International Journal of Recent Engineering Science (IJRES)
ISSN: 2349 – 7157 / doi: 10.1445/23497157/IJRES-V6I1P105
Volume 6 Issue 1, 21-27, Jan-Feb 2019

Design and Development of Force Intense Mutual Assemble Key pre-distribution Proposal in Wireless Device Network

Dr. S. Ravichandran[1], R. Benjohnson[2]
[1](Computer Science Department, Annai Fathima College of Arts & Science, Madurai, India)
[2](Computer ApplicationsDepartment,Coimbatore Institute of Management & Tech.,Coimbatore,India)

Abstract

Key pre-distribution establishment in a sensor network is a stimulating problem due to the resource constraints on sensor nodes. However, it is not feasible to use old-style key management techniques such as asymmetric key cryptosystem and key distribution center (KDC). Also, the physical compromising of sensor nodes by an adversary is an emerging problem in a sensor network. There is several key pre-distribution techniques have been proposed for pairwise key establishment in sensor networks recently. One of the existing schemes which are a combination of probabilistic generation key pre-distribution scheme and polynomial pool-based key pre-distribution scheme. In this work, a new scheme Pairwise Shared Group Key pre-distribution, has been introduced, where the simulation results of the proposed scheme assure high probability and low communication overhead. Analytical results will be further done for retrieving better performance in energy consumption security, memory overhead, and communication overhead by comparing with the existing scheme. Our results clearly show that our scheme performs better in network resilience to node capture than the existing scheme if used in wireless sensor networks with mobile sink.

Keywords – *Wireless Sensor Network, Distributed Wireless Sensor Network, Key Distribution Center, Mobile Sink*

I. INTRODUCTION

The wide-spread organization of sensor systems is not too far off. A network of thousands of sensors may present an inexpensive solution to a variety of our challenging problems: real-time traffic monitoring, building safety monitoring (structural, fire, and physical security monitoring), military sensing and tracking, distributed measurement of wildlife monitoring, seismic activity, wildfire tracking, real-time pollution monitoring and so on. Many applications are enthusiastic about the secure operation of a sensor network and have serious consequences if the network is compromised or disrupted. Energy-aware distributed intelligent data gathering with wireless sensor networks may be a hot stock lately thanks to the emerge of a massive data paradigm. Wireless sensor networks (WSNs) share several common properties with normal wireless networks. The two incorporate varieties of battery fueled hubs have constrained computational capacities and Memory and accept discontinuous remote correspondence through recurrence and, conceivably, optical connections. They also include data-collecting nodes which cache the sensed data and make them available to the processing components of the network and control nodes which monitor the status of the sensor nodes and broadcast

Traditional cryptographic algorithms in unplanned networks will not be adapted to WSN within the near-term future since battery-operated sensor nodes have low power and limited computation power and Memory. For instance, employing a public-key cryptographic during a sensor network is dear thanks to computation cost. Symmetric key algorithms became the tools of option to provide a low-cost, secure communication between sensor nodes. Many research proposals have addressed fixing a (pairwise) key [1] among the communication sensor nodes, mentioned as key. Wireless sensor networks are composed of independent sensor nodes deployed during a neighborhood, working collectively to watch different environmental and physical conditions like motion, temperature, pressure, vibration sound, or pollutants. The most reason for the advancement of wireless sensor network was military applications in battlefields within the start, but now the appliance area is extended to other fields, including industrial monitoring, controlling traffic, and health monitoring. Different constraints like size and price results in constraints of energy, bandwidth, Memory, and computational speed of sensor nodes.

A wireless sensor node during a network consists of the subsequent components,

- Microcontroller.
- Radio transceiver.
- Energy source (battery).

II. RELATED WORK

A. Energy Conservation Schemes

S.Ganeriwal et al. proposed that the power source could be impossible or inconvenient to recharge the battery because nodes may be deployed in a hostile or unpractical environment. Sensor networks should have a lifetime long enough to fulfill the application

requirements. In many cases, a lifetime in the order of several months, or even years, may be required. The most significant energy conservation operation is putting the radio transceiver in the (low power) sleep mode whenever communication is not required. Preferably, the radio ought to be turned off when there is no more information to send/get and ought to be continued when another information parcel gets prepared. In this way, nodes alternate between active and sleep periods depending on network activity [3].

The following are the two parameters that focused.

1. Topology Control
2. Power Management

a) Topology Control

It is possible to take advantage of node redundancy, which is typical in sensor networks, and adaptively select only a minimum subset of nodes to stay active for maintaining connectivity. Nodes that are currently not needed for ensuring connectivity can go to sleep and save energy. The optional subset of nodes that guarantee connectivity is referred to as topology control. In the Location driven protocols, the Node itself decides which Node to turn on and when based on the Location of sensor nodes, which is assumed to be known [2].

GAF (Geographical Adaptive Fidelity) is a location-driven protocol that reduces energy consumption. In the connectivity driven protocols, it dynamically activates/deactivate sensor nodes so that network connectivity, or complete sensing coverage, is fulfilled [8]—span ASCENT (Adaptive Self-Configuring sensor Networks Topologies).

b) Power Management

Active nodes (nodes selected by the topology control protocol) do not need to maintain their radio continuously ON. They can switch OFF the radio when there is no network activity, thus alternating between sleep and wake-up periods. Obligation cycling worked on dynamic hubs as a force on the board. The On-demand protocols take the most intuitive approach to power management. The basic idea is that a node should wake-up only when another node wants to communicate with it. The principle issue related to on-request plots is the way to illuminate the resting hub that some other hub is happy to speak with it. To this end, such plans ordinarily utilize various radios with various vitality/execution tradeoffs.

The idea behind scheduled schemes is that each Node should wake up at the same time as its neighbors. Nodes awaken consistent with a wake-up schedule and remain active for a brief interval to speak with their neighbors. Then, they go to sleep until the next time. With asynchronous protocols, a node can wake up when it wants and still communicate with its neighbors. This goal is achieved by properties implied within the sleep/wake-up scheme; thus, no explicit information exchange is required among nodes.

G. Wener-Allen et al., the approach is the processing of sensing by the sensor nodes are briefly described by carrying out the task of performing.

i. Date reduction
ii. In-network processing
iii. Data Compression
iv. Data Prediction

For the case of Data reduction, this scheme addresses the case of unneeded samples. Next to the In-network processing, it consists of performing data aggregation at intermediate nodes between the sources and the sink. In this way, the quantity of knowledge is reduced while traversing the network towards the sink. In the third case of Data compression, it can be applied to reduce the amount of information sent by the source nodes. This plan includes encoding data at hubs, which produce information, and disentangling it at the sink. Compression techniques are general. For the fourth case of Data prediction, this Model can predict the sensor nodes' values within certain error bounds and reside both at the sensors and the sink.

If the needed accuracy is satisfied, users' queries can be evaluated at the sink through the Model without the need to get the data from modes.

- Stochastic approach - bolstered likelihood inside the accessible information
- Statistic forecasting - Periodical samplings are wont to anticipate a future worth

To attain an energy-efficient data acquisition, three sampling techniques are used. They are as follows.

1) Adaptive Sampling Techniques

It has some Minor deviation in data. It exploits such similarities to reduce the amount of data to be acquired from the transducer. For instance, information of intrigue may change gradually with time. Right now, connections (for example, the way that results in tests do not vary significantly between one another) could likewise be abused to downsize the measure of acquisitions.

2) Hierarchical Sampling Approach

. It assumes that nodes are equipped with different types of sensors. As every sensor is portrayed by a given goal and its related vitality utilization, this framework powerfully chooses which class to enact to encourage a tradeoff between exactness and vitality preservation.

3) Model-based Active Sampling

It takes an approach similar to data prediction. A model of the sensed phenomenon is made upon sampled data in order that future values are often forecasted with certain accuracy. Model-based active sampling exploits the obtained Model to scale back the number of knowledge samples and also the quantity of knowledge to be transmitted to the sink – albeit this is not their main goal. J. Yick et al. proposed that the algorithm Mobility–

based approach is discussed to dissipate a low amount of power by eliminating the Funneling Effect, and therefore the energy will be saved automatically.

i) Funneling effect

In a static sensor, organize parcels originating from sensor hubs follow a multi – jump way towards the sink(s). Thus, a couple of paths are often more loaded than others, and nodes closer to the sink need to relay more packets to be more subject to premature energy depletion.

ii) Mobile-sink Approaches

Mobile Sink can move to a limited number of locations to visit a given sensor and communicate with it (sensors are supposed to be arranged in a square grid within the sensing area). During visits to nodes, the sink stays at the node location for some time. Nodes not in the coverage area of the sink can send messages along multi-hop paths ending at the M.S. and obtained using shortest path routing. One of the foremost well-known approaches is given by the message ferrying scheme. Message ferries are particular mobile nodes introduced into a sparse mobile ad hoc network to offer the service of message relaying. Message ferries move around within the network area and collect data from source nodes. They carry stored data and forward them towards the destination.

B. Key Management Schemes

a) Polynomial Pool-based Key pre-distribution

Pairwise key establishment in this framework has three phases: setup, direct key establishment, and path key establishment. The setup phase is performed to initialize the nodes by distributing polynomial shares to them. After being deployed, if two sensor nodes established a pairwise key, the first plan to do so through the direct key establishment. If they can successfully establish a common key, there is no need to start path key establishment; otherwise, these two nodes start path key establishment, trying to establish a pairwise key with the assistance of other sensor nodes. There are three phases.

i. Setup (Pre-distribution): Initialize the sensors by distributing polynomial shares to them.

ii. Direct Key Establishment: Sensors first attempt to set up direct keys

iii. Path Key Establishment: Establishpairwise keys with the help of other sensors

1) Phase-1 Pre-distribution

- Setup server randomly generates a group F of t-degree polynomials over the finite field Fq
- For each sensor node i, the server picks a subset of polynomials
- The server assigns the polynomial shares of these polynomials to node i

2) Phase-2 Direct key Establishment

- If both sensors have polynomial shares on an equivalent polynomial, they will establish the pairwise key directly
- Polynomial share discovery: the way to find a standard polynomial of which both sensors have polynomial shares
    - Pre-distribution
    - Real-time discovery

3) Phase-3 Path key Establishment

- Node i and j cannot build up a key legitimately
- Node i must find a path between I and j s.t. any two adjacent nodes within the path can establish a pairwise key directly
- Path discovery: How to find the key path
    - Pre-distribution
    - Real-time discovery

b) Probabilistic Generation key pre-distribution Scheme

There are three phases in this method. They are polynomial and generation key subsets assignment, mobile sink-sensor direct key establishment, and mobile sink-sensor path key discovery. Initially, the server generates two pools of random bivariate polynomials, each with unique I.D. and degree. To dynamically establish a link between the Mobile sink and a sensor node u, both have to identify that they have polynomial shares of a common polynomial. If the M.S. is not able to establish secure communication with S.N., then it has to start the path key discovery phase.

Eschenauer and Gligor [5] Relies on probabilistic key sharing among nodes of WSN. Utilizations straightforward shared-key disclosure convention for key dispersion, denial, and hub re-keying, three stages are included: key pre-circulation, shared-key revelation, and way key foundation.

1) Phase-1 Key pre-distribution

Generate an outsized key pool P and corresponding key identifiers, Create n key rings by randomly selecting k keys from P Load keyrings into nodes memory, Save key identifiers of a hoop and associated node identifier on a controller, for every node load a key which it shares with a base station.

2) Phase-2 Shared Key Discovery

Takes place during initialization phase after WSN deployment. Each Node discovers its neighbor in the communication range with which it shares a minimum of one key Node can exchange ids of keys that they pose and during this way discover a standard key. A safer approach would involve broadcasting a challenge for each key within the ring, such each challenge is encrypted with some particular key. The decryption of a challenge is possible as long as a shared key exists.

3) Phase-3 Path Key Establishment

During the path-key establishment phase, path-keys are assigned to choose pairs of sensor nodes within the communication range of every other but do not share a key. A node may broadcast the message with its id, id of intended Node, and a few keys that it possesses but not currently uses to all or any nodes with which it currently

has a longtime link. Those nodes rebroadcast the message to their neighbors. Once this message reaches the intended Node (possible through an extended path), this Node contacts the initiator of path key establishment. The analysis shows that after the shared-key discovery phase sort of keys on a hoop is left unused.

C. Key pre-distribution using Random Subset Assignment

This scheme is often considered as an extension of the essential probabilistic scheme in [5]. Rather than randomly selecting keys from an outsized key pool and assigning them to sensors, our method randomly chooses polynomials from a polynomial pool and assigns their polynomial shares to sensors. However, our scheme also differs from [5]. In [5], an equivalent key could also be shared by multiple sensors. In contrast, in our scheme, there is a singular key between each pair of sensors. If no quite t shares on an equivalent polynomial are disclosed, no pairwise keys constructed using this Polynomial between any two non-compromised sensors nodes will be disclosed. Now allow us to describe this scheme by instantiating the three components within the general framework.

a) Phase-1 Subset Assignment

The setup server randomly generates a group F of s bivariate t-degree polynomials over the finite field Fq. for every sensor node, the setup server randomly picks a subset of s' polynomials from F assigns polynomial shares of this s' polynomials to the sensor node.

b) Phase-2 Polynomial Share Discovery

Since the setup server does not pre-distribute enough information to the sensors for polynomial share discovery, sensors that require determining a pairwise key need to determine a standard polynomial with real-time discovery techniques. to get a standard bivariate polynomial, a sensor node may broadcast an inventory of polynomial I.D.s, or broadcast an encryption list α, Ekv (α), v = 1, ..., |Fi|, where Kv may be a potential pairwise key the opposite Node may have, as suggested in [5,6].

c) Phase-3 Path Discovery

If two sensors fail to work out a pairwise key directly, they have to start the path key establishment phase. During this phase, a source sensor node tries to hunt out another node, which can help set up a typical key with the destination node. The source node broadcasts an invitation message, which incorporates two lists of polynomial I.D.s (one for the source node and therefore the other for the destination node) to determine a pairwise key. If one among the nodes that receive this request is in a position to determine a standard key with both of the source nodes and therefore the destination node, it replies with a message that contains two encrypted copies of a randomly generated key: one encrypted by the pairwise key with the source node, and therefore the other encrypted by the pairwise key with the destination node. Both the source and, therefore, the destination node can then get the new pairwise key from this message. (Note that the intermediate Node acts as a KDC during this case.) In practice, we may restrict that a sensor only contacts its neighbours within a particular range. The conclusion of this paper [5] is Probabilistic generation key pre-distribution scheme provides node-to-node authentication and excellent resilience to node capture.

III. PROJECTED TECHNIQUE

. We assume a model sensor network has hundreds to several thousand low-cost power constrained, limited computation power, and nodes with limited storage. Sensor nodes conserve communication energy by aggregating the info in their internal buffer. The network has a high-end mobile sink. This versatile sink sensor is incredible than any sensor and has more calculation correspondence, vitality supply, and capacity ability. It goes about as a specialist to gather sensor te hub Sensor readings; each sensor hub can put away to 210 keys, an M.S. is equipped for hiding away to 1200 keys.

The key establishment patterns for a secure link between a node and the mobile sink falls into two methods, Direct and Indirect MS- sensor path key establishment. In direct key establishment, the mobile sink and the sensor share a common bivariate polynomial and at least one common generation key. In MS-sensor path key establishment, the M.S. and a sensor node "u" attempt to establish a pairwise key with the assistance of an intermediate node "i."

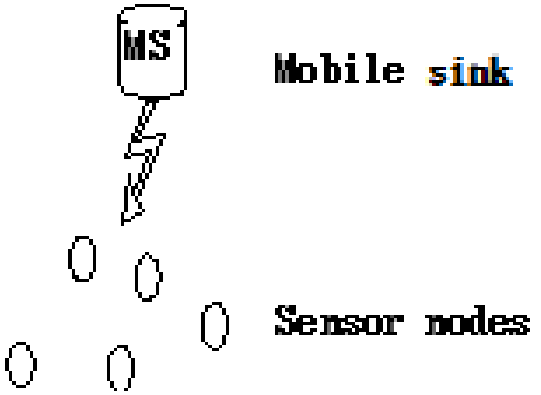

Figure1. Direct Key Establishment

Node i need to share a pairwise-key with both the M.S. and sensor node u; Node i randomly generates a replacement shared key, which will be sent on to M.S. and indirectly to Node u over the secure path i-MS-u.

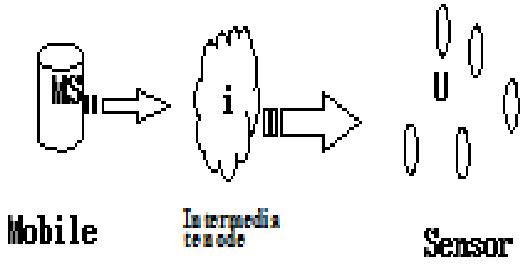

Figure2. Indirect Key Establishment

IV. IMPLEMENTATION

A. Distribution vs Shared Key Distribution Scheme

The framework of the proposed scheme is divided into three parts, Polynomial and Generation key subsets assignment, Mobile sink-sensor direct key establishment, and Mobile sink-sensor indirect key establishment.

a) Generate key pools for Polynomial and generation key scheme

The first step setup server separately generates two pools, it is called as |Sp| and |Sk|.

- Pool of |Sp| and Pool of |Sk
- Pool of |Sp| random bivariate polynomials each with a unique identification, namely IDp and degree t.
- Pool of |Sk| random generation keys each with a singular identification IDgk

Before the network deployment for each sensor node u, the setup server randomly picks a subset of S polynomial out of |Sp| and assigns polynomial shares of those S polynomials to the sensor node. Additionally, for each sensor node u, the setup server randomly selects a subset of K(K≤S) generation keys out of |Sk| and assigns them to the sensor node u. from these generation keys, KXC random keys are often calculated effectively, where C is that the total number of keys generated independently through a singular generation keys gi and a publicly known seed S. By applying a keyed hash algorithm repeatedly, the nth key employing a generation key gi, and a publicly known seed S is computed as,

K = Hashn (S, gi) ----------4.1

The setup server picks a subset of m (m k) generation keys randomly out of |Sk|, and a subset of S Polynomials out of |Sp|. Having an outsized number of generation keys within the mobile sink guarantee that M.S. can discover one common generation key with a sensor with high probability. The MS can establish a pairwise digital communication key with any sensor node on the fly. The MS and a sensor node share a minimum of one generation key and a standard bivariate polynomial; the 2 can establish a secure digital communication link directly. If the M.S. and therefore the sensor node does not share sufficient bivariate polynomials, however, the M.S. and therefore the sensor node start an MS-sensor path key discovery, trying to determine a pairwise data communication key with the help of other nodes.

b) Direct Key Establishment for MS-Sensor

In this module establishing a secure M.S.- sensor link dynamically between the M.S. and any node u within its communication range, the M.S. and a sensor u got to discover that both have the polynomial shares of a standard polynomial. The MS broadcasts "Hi" messages containing the MSid (IDms). Sensor node u within the M.S. range that heard the hello message can compute its keys by evaluating each of its assigned polynomial shares fID (u,y) at point IDms. The sensor node u sends one message for every computed s key containing the I.D. of the Node and s client puzzles. If the M.S. responds with the right answer to a minimum of one client puzzle, it's thus identified as having equivalent polynomial shares of a standard polynomial. Then next, after discovering a shared polynomial between M.S. and therefore the sensor node u, the M.S. broadcasts messages which contain a randomly generated number n were [0 ≤ n ≤ C]. If Node u heard the M.S. message, then for every preloaded generation key and a publicly known seed S, u can compute its nth keys as in (equation 3.1). For locating that both u and therefore the M.S. share a minimum of a standard generation key, Node u uses an equivalent method (Merklepuzzle). After the shared Polynomial and thus the shared generation key discoveries, a replacement MS-sensor data- communication link key Kd is generated because the hash of the key is evaluated from the shared Polynomial. Thus, the key is computed from the shared generation key. MS-sensor key setup is not performed between the M.S. and any node if a minimum of the 2 do not share a standard generation key or don't have the polynomial shares of a standard polynomial.

c) Path key Establishment for MS-Sensor

This phase occurs between any sensor node, such as node Y and the M.S. If the M.S. fails to determine an MS-sensor secure link directly with node Y, then it must start the MS-sensor path key discovery phase. In this phase, the M.S. needs to discover at least one of Node's Y.Neighbors that can act as an intermediate node which shares a common polynomial with the M.S., and a common polynomial with the destination node Y. We consider that M.S. can find a standard generation key with the node Y with high probability.

To establish an MS-sensor pairwise key with a destination node Y, MS needs to find a secure MS-sensor path through some of Node's Y neighbours which they can act as intermediate nodes along with the M.S. to node Y's path, which they can establish secure MS-sensor pairwise keys directly with both the M.S. and the destination node Y. The MS broadcasts a request message, which includes two lists of polynomial I.D.s (one for the M.S. and the other for the destination node Y). If an intermediate node v receives this request message, it tries to identify the polynomials in common with the M.S. and the polynomials in common with the destination node Y. If node v can identify at least one common Polynomial with the M.S. and one common Polynomial with node Y. Node v can establish a common key with both of M.S. and therefore the destination node Y to determine a pairwise key with both M.S. and the destination node Y. Node v replies with a message that contains two encrypted copies of a randomly generated key Kc: one encrypted by the pairwise key with the M.S.; the other by the pairwise key with the destination node. Both MS and Y can get the new key Kc from this message. The new M.S.- sensor data-communication link key is the hash value of Kc and the key computed from the shared generation key between M.S. and node Y.

.V. SIMULATION AND RESULTS

The Proposed Scheme provides more security along with energy consumption with the reputation of keys for the authenticated nodes which are participated in the network. Performance is measured by the following factors: security, time, Communication overhead, and Memory overhead. Gun plot is used to compare the distribution and shared key distribution scheme, which makes a vast difference in the key assigning process. The number of keys used in distribution and shared key distribution schemes is taken as a major problem. The total number of keys used in both schemes is assigned as pairwise- key. The pairwise-key difference for both the schemes is the total number of keys assigned and used for the sensor nodes. Each sensor node takes each unique key for transmission; hence it increases the Memory, key size, communication cost, storage capacity, which leads to the main problem in assigning keys for the sensor node. The shared distribution scheme is implemented to reduce the usage of keys in sensor nodes for transmission. The number of keys is reduced compared to the distribution scheme as half. When the number of keys is reduced in sensors, hence automatically, the major disadvantages will be rectified respectively.

A. Network Size vs Total no. of keys

The comparison between network size and the total number of keys is analyzed. The analysis takes the responsibility of the network with the number of sensor nodes in it and the number of keys used by the sensor node. When the size of the network increases accordingly, the number of keys increases. The graph shows the linear increase in the number of keys in distributed schemes and comparatively reduced in the shared key schemes. The better performance of the shared key distribution is shown respectively.

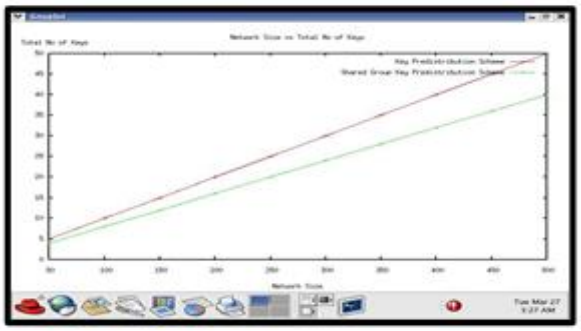

Figure3. Network Size vs total no. of keys

B. Simulation Time vs End to End Delay

The comparison between simulation time and an end to end delay process is made for both the schemes. When the number of keys increases, the simulation time also increases in the distribution scheme. When the simulation time increases automatically, the end-to-end delay also increases in the distribution scheme. The graph shows that the shared key distribution scheme gives a less simulation time and less end to end delay, which gives a better performance in the pairwise key assigning process.

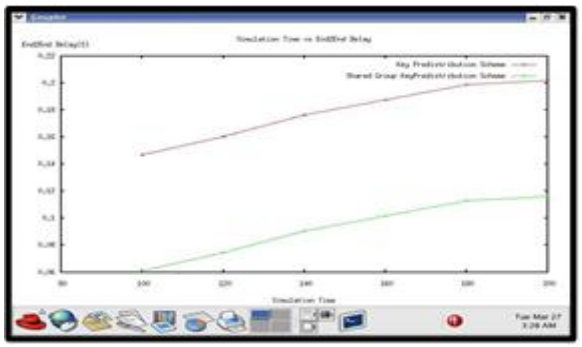

Figure4 Simulation Time vs End to End Delay

C. Simulation Time Vs. Average Remaining Energy

The comparison between simulation time and the average remaining energy is done for these schemes. As the number of keys is reduced in the shared key distribution scheme, the average remaining energy is increased in this scheme. Comparatively, the simulation time and the average remaining energy is decreased, as the number of keys used in this scheme is larger than the shared key / pairwise key generation.

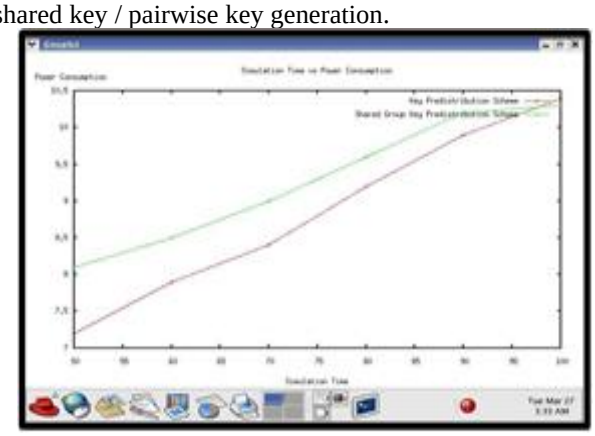

Figure5. Simulation Time vs Average Energy

D. Simulation Time vs Power Consumption

The comparison between simulation time and power consumption is done for both the schemes. The power consumption is linearly increased in the shared-key distribution scheme compared to the distribution scheme. As the key generation process is decreased, where less number of keys are provided. Hence the power consumption for the shared key distribution scheme is very less compared to the distribution scheme.

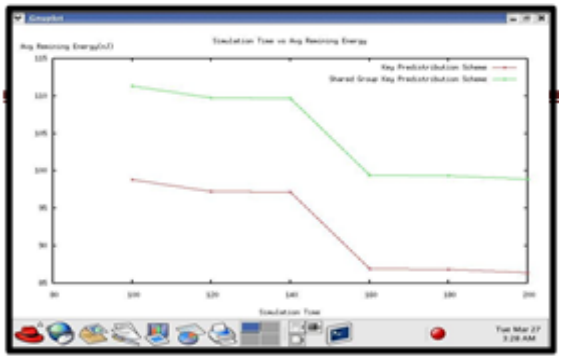

Figure6. Simulation Time vs Power Consumption

VI. CONCLUSION

Robust security mechanisms are vital to the wide acceptance and use of sensor networks for several applications. Security in WSN is quite different from traditional (wired) network security such as the Diffie-Hellman or RSA, which are inappropriate for wireless sensor networks due to the limited computation and energy resource of sensor nodes. Various peculiarities of WSN make the development of a good key scheme for a challenging task. In order to solve the problem, the key distribution scheme using the trusted server was proposed based on a Reputation Trust based key Distribution Scheme that saves the key information along with low power consumption before installing the sensor node was proposed, which is known to be very useful and guaranteeing that any number of nodes can find a common secret key between themselves by using the keys assigned by key pre-distribution schemes and shred group key pre-distribution scheme. In our future work, we will analyze the optimal resources toward the maximal rewards along with power consumption with raise insecurity.

ACKNOWLEDGEMENTS

The authors are thankful for m. A. Goyal, D. Liu, and H. Chan for providing the necessary facilities for preparing the paper. Also, thanks to the IJRES Journal staff to publish this paper.

REFERENCES

[1] A.Goyal, N.Kaur, Padmavati, Kuldeep, and R. Garimella, "*Distributed energy-efficient key distribution for dense wireless sensor networks*," in Proceedings ofthe1stInternational Conference Computational Intelligence, Communication Systems and Networks (CICSYN'09), pp.143–148, July 2009.

[2] K.T.Kim, B.J.Lee, J.H.Choi, B.Y. Jung, and H.Y.Youn, "*An energy-efficient routing protocol in wireless sensor networks*," in Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE' 09), pp. 132–139, August 2009.

[3] J. Yick, B. Mukherjee, D. Ghosal, "*Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm*," Proceedings of the IEEE Second International Conference on Broadband Networks(BROADNETS),2005.

[4] D. Liu and P.Ning, "*Establishing pairwise keys in distributed sensor networks*," in Proceedings of ACM CCS, Washington D.C., WA, 2003.

[5] J.Yick, B.Mukherjee and D.Ghosal, "*Wireless sensor network survey*," Computer Networks, vol.52, no. 12, pp.2292–2330,2008.

[6] H. Chan, A. Perrig, and D. Song, "*Random key pre-distribution schemes for sensor networks*," in Proceedings of the IEEE Symposium on Security and Privacy,2003.

[7] S.Ganeriwal, D. Ganesan, H. Shim, V. Tsiatsis, B.Srivastava, "*Estimating clock uncertainty for efficient duty-cycling in sensor networks*", in Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys),2005.

[8] A. PeringH. Chan and D. Song, "*Random key pre-distribution schemes for sensor networks*," in Proceedings of IEEE Security and Privacy Symposium, Oakland, CA, 2003.

[9] L. Eschenauer and V. Gligor, "*Akey- management scheme for distributed sensor networks*," in The 9th ACM Conference on Computer and communications security, pp. 41-47, Washington D.C., 2002. Eduru Hariprasad, J.S.V.R.S.Sastry,

[10] N. Subhash Chandra, (2014). "*Vastly Efficient Key Pre Distribution and Authentication scheme for Wireless Sensor Networks"*. SSRG International Journal of Computer Science and Engineering 1.7, 23-26.

[11] Vishal Garg , Mukul Jhamb. "*A Review of Wireless Sensor Network on Localization Techniques* ". International Journal of Engineering Trends and Technology (IJETT). V4(4):1049-1053 Apr 2013. ISSN:2231-5381.

[12] G.Wener-Allen, K.Lorincz, M.Ruiz, O. Marcillo, J.Johnson, J.Lees, M.Walsh, "*Deploying a wireless sensor network on an active volcano*, *Data-Driven Applications in Sensor Networks(Special Issue)*", IEEE Internet Computing,2006