International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21715

Efficient Resource Allocation in Hybrid Wireless Networks Increase the Capacity

B. Senbagappriya*, Dr. S. S. Dhenakaran
Department of Computer Science, Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

Article Info
Volume 7, Issue 1
Page Number: 41-48
Publication Issue :
January-February-2021

Article History
Accepted : 01 Jan 2021
Published : 10 Jan 2021

In many wireless sensor network (WSN) the Mobile sinks(MSs) are very essential applications for efficient data gathering, restricted sensor reprogramming, and for distinguishing and revoking compromised sensors. The sensor network that formulate use of the existing 2-tier security structure, elevate a new protection challenge i.e an attacker can easily create a replicated node and can gain control of the data in the network. This project describes a polynomial pool based approach hybrid three-tier general framework that permits the use of any pairwise key predistribution scheme as its basic component. In this technique we implement a special kind of sensor node, which is called as polynomial pool. This sensor node not the part of actual communication. Polynomial pool checks all key of that intruder node and if key matches it allowed that node into network otherwise throwaway from the network. In this project we implemented a new technique with an algorithm named GNDA Good Node Detection Algorithm Based Approach technique with Wireless Sensor Networks. As we all know that, secured files are easily hacked by attacked by they are using several software. In my project the main aim is to avoid this kind of attackers & also increase the capacity by sending by files. Propose a Hybrid Distributed Three-hop Data Routing protocol (HDTR). HDTR protocol improves the Network efficiency and reduces the Overhead. This will also identify the good neighbor node to transfer the data.

Keywords : Wireless sensor network (WSN) Mobile sinks(MSs) GNDA, HDTR, Routing Algorithm

I. INTRODUCTION

A Hybrid Wireless sensor network (HWSN) consist of spatially distributed independent sensor. These sensor are used to check physical or environmental condition, such as temperature, sound, pressure, etc. The industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring and so on. Compromising security in network is very simple unless we supply strong verification method. The proposal of using single polynomial pool is certainly outdated as it opens windows to many node replication attacks. Single polynomial certification is compromise, we move on to create 2- polynomial pools namely static polynomial pool and mobile polynomial pool.

Electronic technology have paved the way for the development of a new generation of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate wirelessly. The resource constraints of the sensors and their nature of communication over a wireless medium make data confidentially.

The three-tier security scheme was robust against a stationary access node replication attack, as this scheme makes use of a one-way hash chains algorithm along with the static polynomial pool based scheme. Technique polynomial pool-based key pre-distribution scheme both mobile sink and inactive way in point generate the separate subset of keys which result in the high computational cost. Random pair wise pre- distribution scheme only mobile sink generate a key with key identifiers and broadcasted to stationary access point and sensor node.

II. LITERATURE SURVEY

Amar Rasheed et.al [1] group key pre distribution. The pair wise key establishment in the context of sensor network is the final target. This organization is totally secure and t-collusion resistant. The network resilience is considerably improved to the mobile sink duplication attack. The small fraction of preselected sensor nodes is called as sensor node. In this new protection agenda stationary access nodes act as an authentication access point to a network to elicit the sensor node to transmit the collected to the mobile sink.

Chan et al. [2] present unmitigated this proposed two key redistribution schemes: the q-composite key predistribution scheme and the random pairwise key technique In q-composite key pre-distribution scheme two sensor node are essential to compute a pairwise key from the shared q predistributed key. In random pairwise keys scheme pair of sensor node is randomly picked and assign each pair a unique random key.

Liu et al.[3] The sensor nodes are communicated securely with each other using cryptographic techniques by enabling bi variate key polynomial. This is one of the majority primary protection service. The algorithm assures a direct key established between any two neighbour sensors in any deployment group.

I.F. Akyildiz, W. Su, Y. S [4] This paper decrease the communication cost by using group deployment knowledge. Ho *et al.* Also presented a SPRT method for replica detection in mobile sensor networks, in which all sensors are mobile. Pietro, Oligeri *et al.* consider one more type of mobile sensor network in which mobile sink appointment stationary sensors and collect the data once in each round.

T. Gao, D. Greenspan, M. Welesh [5] Suggested an efficient method of membership verification for re-authentication of mobile node and shows the performance analysis of our membership verification. This technique proposed a proficient and scalable re-authentication protocol over wireless sensor network also they provide security.

III. METHODOLOGY

3.1 Computational Intelligence

The expression computational intelligence (CI) usually refers to the ability of a computer to learn a specific task from data or experimental observation. Level even if it is commonly considered a synonym of soft computing, there is still no usually usual definition of computational intelligence. In the main, computational intelligence is a set of nature-inspired computational techniques and approach to address complex real-world problems to which mathematical or traditional modeling can be useless for a few reasons: the processes might be too complex for mathematical reasoning, it might contain some uncertainties during the process, or the process might simply be stochastic in nature. Certainly many real-life problem cannot be translated into binary language (unique values of 0 and 1) for computers to procedure it. It is therefore provides solution for such harms.

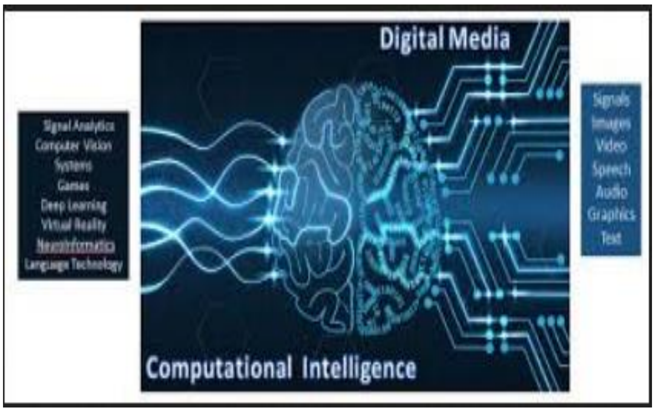


Figure 3.1 Computational Intelligence

3.4 PROPOSED ALGORITHMS

3.4.1 Random pair wise key pre distribution

Two steps are involved in the key discovery phase. In the first step, each sensor attempts to discover shared key(s) with each of its neighbors. To achieve this, the sensor can broadcast its key ring identifier to its neighbours. After the first step of the key discovery phase, the sensor knows all its neighbors. The set of all neighbors of sensor is represented by W_i and $|W_i|=n'$. The set of neighbours of sensor i who share at least one key with the sensor i is represented by R_i. Thus, we have $W_i = Q_i \cup R_i$ and $|Q_i|+| R_i|= n'$.

3.4.2. Pair wise key establishment phase:

If sensor shares at least one key with a given neighbor, the shared key(s) can be used as their pair wise key(s)

3.4.3 ROUTING ALGORITHM

The polynomial pool based approach is divided into two stage. They are (i) Static and mobile polynomial pre-distribution and (ii) Key discovery between mobile node and stationary node. Tame-based key pre-distribution approach, where we exploit tame auto orphisms to get symmetric and two-one bivariate maps for the pairwise key establishment. This tame-based approach can provide deterministic authentication between two parties. The tame transformation ti = (ti,1,…,ti,m) is defined as either a linear transformation or of the following form in any order of variables a1,a2,…,an with polynomials di,j,

$$ti,1\ (a1,\dots,an) = a1+di,1(a2,\dots,an) = b1$$
$$ti,2\ (a1,\dots,an) = a2+di,2(a3,\dots,an) = b2$$
$$ti,j\ (a1,\dots,an) = aj+di,j(aj+1,\dots,an) = bj$$
$$ti,n\ (a1,\dots,an) = an = bn$$

If the tame transformation is invertible then it is called as tame automorphism

Let **G** be a finite field of 2^l elements. Let $\mu^1, \mu^2, \mu^3, \mu^4$ be tame mappings of the $n+r$ dimensional affine space **G**$^{n+r.}$ Let the composition $\mu^1, \mu^2, \mu^3, \mu^4$ be π. The mapping π and the $\mu i's$ will be hidden. Let the component expression of π be

$(\pi 1(a1,\dots,an+r)= \pi n+r(a1,\dots,an+r))$

The field **G** and the polynomial map $(h1,\dots,hn+r)$ will be announced as the public key. Given a plaintext

$(a'1,\dots,a'n) \in$ **G**n

Assume that,

$b'i=hi(a'1,\dots,a'n)$

then the ciphertext will be

$(b'1,\dots,b'n+r) \in$ **G**$n+r$

Given μi and $(b'1,\dots,b'n+r)$, it is easy to find $\mu\text{-}1i(b'1,\dots,b'n+r)$

The private key will be the set of maps { $\mu 1, \mu 2, \mu 3, \mu 4$}. The security of the system rests in part on the difficulty of finding the map π and the factorization of the map π into a product of tame transformations $\mu i's$.

Polynomial bool based Scheme is the main scheme used for finding the polynomial share of each node. Every node is assigned with an id. And the steps of this scheme are given below.

1. Each node has an id rU which is unique and is a member of finite field Zp.

2. Three elements a,b,care chosen from Zp.

3.Polynomial f(x,y) = (a + b(x + y) + cxy) mod p is generated, where p is aprime.

4. For each node, polynomial share gu(x) = (an+ bnx) mod p where an= (a +brU) mod p and bn= (b + crU) mod p is formed and pre-distributed .

5. In order for node U to be able to communicate with node V the following computations have to be performed:

6. Ku,v= Kv,u= f(ru,rv) = (a + b(ru+rv) + crurv)mod p.

7. U computes Ku,v= gu(rv).

8. V computes Kv,u= gv(ru)

9. If Ku,v=Kv,u , then the nodes share the same polynomial and then they can set up communication.

Algorithm Used In Hybrid Distributed Three-hop Data Routing protocol

Step 1:

First the base station os server gets started. Then, the all sensor node and mobiles sinks sub servers are get registered and activated.

Step2:

A predistribution pairwise key is generated and securely distributed between sensor node and mobile sink to check whether sensor node and mobiles sinks are in activation mode or not. The same pairwise key is used for encryption and decryption.

Step 3:

Once the pairwise key distributed then sensor are ready to browse the information from the environmental accepts.

Step 4:

The data of information has to send base station. Before sending the it gets encrypted and authenticated by mobile sinks; if sensor is non-compromised and authorized client then data is retrieved by mobile sinks from sensor.

Step 5:

Polynomial pool based, random pair wise key algorithm is used for encryption and decryption and for authentication 64 bit algorithm is used

Step 6:

Finally, the server retrieves the data and stored in database

3.4.4 JAVA TOOL

Java technology is both a programming language and a platform. The Java Programming Language. The Java programming language is a high-level language that can be characterized by all of the following buzzwords : Simple, Architecture neutral, Object oriented, Portable, Distributed Highperformance, Interpreted, Multithreaded, Robust, Dynamic, Secure With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is strange in that a program is both compiled and interprets. With the compiler, first you translate a program into an intermediate language called *Java byte codes* —the platform-independent codes interpreted by the interpreter on the Java platform. Compilation happens just once; interpretation occurs each time the program is executed.

IV. EXPERIMENTAL RESULT

The proposed system has been implemented using JAVA tool. Proposed a general three-tier security framework for authentication and pair wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key pre-distribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. Propose a Hybrid Distributed Three-hop Data Routing protocol (HDTR). HDTR protocol improves the Network efficiency and reduces the Overhead.

4.1 IMPLEMENTATION MODULE

CLIENT MODEL

A client is an application or system that accesses a remote service on another computer system, known as a server, by way of a network. The Client machine is always used for sending request to the server machine.

SERVER MODEL

A server is any combination of hardware or software designed to provide services to clients. When used unaccompanied, the term typically refer to a computer which may be running a server operating system, but is usually used to refer to any software or dedicated hardware capable of providing services to the requesting client.

SECURITY ANALYSIS METHOD

GNDAs from the mobile GNDA pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single GNDA from the mobile pool to gain access to the network for the sensor's data gathering. GNDAs from the static GNDA pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes. GNDAs from the mobile GNDA pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single GNDA from the mobile pool to gain access to the network for the sensor's data gathering. GNDAs from the static GNDA pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.

Threat Analysis Method

Analyze the security performance of the proposed scheme against a mobile sink replication attack. As stated in the previous section, for an attacker to launch a mobile sink replication attack on the network, the adversary has to compromise at least one GNDA from the mobile GNDA pool. To achieve this, the adversary must capture at least a specific number of stationary access nodes that hold the same mobile GNDA

A Hybrid Distributed Three-hop Routing Protocol

The hybrid three-tier security scheme provides better network resilience against mobile sink replication attack compared to the GNDA approach. This scheme delivers the same security performance as the GNDA when the network is under a stationary access node replication attack. In both scheme, for any sensor node u that wants to validate and establish a pairwise key with a stationary access node A, the two nodes must share at least a common GNDA in their GNDA rings. To perform a stationary access node replication attack on a network, the adversary needs to compromise at least a single GNDA from the static pool. This can be obtain simply by capturing arbitrary sensor nodes in the network. Then, the adversary can make use of this compromised GNDA by a replicated stationary access node to enable insecure access to the network.

4.2 RESULT

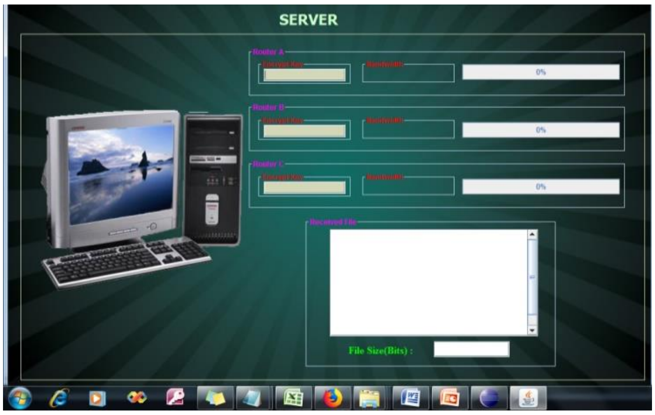
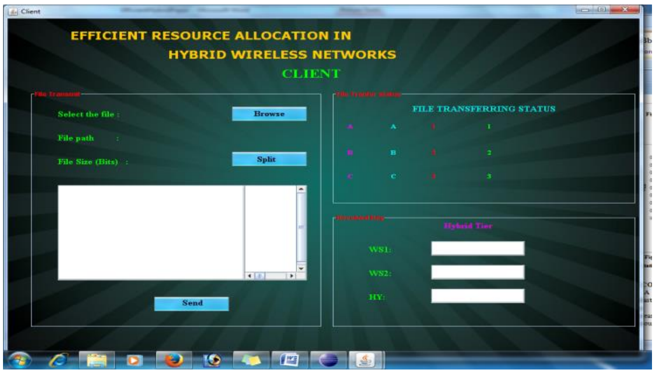


Fig: 4.2.1 Client Module



Select the file :

File path :

File Size (Bits) :

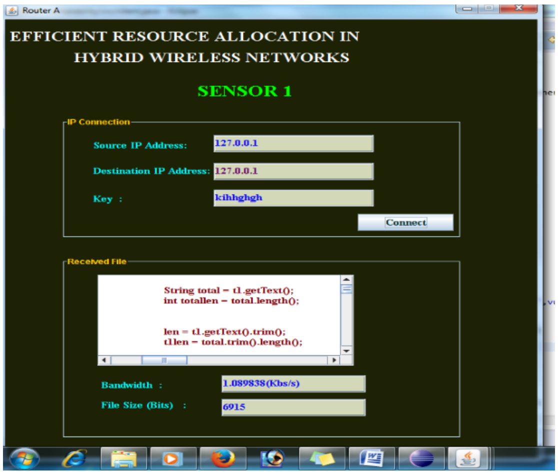
A	A	1	1
B	B	2	2
C	C	3	3

WS1:

WS2:

HY:

Fig : 4.2.2 Server Module



Source IP Address: 127.0.0.1

Destination IP Address: 127.0.0.1

Key : kihhghgh

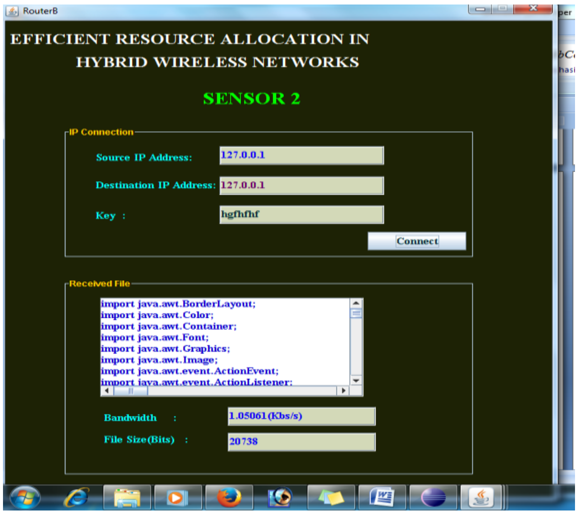
```
String total = t1.getText();
int totallen = total.length();


len = t1.getText().trim();
t1len = total.trim().length();
```

Bandwidth : 1.089838(Kbs/s)

File Size (Bits) : 6915

Fig: 4.2.3 Sensor 1



Source IP Address: 127.0.0.1

Destination IP Address: 127.0.0.1

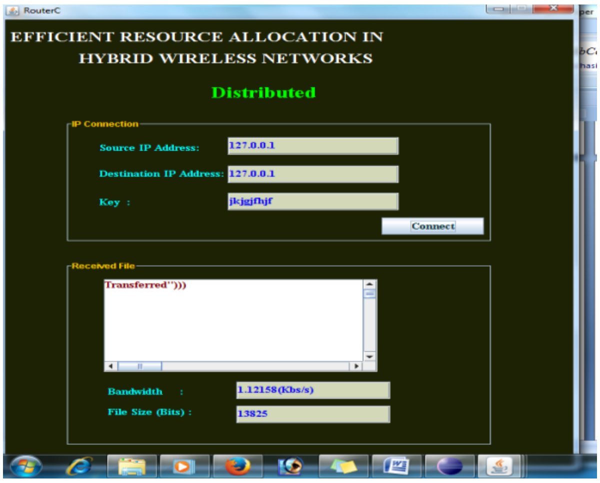
Key : hgfhfhf

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
```

Bandwidth : 1.05061(Kbs/s)

File Size(Bits) : 20738

Fig : 4.2.4 Sensor 2



Source IP Address: 127.0.0.1

Destination IP Address: 127.0.0.1

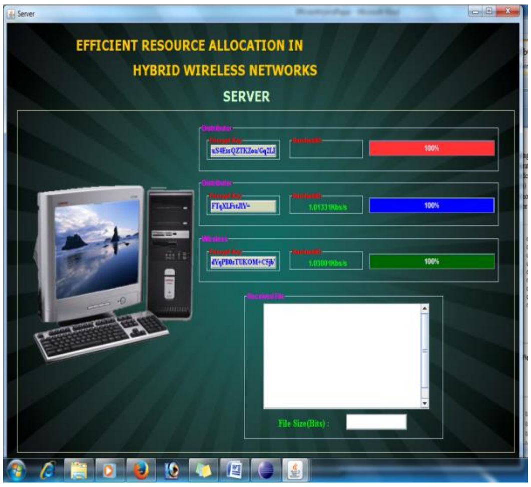
Key : jkjgjfhjf

```
Transferred")))
```

Bandwidth : 1.12158(Kbs/s)

File Size (Bits) : 13825

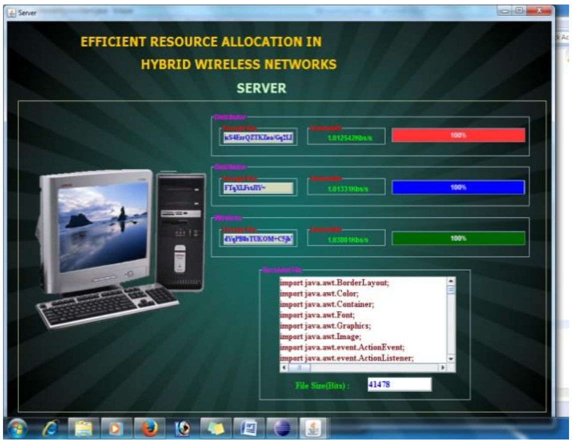
Fig: 4.2.5 Distributed



Encrypt Key	Bandwidth	
uS4EssQZTKZoa/Gq2LI		100%
FTqXLFvtJIY=	1.01331Kbs/s	100%
dYqPB0sTUKOM+C5jb'	1.03001Kbs/s	100%

File Size(Bits) :

Fig : 4.2.6 Server Received



```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
```

File Size(Bits) : 41478

Fig : 4.2.7 Server File Download

4.3 PERFORMANCE EVALUATION

The proposed scheme has been implemented and analyzed in the network simulator JAVA. The possible outcomes when there is a change in the key size is to be determined. The various sets of key size is given and the change of key size broadcasted from mobile sink to stationary access node and stationary access node to sensor node is to be determined. Table 1 shows the calculation of broadcasting the key from the mobile sink to stationary access node and stationary access node to sensor node.

Size of Key Generated in Mobile Sink	Size of Key Broadcasted to Stationary Access Node	Size of Key Generated in Stationary Access Node	Size of Key Broadcasted to Sensor Node
5	4	5	4
10	9	10	9
20	19	20	19
30	29	30	29
40	39	40	39

Table 4.3. Calculation of Broadcasting the Key of Various Size

The key size is larger it should be store in a disk file which can be discover by some one else. Thus large key size is not only convenient to use but also it is a security risk. It significantly take longer time to encrypt and decrypt message and broadcast the generated key. So it is convenient to use the smaller key size. The key size used in this project is 4 (32 bit). The following analysis show that as the size of the polynomial pool increases the probability of sharing the key size also increase. The key is generated in the static polynomial pool and it is broadcasted to the sensor node. Fig 4.3(a) and Fig. 4.3(b) represent the sharing of the key from static polynomial pool to the Stationary access node and sensor node.

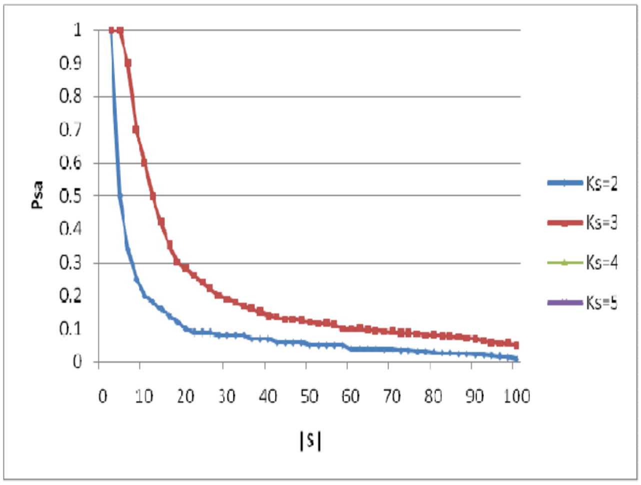


Fig 4.3(a) The probability P_{sx} that a sensor and stationary access node share a static polynomial versus the size|S|

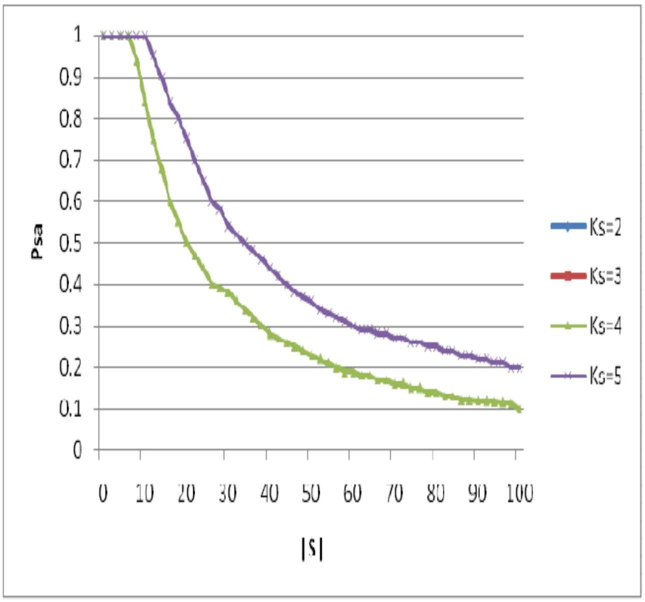


Fig 4.3(b) The probability P_{sx} that a sensor and stationary access node share a static polynomial|S|

V. CONCLUSION

A Resource Allocation network combining an infrastructure wireless network and a mobile ad-hoc network leverages their advantages to increase the throughput capacity of the system. Resource Allocation networks simply combine the routing protocols in the two types of networks for data transmission, which prevents them from achieving higher system capacity. In this propose a Hybrid Distributed Three-hop Routing (DTR) data routing protocol ,Good Node Detection algorithm that integrates the dual features of Resource Allocation networks in the data transmission process In DTR a source node divides a message stream into segments and transmits them to its mobile neighbors, which further forward the segments to their destination through an infrastructure network.

VI. REFERENCES

[1]. A. Rasheed and R. Mahapatra, “An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks,” Proc. Third Int’l Conf. Intelligent Sensors, Sensor Networks and Information Processing,2007.

[2]. H. Chan, A. Perrig, and D. Song, “Random Key Pre-Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.

[3]. D. Liu and P. Ning, “Location-Based Pair wise Key Establishments for Static Sensor Networks,” Proc. First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.

[4]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[5]. T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, “Vital Signs Monitoring and Patient Tracking over a Wireless Network,” Proc. IEEE 27th Ann. Int’l Conf. Eng. Medicine and Biology Soc. (EMBS), Sept. 2005.

[6]. L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002.

[7]. H. Chan, A. Perrig, and D. Song, “Random Key Pre-Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.

[8]. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly-Secure Key Distribution for Dynamic Conferences,” Proc. 12th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’92), pp. 471-486, 1993.

[9]. P. Ning, and R.Li. Establishing, “Pairwise Keys in Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.

[10]. L. Lamport, “Password Authentication with Insecure Communication,” Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.

[11]. A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin, “Intelligent Fluid Infrastructure for Embedded Networks,” Proc. Second ACM Int’l Conf. Mobile Systems, Applications, and Services (MobiSys ’04), June 2004.

Cite this article as :

B. Senbagappriya, Dr. S. S. Dhenakaran, "Efficient Resource Allocation in Hybrid Wireless Networks Increase the Capacity", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 1, pp. 41-48, January-February 2021. Available at doi : https://doi.org/10.32628/CSEIT21715
Journal URL : http://ijsrcseit.com/CSEIT21715