance, Fault Revoking and Mobility in Wireless Sensor Networks.

Dr. R. B. Patel received PhD from IIT Roorkee in Computer Science & Engineering, PDF from Highest Institute of Education, Science & Technology (HIEST), Athens, Greece, MS (Software Systems) from BITS Pilani and B. E. in Computer Engineering from M. M. M. Engineering College, Gorakhpur, UP. Dr. Patel is in teaching and Research & Development since 1991. He has supervised 30 M. Tech, 7 M. Phil and 1 PhD Thesis. He is currently supervising 3 M. Tech, and 8 PhD students. He has published more than 100 research papers in International/National Journals and Refereed International Conferences. He had been awarded for Best Research paper many times in India and abroad. He has written numbers books for engineering courses (These are “Fundamentals of Computing and Programming in C”, “Theory of Automata and Formal Languages”, “Expert Data Structures with C,” “Expert Data Structures with C++,” “Art and Craft of C” and “Go Through C”. His research interests are in Mobile & Distributed Computing, Mobile Agent Security and Fault Tolerance, development infrastructure for mobile & Peer-To-Peer computing, Device and Computation Management, Cluster Computing, Sensor Networks, etc.