I. J. Computer Network and Information Security, **2013, 1, 56-64**
Published Online January 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.01.07

An Efficient Novel Key Management Scheme for Enhancing User Authentication in A WSN

Harjot Bawa
Research Scholar, Department of IT CEC, Landran
harjotbawa@ymail.com

Parminder Singh
Assistant Professor, Department of IT CEC, Landran
singh.parminder06@gmail.com

Rakesh Kumar
Associate Professor, Department of CSE Sachdeva Engg. college for Girls, Kharar
rakesh77kumar@yahoo.com

Abstract—The Wireless Sensor Networks are energy constrained and are normally low cost and low power devices. These nodes are deployed over a specific area for specific goals. Due to energy and memory constraints, secure communication among these sensors is challenging management issue. In order to ensure security, proper connectivity among nodes and resilience against node capture, we propose a scheme called as Random Pre-Key distribution scheme which takes advantage of the binomial key pattern while creating and distributing keys. The value of keys would develop the number of patterns, which is given by the binomial distribution, which would be helpful in maintaining a key pool which is all though random in nature and following a pattern leads to more probability of network connection links. This paper provides a secured communication in WSNs environment and pairing user authentication has been proposed. We employ the idea of dividing the sensor network field into scattered nodes. Inside the scenario, one of the sensor nodes is selected as a server sensor node which is responsible for delivering the key. The novelty of the proposed scenario lies behind the idea of incorporating the sensor nodes along with the proper user authentications. We calculate the throughput involving a periodic traffic and obtained results from the xgraph utility with the use of Network Simulator. The results of this key scheme are obtained and show that improvement in terms of connectivity.

Index Terms—Wireless Sensor Networks, Key Management Schemes, Random Pre-Key distribution

I. INTRODUCTION

A wireless sensor network is a network which consists of a number of sensor nodes that are wirelessly connected to each other. This low-cost, low-power, multifunctional sensor nodes can communicate in short distances. Each sensor node consists of sensing, data processing, and communication components. A large number of these sensor nodes collaborate to form wireless sensor network [1]. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing**.** To ensure scalability and to increase the efficiency of the network operation, sensor nodes are often grouped into clusters [2, 3]**.** A sensor node is battery powered and is equipped with integrated sensors, data processing capabilities, and short-range radio communications [4].

1.1 Sensor Nodes

Wireless sensor networks (WSNs) consist of a large number of tiny, cheap, computational, and energy-constrained sensor nodes that are deployed in network service area. Due to wireless nature, it is easy to add more sensor nodes or move deployed nodes for better coverage and reach.

In a Wireless Sensor Network, the sensors perform two main functions: sensing and relaying data. The sensing component is responsible for probing their environment to track a stimuli or target. The collected data are then relayed to the gateway(s). Nodes that are more than one hop away from the gateway send their data through relaying nodes.[6] The following figure describes the architecture of a sensor node.

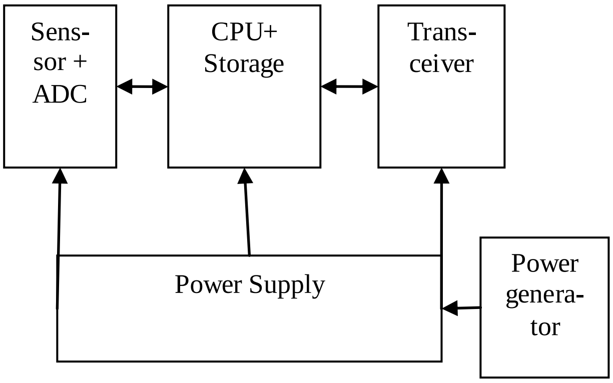

Fig 1.The architecture of a sensor node

A typical sensor node consists of 4 main parts.

- Sensing unit -sensor and analog to digital converter (ADC)
- Processing unit -Processor and storage memory
- Power unit
- Transceiver

1. Sensing unit- The sensing unit collects the data (analog signal) and its analog to digital converter (ADC) converts the data to digital then sends it to the processing unit.

2. Processing unit- The processing unit manages the task list and procedures to collaborate with other sensor nodes. The processor can perform simple operations on the received digital signal, and can store it into its memory

3. Power unit- The power unit manages and sometimes generates the power using solar cells if available. The power supply is to power the node. The sensor circuitry can transform physical quantities into a electric signal responses.

4. Transceiver- The transceiver unit sends and receives the data to neighboring sensors [5, 6].

1.2 Major Differences Between Sensor Networks and Ad-Hoc Networks

- The sensor nodes in a sensor network are deployed densely as compared to the nodes in an ad hoc network.
- Sensor nodes are limited in power, consumption, computational capacities and memory [1, 7].
- The topology of a sensor network may change more frequently in comparison with topology in ad hoc networks.
- The sensor nodes are more prone to failures as compared to ad hoc network nodes.
- Broadcast communication is used in sensor networks due to random deployment and lack of location information.
- Sensor networks focus on interaction with environment rather than focus on interaction with human whereas ad-hoc network nodes are always in touch by human beings (e.g. laptop computers, PDAs, mobile radio terminals etc).
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors [1].
- Ad-hoc networks are used for data and information exchange whereas sensor network nodes are usually embedded in the environment to sense some phenomenon and possibly actuate upon it.

II. KEY MANAGEMENT IN WSN

Key is the most important component for most of the Cryptographic algorithms. Keys are generally the numbers that are randomly selected from a large set of numbers. Management of these keys are very important in cryptography. Management of keys includes the following:

1. Key Generation: It is the process in which a pool of keys is generated. It can be done in offline or online mode by a trusted authority or automated algorithm.

2. Key Establishment: It is the most important phase of key management process. Key establishment is the process by which right keys for right users (sensors) can be determined and key rings for each user are sent to them accordingly.

Key establishment can be done in many ways. Trusted Authority can help in sending the keys to each user through a secure channel. But this mechanism is a costly one and does not suit for sensor networks. So, in sensor networks Key Pre-distribution is used in which key rings are installed in the nodes before deployment of network in offline mode [9].

2.1 Three Phases of Key Establishment

1. Key pre-distribution: Pre-loading keys in sensor nodes prior to deployment. The keys present in a sensor node constitute the key ring of the sensor.

2. Shared key discovery: To find a common shared key between two communicating nodes.

3. Path key establishment: If a common key does not exists, then a path has to be found between the communicating nodes. A path key is then established between the communicating nodes.

2.2 Random Pre-Key Distribution

In Key Pre-Distribution scheme, secret keys are placed in sensor nodes before deployment. When the nodes are deployed over the target area, the secret keys are used to create the network.

2.2.1 Key pre-distribution

The important key pre-distribution schemes which are highly used can be classified as follows:

- Probabilistic key pre-distribution scheme.
- Polynomial-based key pre-distribution schemes [10].
- Blom’s matrix-based key pre- distribution schemes.
- Deterministic key pre-distribution schemes.

During the phases of Key Pre-distribution, 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 [10].

III. KEY MANAGEMENT SCHEMES

3.1 Eschenauer and Gligor’s Method [9]

Eschenauer and Gligor’s method is the first key distribution scheme especially designed for sensor networks. It also constitutes the foundation of the subsequent key distribution schemes in sensor networks Before sensor deployment, a key pool P of p distinct keys with key identifier is randomly generated. For each sensor node si, a subset Ri of r keys with their key identifiers is randomly chosen from P. After sensor deployment, two sensor nodes with (at least) one common key in their key rings can use this common key as the shared key. This procedure of discovering the common key in two key rings is often called shared key discovery.

After the shared key discovery, if two sensor nodes do not have the common key in their respective key rings, they resort to a procedure called path key establishment. The goal of path key establishment is to find a sequence of secure links, which is defined as the communication links whose two ends have found their shared key in shared key discovery. Once path key establishment is successfully finished, that is, a sequence of secure links has been achieved between two sensor nodes that cannot find their shared key in shared key discovery; these two sensor nodes can establish their shared key by, for example, sending the shared key from one end to the other end. During the transmission, as each link is the secure link, the confidentiality of shared key between two ends can be guaranteed [11].

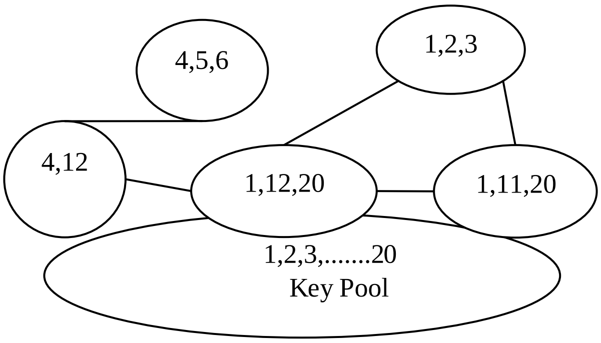

Fig 2 Example of Eschenauer and Gligor's method [11]

3.2 Q-Composite Key Pre-Distribution Scheme [12]

Q-Composite scheme can be thought of as a natural extension of Eschenauer and Gligor's method. Its security enhancement is mainly due to the use of multiple keys, instead of single key in Eschenauer and Gligor's method. After sensor deployment, the shared key discovery and the path key establishment are also the same as those in Eschenauer and Gligor's method. The only difference is that, in q-composite scheme, q common keys in the key rings, instead of a single common key, should be found to construct the shared key.

For both the EG and the q-composite schemes, if a small number of sensors are compromised, they may reveal to a large fraction of pair wise keys shared between non-compromised sensors [14].

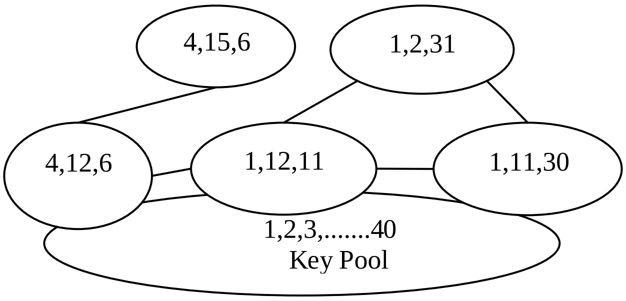

Fig 3. An example of q-composite key pre-distribution scheme

3.3 Method by Blundo et al. [11]

Assume that the authority randomly selects a bivariate t-degree symmetric polynomial. The symmetric polynomial possesses a property of f(x, y) = f(y, x). For sensor node si, a polynomial share f (i, y), which is a univariate t-degree polynomial, is calculated. Then, f(i, y) is stored in sensor node si. After sensor deployment, the key can be obtained by sensor node si by calculating f (i, j) as long as sensor node si would like to have a shared key with sensor node sj. For sensor node sj, similar procedures can be conducted by sensor node sj; that is, f (j, i) is computed. Because of the property of f(x, y) = f(y, x) in the underlying symmetric polynomial, their calculated keys should be the same and can be the shared key.

3.4 Random Perturbation-Based Key Establishment Scheme [13]

The method by Blundo et al. can guarantee perfect connectivity. However, its resilience against sensor compromises is not considered to be acceptable because once a fixed number of sensor nodes have been compromised, the security of the entire sensor network will suddenly crash. To address this issue while preserving perfect connectivity, a random perturbation-based key distribution scheme is proposed. In essence, certain random perturbations are introduced into the method by Blundo et al. Because of the added random perturbation, the original shared key is gone. However, some portions of destroyed keys can be extracted by the sensor nodes and can be used as the shared key. Before sensor deployment, a bivariate t-degree symmetric polynomial is randomly generated as in the method by Blundo et al. Unlike the method by Blundo et al., the perturbation polynomials for each sensor node are further generated. The generation of perturbation polynomial is not totally random, and has to follow the rule that adding the perturbation into the univariate polynomial generated from the bivariate t-degree symmetric polynomial will not lead to the fluctuation of coefficients. In particular, assume that a bivariate t-degree symmetric polynomial f(x, y) is chosen, and the perturbation polynomial φi(y) is chosen for sensor node si. Then, instead of f(i, y), f(i, y) +φ(y) is stored in sensor node si.

IV. RELATED WORKS

The proposals common goal is to provide certain end-to-end performance guarantee. This requires the Model used in this paper to utilize the available paths in order to select the route that matches key. it is very important also to detect, avoid and handle network congestion. Several research papers are written on this topic. A few papers are enumerated below.

In [14], a trade-off between communication overhead] computational overhead , network connectivity and resilience against node capture attack have been discussed.

The Authors tried to overcome the limitations of public key cryptography techniques which are having high computational overhead and unsuitable for WSN. This paper has also discussed about pre-key distribution schemes and its limitations. The author also discussed the polynomial based pre-distribution schemes in which it finally concludes that it is non-viable for WSN due to large memory requirement. Their proposed scheme is location adaptive key establishment scheme which has been analyzed with respect to network connectivity in terms of its probability. They have taken a very large network of 10,000 nodes and large key pool and have also introduced the concept of key ring of size 100.The communication range (ρ) of a sensor is 30 meters and they have deployed in an area w.r.t to the formula.

$$n=A^*(d+1)/\pi\rho \quad (30)$$

Here, d-average number of sensors for each node
ρ=communication range

This scheme is actually an alternative to path key establishment phase of boot-strapping protocol.

Research gap- This scheme is although good and showing good results as per as network connectivity is concerned in large WSN. But this scheme is also creating random numbers which are symmetric in nature in which there is some typical calculation to be done between two nodes establishing keys. The protocol of the key looks like zero proof algorithm in which large number of round trip is required between the nodes to remain secure.

This paper [15] discussed the need for developing key management schemes that would require less memory per storage of keys as well as exchange of keys for authentication. They called this scheme as ARP in which one way hash function scheme is extended and developed into a better resilient ARP (Adaptive Random Pre-distribution) scheme. The author has also conducted a survey of key management schemes which are contemporary to their work which includes PSK pre-distribution, SPIN, multilevel chain schemes, etc.

Then they have discussed the working of ARP scheme in which they give method related key pool generation and key selection algorithm. They are also discussing the usage of random graph theory for developing key decision algorithm and they further also elaborate how mutual authentication occurs between two nodes to get response in terms of connectivity. After giving the detail about scheme they have given criteria on how they are establishing the evaluation strategy for understanding the resilience of ARP scheme. The most important criteria for evaluation as per the paper are probability against number of keys required, thereby reducing the probability of connectivity.

Research gap- This paper basically attempts to get a tradeoff between two schemes namely adaptive random pre-distribution and uniquely assigned one way hash function. They have discussed the memory requirement w.r.t to the minimum network size that it can support. However, they have not been able to establish confidence in terms of how much is the packet delivery ratio.

Exhaustive survey[11] of state of art techniques for doing key distribution in WSN .They have also further classified the various key management schemes into location independent schemes and location dependent key management schemes. In the initial introductory paragraphs they are discussing the importance of confidentiality, authenticity of the network and various possible attacks like wormhole, sibble attack.

Then they are giving the various characteristics of sensors as a device in terms of its cost, battery, power requirement, memory requirement and limited computational power. For conducting the survey for each scheme, they have also suggested for some evaluation metrics which include resilience against adversaries and resource efficiency with connectivity and adaptability. They have listed about 26 types of various key location independent schemes in table1 and have discussed their various characteristics in terms of storage overhead, computational overhead and communication overhead .They have also discussed 7 location dependent key schemes in which they are giving their description and their various characteristics with some special assumptions. This paper is good enough to get overview of various schemes and it helps us to understand the various overheads involved in key management designs.

A scenario [16] used and mentioned the various types of key management schemes which include network level /Wide- shared key scheme in which a symmetric key is used by every node to secure communication and links. It has also been that this scheme is not resilient as compared to another scheme i.e. Master key and link key. In the Master key scheme there is a node which maintains a Pre-configure master key and every other node fetch a set of link keys corresponding to its communication link with others.

As per this paper, they claim that this a bit more secure than the network level key scheme as no node will be able to communicate if master key is not available or erased.

The access control protocol [17] called Elliptic curve cryptography based new framework and protocol have been discussed. They claim that this proposed variants of ECC protocol provides a defense mechanism against most well organized attacks on WSN's. They claim that protocol is more efficient than the conventional ECC as well as those based on RSA. In their protocol, the control occurs only by identifying the identity of each node by differentiating old and new nodes. In addition to this each new node, as per this protocol can establish a shared key with its neighborhoods during the authentication procedure.

They have discussed and demonstrated a scenario in which the access control mechanism is attacked and compromised and adversaries manipulate the old nodes and introduce new malicious nodes which are taken care of by this proposed ECC method. Here the Key management scheme is defensive in nature and tries to build the scheme in such a manner the way packet leech mechanism works.

In this paper they have not proposed a key management system whose goal is to be memory efficient and remain resilient enough even after scalability or after the introduction of adversaries. The entire mechanism discussed here is to defend against particular attack.

V. Motivation

In a Wireless Sensor Network, individual sensor nodes are constrained in energy, computing, and communication capabilities. Typically, sensors are mass-produced anonymous commodity devices that are initially unaware of their location. Once deployed, sensors should self-organize into a network that works unattended .Due to the fact that individual sensor nodes are anonymous and that communication among sensors is via wireless links, sensor networks are highly vulnerable to security attacks that leads to usage of more memory and overhead in the gateways and nodes and basic mechanism used to secure them is by using some Key management scheme.
A key management scheme called as Random Pre-Key Distribution scheme is used for distributing keys randomly to the various sensors deployed over a network. When these sensor nodes want to communicate with each other, there’s an authentication process which is followed. In this authentication process, a key match is done. If there's a key match between the sensor nodes, they are allowed to communicate. If the keys allocated to the sensor nodes during the pre-key distribution process do not match, then the sensor nodes cannot communicate with each other.

5.1 Proposed Work

The flow chart in the above Figure depicts the various steps which are carried out during the Pre-key distribution process. The simulation is carried out using the Network simulator (version 2.35), which simulates the events such as sending, receiving, dropping, forwarding, etc. The wireless channel is used as the sensor nodes deployed communicate wirelessly with each other. The propagation models are used to compute the received power. When a packet is received, the propagation model determines the attenuation between transmitter and receiver and computes the received signal strength. The two-Ray ground Radio propagation model is used. An omni-directional antenna is employed for carrying out the transmissions which can transmit signal over a 360 degree angle. Omni-directional wireless sensor networks are modeled such that a bidirectional link is established between neighboring sensor nodes if they are within communication radius [8].

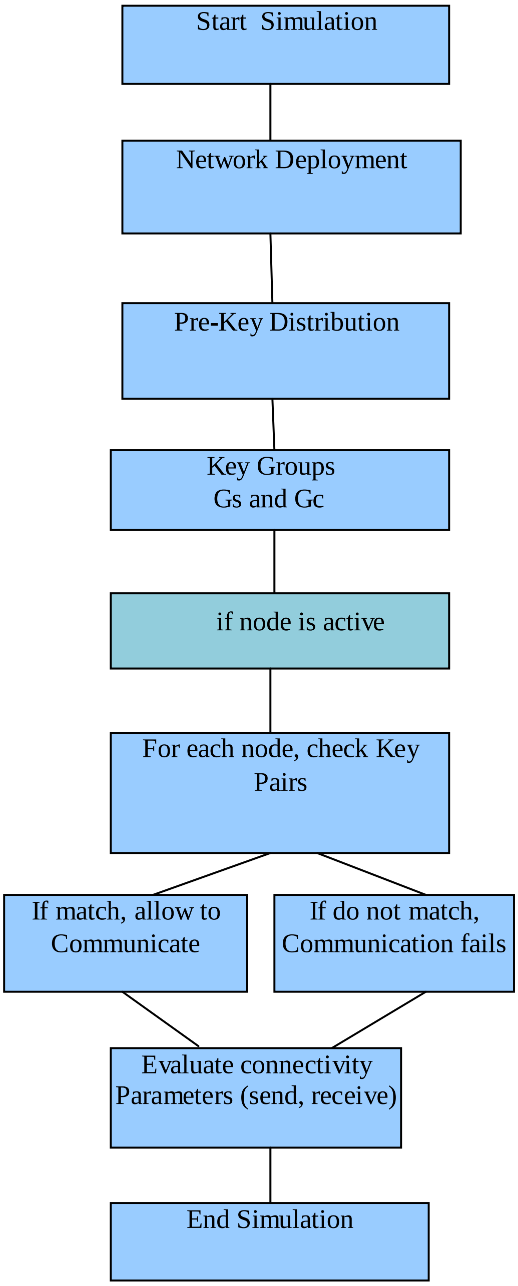
Start Simulation
Network Deployment
Pre-Key Distribution
Key Groups
Gs and Gc
if node is active
For each node, check Key Pairs
If match, allow to Communicate
If do not match, Communication fails
Evaluate connectivity Parameters (send, receive)
End Simulation

Fig 4. Flow Diagram

The scenario is simulated for 150 seconds. The participating nodes are mobile. The routing protocol which monitors and carries out the transmission is Ad-hoc On Demand Distance Vector routing Protocol (AODV).The following table gives an overview of all the simulation parameters used.

Table 1.Simulation Parameters

Parameter	Value
Simulator	NS-2.35
Channel Type	Wireless Channel
Mobility model	Two-Ray ground Radio Propagation Model
Network Interface Type	Wireless Phy/IEEE 802.15.4
Antenna Model	Omni-directional
Number of mobile-nodes	50
Routing Protocol	AODV
Simulation Time	150 sec
Simulation area (m*m)	1000 *1000
Packet Size	1024 bits

5.1.1 Pre-Key distribution:

In pre-shared key scheme, the manufacturer of the sensors normally gives predefined keys to each sensor. This group of keys is denoted by G. This group has a concept of having keys for client and server. So therefore, for a successful communication among these, there has to be a pre-shared key between client and server. In this each client must also store the key from the server, so in case of scalability we need to be very careful to buy only those sensors which have pre-configured keys and which have a common key with the server and belongs to a particular G-group.

Typically when these pre-configured keys are distributed among sensors, they are created on the basis of pseudo random algorithm in which no case is taken whether these keys will finally have a certain level of connectivity in a sense that they will be helpful in securing a network but at the same time having large number of key sets which are an intersection of the key group pairs. So therefore it reaches a point sometimes that inspite of the fact these sensors are in a comfort zone to communicate with each other**.**

5.1.2 Mathematical Model of Pre-Shared Key

1.let S be the number of sensors to be deployed in the network.

2. Let S_{sn} be the number of servers which are to be deployed as sensors.

3. Let S_{Cn} be the number of sensors which are to be deployed as clients in a network.

4. Let G be the group of keys allotted to a network.

5. Let the group be bifurcated into G_c and G_s representing keys that belong to server nodes and client nodes.

6. Since the number of servers will be less and number of clients will be more, the groups need to be allotted accordingly.

5.1.3 Disjoint sets

Two sets are said to be disjoint if both the sets have nothing common among them.

Let there be two sets of keys Gs and Gc. The set of Gs and Gc is said to be disjoint , if the keys in these two sets do not match at all.

If, $Gs= \{PSK_{sk1}, PSK_{sk2}, ...PSK_{skn}\}$

$Gc=\{PSK_{ck1}, PSK_{ck2}, ...PSK_{skn}\}$

Then, Probability (Gs η Gc) =φ or

Probability <0.2

The intersection of these two key sets is a null value or it's a very small value. Thus in case of disjoint sets the connectivity represented by the number of packets received at the other end is less.

5.1.3 Simulation Model

We have developed a network model that is dedicated to evaluate the performance of the WSN. There is a set of client sensors and server sensors. The client and server sensors are organized into clusters as shown in the figure 5. These server sensors and client sensors are communicating with each other on the basis of key match between them. If the key match occurs between the server and the client sensor, then the communication takes place otherwise there's an authentication failure.

In a Pre-Shared scheme, as there are sets of server and client sensors. Each server sensor stores the key information of each client sensor and each client sensor stores the information of the each server sensor. Each sensor has maintained a key pool with it. When a node wants to communicate with another node, it checks for the availability of the keys in its key pool. If there's a match of keys, the communication occurs otherwise it fails.

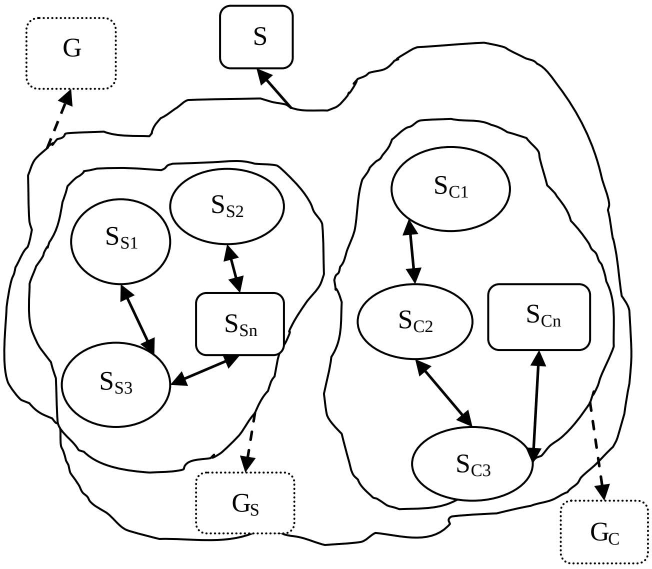

Fig.5 Wireless Sensor Network

If there exist a network with 1000 server sensors and 1000 client sensors, then the communication overhead of each node would increase to a greater extent. As each client sensor needs to store the information of the rest 999 server sensors in the network and each server sensor needs to store the information of the remaining 999 client sensors. Also the Wireless Sensor Network is an ad-hoc network, which further leads to an increase in the overhead of the individual nodes in the network and thus reduces the performance of the network.

As the sensors are memory constrained devices which means that they would become dead at regular intervals of time. This leads to an authentication failure. Under this scheme only 10% of the communication takes place and rest is the failures.

VI. SIMULATION RESULTS

The following are the graphs obtained after allocating keys to the sensor nodes.

6.1 Throughput of Sending Packets

To calculate the Throughput of packets from figure 6 states that the length of time between two neighboring packet transmissions of the tagged node. These transmissions include both successes and collisions. The figure 6 shows that there is a steady increase of request sent to the other nodes starting from default source to the destination. It can be seen from the graph that with the passage of time, the rate of increase is exponential in nature .Since more and more nodes start communicating and sending request to each other .It's at this stage of sending HELLO message, which confirms that request has been sent to the nodes and they want to communicate with each other.

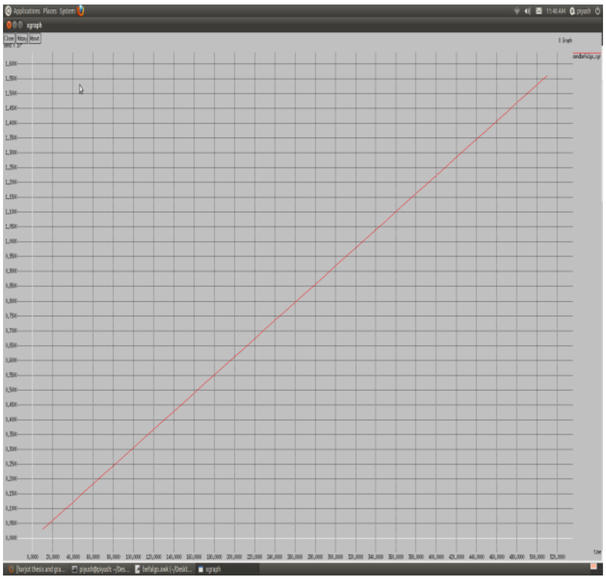

Fig 6. Number of packets sent versus time

6.2 Throughput of Receiving Packets

It's apparent from the graph that as the packets are sent, they are received but there is a sudden drop as the simulation proceeds. This means that at this stage the Key Pre-Distribution scheme works. But due to some resilience, there is a sudden drop of packets in the network. In other there is an implementation of disjoint sets. This is attributed to the fact that inspite of nodes being in the same range and having minimum cost of route as well as have established message routing protocol cycle complete, it suddenly shows drop in receiving data .As the key pairs seem to be not matching with each other and therefore they do not receive data and there's a dip. Although with the passage of time there's always an increase in peaks and valleys. In the graph the packets received are shown by the graphs and the packets dropped are shown by the valleys.

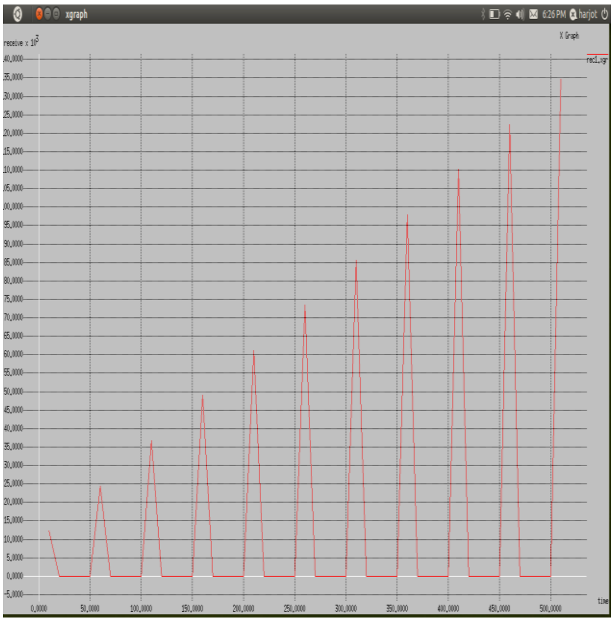

Fig 7. Number of packets received versus time

The graph illustrates that it has high computational overhead which is not too much suitable for WSN due to effect of resilience and require more memory for storage of keys as well as exchange of keys for authentication

6.3 Drop Packets

This drop analysis depends on the send and receive graphs. Mathematically, drop is the difference between packets which are sent and received during a time span. As seen from the graph that with the passage of time if the packets are being received normally then there's a steady increase in the straight line but the packets are dropped, it shows a dip in the graph.

The drop here (PSK) is due to large number of pre-configured keys which are random in nature and may not lead to a common set of key pairs which would have ensured the connectivity. It is apparent from the graph when the communication starts, as the keys are exchanged when two nodes as per the protocol can communicate are unable to communicate as per their keys are disjoint in nature. So, more and more communication occurs, after some steady increase there is a dip.

The graph also explains that the packet delivery ratio has not proper connectivity with respect to scheme known as PSK. The probability against number of keys required is not proper which reduces the probability of connectivity.

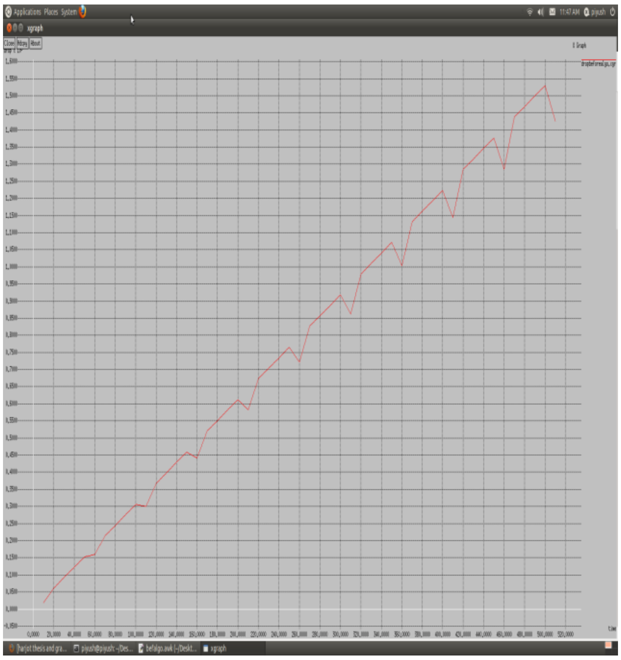

Fig 8. Number of packets dropped versus time

VII. CONCLUSION AND FUTURE WORK

We build the user authentication scheme for security purpose and to improve End to End (E2E) communication that meet efficiency and reliability. We showed superiority of the proposed model to enhance the performance with reduced congestion over the network. When connectivity of a network is affected due to particular key scheme, it also affects many other parameters including energy as well as memory consumed by the sensors which is a very critical parameter in area of sensors. Therefore there is urgent need for more research that should be done not just in terms of packet delivery ratio but also on parameters like energy and memory. We have already covered the energy parameters namely send, receive and drop of packets and we can conclude from the result graphs that there is improved performance in terms of receiving packets which completes the cycle of network connectivity communication, thereby also reducing the number of packet drops.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,(2002) "Wireless sensor networks: a survey," in Computer Networks. vol. 38, pp. 393-422.

[2] http://www.worldscibooks.com/compsci/6288.html, *"Information Processing and routing in Wireless Sensor Networks "*© World Scientific Publishing Co. Pte. Ltd.

[3] Muhammad,S., et.al." A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks", Department of Computer Engineering Kyung Hee University (Global Campus), Korea.

[4] Wenliang Du,et.al "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge.". Department of Electrical Engineering and Computer Science Syracuse University, Syracuse, NY 13244-1240, USA Email: {wedu, jdeng01, varshney}@ecs.syr.edu

[5] Mokhtar Aboelaze, Fadi Aloul,(2005) "Current and Future Trends in Sensor Networks: A Survey", IEEE.

[6] Mohamed F. Younis, Senior Member, IEEE, Kajaldeep Ghumman, and Mohamed Eltoweissy, Senior Member, IEEE. "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks" .

[7] [10] Dressler, F.(2008)"A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks. Elsevier Computer Communications", vol. 31 (13), pp. 3018-3029.

[8] Ji Heon Kwon, "Improved Connectivity Using Hybrid Uni/Omni-directional Antennas In Sensor Networks", Department of Electrical and Computer Engineering Texas A&M University.

[9] Laurent Eschenauer and Virgil D. Gligor.(2002)A key-management scheme for distributed sensor networks. In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 41- 47, New York.

[10] Noor J. Ottallah (2008) "Implementation of Secure Key Management Techniques in Wireless Sensor Networks" , B.S University of New Orleans.

[11] Chi‐Yuan Chen, et.al.,(2011) "A survey of key distribution in wireless sensor networks", Security Comm. Networks Published online in Wiley Online Library.

[12] Chan H, Perrig A, Song D.(2003) "Random key pre-distribution schemes for sensor networks". In Proceedings of IEEE Symposium on Security and Privacy (S&P).

[13] Zhang W, Tran M, Zhu S, Cao G.(2007) A random perturbation‐based scheme for pair-wise key establishment in sensor networks. In Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), September 9–14, Montreal, QC, Canada.

[14] Ashok Kumar Das,(2009) " A Location-Adaptive Key Establishment Scheme for Large-Scale Distributed Wireless Sensor Networks", Journal Of Computers, Vol. 4, No. 9,.

[15] Shih-I Huang ,et.al, Department of Computer Science and Information Engineering National Chiao Tung University "Adaptive Random Key Distribution Scheme For Wireless Sensor Network".

[16] Mohit Saxena (2007), "Security In Wireless Sensor Networks -A Layer Based classification", Purdue University, West Lafayette, IN 47907-208

[17] Yun Zhou et.al (2006)." Access control in wireless sensor networks ",Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, United States Available online 5 July 2006.

Harjot Bawa, born on 1989, is pursuing her M.Tech in Information Technology from Punjab Technical University, Jalandhar. She has completed her B.Tech in Information Technology from Punjab Technical University. She has published a research paper on Wireless Mesh Networks in International Conference on Advancement in Computing and Communication (ICACC) in Feb 2012.

Parminder Singh has Six years and 3 Months of experience in academics. He has done his M.Tech in Computer Science and Engineering from Punjab Technical University, Jalandhar and is pursuing Ph.D. He is currently working as an Assistant Professor of Information Technology in CEC Landran. He has more than 45 publications in archival journals, International and National conferences. He currently serves on the Reviewer of many reputed Journals. His research interests are TCP performance and QOS issues in wireless and Sensor networks.

Rakesh Kumar has eleven years experience in academics. He completed his Master Computer Application and MTech (CSE). He is also pursuing Ph.D in computer Science. He is currently the Dean and Head of Department in computer Science & Engineering in Sachdeva Engineering College for Girls, Gharuan, Distt. Mohali. He has published number of papers in International and National journals. He has also published two books i.e. How to Program in c++ and Network Security. He is guiding some of the students in the field of Natural Language Processing.