Journal of Theoretical and Applied Information Technology
31st August 2014. Vol. 66 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

N-CRYPT: A HIGHLY SECURED DATA TRANSMISSION FOR WIRELESS SENSOR NETWORK

[1]S.GOPALAKRISHNAN, [2]Dr.P.GANESHKUMAR

[1] Assistant Professor, Department of ECE, PSNA College of Engineering and Technology, Dindigul, India

[2] Professor, Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, India

E-mail: [1]lapog.gopal@gmail.com , [2]drpganeshkumar@gmail.com

ABSTRACT

Mulling over of any system the defenselessness of malevolent movement influences the information straight forwardly or by implication. The principle destination of this paper is to transmit the information in a multi bounce WSN in a secured way. On the off chance that a modest segment of information could be recuperate by a malevolent node then a malignant node can ruin the whole information throughout the information transmission. To conquer this issue and enhancing the information level security in this paper N-Crypt methodology is presented for giving high security to information while information transmission. N-Crypt is a cyclic procedure of Encryption, Decryption on the information from Source Node to Destination Node in the WSN. N-Crypt is having two modules N-Crypt-I for Encryption at every node and N-Crypt-II for Decryption at Destination node where it can maintain a strategic distance from clashes on the procedure of Encryption and Decryption. The Simulation result indicates that the execution of N-Crypt is superior to the current methodologies.

Keywords: *Security in Wireless Networks; Malicious Node; Intrusion Detection; N-Crypt.*

1. INTRODUCTION

WSN is a gathering of sensor nodes teamed up with a set of objectives. Those objectives are checking, cautioning and giving data on-interest in WSN. The majority of the usefulness of the WSN is information driven additionally it is conceivable to utilize WSN as a dispersed processing stage under an extraordinary situation, for example, remote. All the usefulness of the sensor system is given because of the other distinctive capacities of the sensor nodes in the system. A sensor node has an implicit sensor, constrained computational capacities and imparts through remote medium. Hence they can fit to gather the physical data of nature's turf, which prepare that crude data and speak with the other neighbor nodes in the WSN-course.

Since a node can fit to get the data about alternate nodes in WSN there are conceivable outcomes to ruin the information by any malignant node. Different malignant exercises happen in the course to ruin the information, for example, Sinkhole, Wormhole, and Sybil, parcel dropper assaults. All these malevolent nodes are focusing on the information throughout transmission. In this paper N-Crypt gives a high information security by applying Encryption and Decryption in cyclic way. The related work talked about the pertinent methodologies presented in prior exploration.

2. RELATED WORKS

The power consumption, and the security is considered in the MIMO based transmitter and receiver [2], [3], and it is difficult to implement multiple antennas in some cases with handheld terminals and sensor nodes. In [4] and [5], the author showed how to enhancing the physical layer for security and improving the secret communication among nodes in co-

Journal of Theoretical and Applied Information Technology
31st August 2014. Vol. 66 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

operative networks. Further enhancing the physical layer for security by examining the two way relay model in [6] and [7], multiple two-way relays are exploited to improve the confidentiality volume against snooping attack. In addition, the authors of [8] and [9] examined the physical-layer safekeeping in MIMO relay networks and presented the substantial enhancement in terms of secrecy volume through the use of MIMO relays. Opposing from the outdated relay selection in [10]-[15] where only the channel state information (CSI) of two-hop relay links are measured, we here have to take into explanation additional CSI of the wiretap links, in addition to the two-hop relay links' CSI.

3. PROBLEM STATEMENT

These days WSN based requisitions are utilized within developing circumstances like Military, observation and human services industry. Because of the qualities of Sensor nodes [mobility, haphazardness, perception inside a reach etc.,] it is getting expanded the movement of noxious nodes in the WSN.Security is one of the most important factor in all sensor network. The sensor nodes or the communication channel can be manipulated by any unauthorized nodes for its own benefit. The factors also to be considered are energy, malicious node detection rate and packet transmission. The issue taken in this paper is to give an information security by exceptionally secured information transmission without any information misfortune. VEBEK-I [virtual Energy-Based Encryption and Keying] methodology was presented by Aditya et al. which gives a security calculation to scramble and unscramble the information utilizing irregular key system.

4. PROPOSED MODEL

N-Crypt is one of a secured information transmission model. One time element key is working for one parcel just and it makes part of key bungling caution throughout decoding. Likewise the transitional nodes in the course can additionally have the capacity to demonstrate their validity and truthfulness. Utilizing DRK – [dynamic Random Key] system nodes accessible on the course can produce element enter in a specific time. Utilizing that time based key the information bundle is scrambled and forward to the following node. To settle the information sending the configuration of the information bundle helps by having the data like:

Packet | Source-Address | Destination-Address| Current-Node-Address | Key | TTL (1)

From source node to destiny node every node creates their key with help of DRK and passes it with the information to N-Crypt-I. The same methodology is rehashed and encoded information is sent to the following next node until it achieves the Destination Node. Each one time the terminus node locations is contrasted and the current node address and stop the information sending process and call the N-Crypt-II calculation for information decoding. The general usefulness of the N-Crypt methodology is demonstrated in Figure-1, Figure-2 plainly. Over all usefulness of N-Crypt is viewed by an observing Node-W [Watchdog]

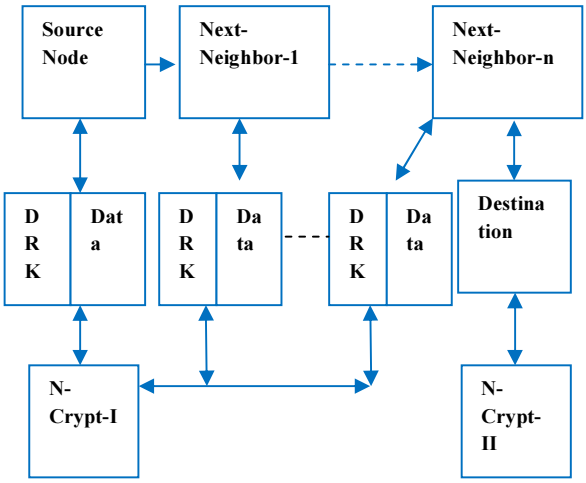

Figure-1: N-Crypt Model

4.1 Dynamic Random Key

The strategy DRK contains two shares. The key game plan stage will make the introductory change from a key arbitrarily of size

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

k bytes. Naturally k will be in the combination around 5 and 64 in size. The best key size is k = 256. The fore most partition of the method is a pseudo arbitrary inventor that handles one byte profit in each one stage. The encryption will be a XOR of the pseudo arbitrary request with the message, as typical for information stream images or the codes. For the examination of DRK it is suitable to substitute the inventive system that workings on bytes (Z/256z) by a disentanglement that deals with Z/kz for some k N. For k = 256 we get the interesting calculation.

4.2 Algorithm DRK Key Arrangement

Do initialization of all the variables (2)

For j from 0 to k – 1 do (3)

S[j] ← j (4)

Next j (5)

I ← 0 to 6 //{generate a random permutation} (6)

For j from 0 to k-1 do (7)

I ← (i + S [j] +k [j mod l] mod k (8)

Exchange S [j] and S [i] (9)

Next j (10)

4.3 Algorithm DRK Pseudo Random Creator

Do initialization of all the variables (11)

i ← 0 (12)

j ← 0 (13)

{Generate pseudo random sequence} (14)

label L (15)

i← (i +1) mod k (16)

j← (j+ S [i]) mod k (17)

Swap S[i] and S [j] (18)

k← (S[i]+ S [j]) mod k (19)

Print S[k] (20)

End label K (21)

The DRK calculation based key might be utilized just as a part of one round. For the following adjust the key is reset to zero [0] and the recovered key will be utilized. On the off chance that an

ambush node use bytes from the i^{th} round or later we will call it an i^{th} round assault in the system.

4.4 N-Crypt-I

The first module of the N-Crypt methodology is N-Crypt-I, where each one halfway node scrambles the accepted information with own key produced by them utilizing DRK and passes the key promptly to the Key-table with their ID including the source node. Case in point in figure-2, the source node S is sending the information bundle to the end node D. The moderate nodes are 1, 2, 3, and 4. The node S is producing a "xxx" key alertly utilizing DRK and scramble the information parcel utilizing that key and send it to the node 1. Likewise node S stores the key with the ID, xxx and S separately in the key-table all the while is indicated in Figure-2. In the same way all the nodes from source to node 4 over and over do the encryption and key overhauling in the key-table. The Node W viewing the usefulness.

4.5 Data Forwarding Module

The node after acceptance the packet desires to follow the sub sequent levels:

Level-1: verify for data acknowledged

Level-2: if yes get Node Id

Level-3: if [acknowledged node id =Valid] //Node-W

Level-4: forward the data to subsequent node go to level-1

Level-5: decrypt data, validate genuineness if genuine go to level-7 Else go to level-8

Journal of Theoretical and Applied Information Technology
31st August 2014. Vol. 66 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Level-6: Get current (my) Key value Encrypt data with my key value

Level-7: forward data

Level-8: go to level-1

The topological structure is occupied with multiple group .All the sensor nodes communicate to heir group heads which in turn forwards message to the destination node or the base station.

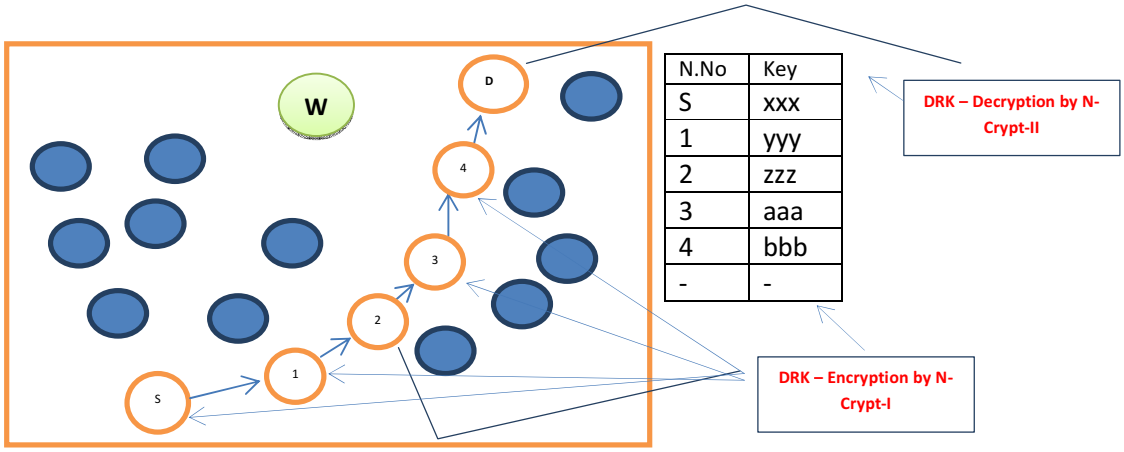

Figure-2: N-Crypt for WSN

5. N-Crypt-II

Once the information bundles arrived at the terminus node, the N-Crypt-II will be called for decoding the information. While N-Crypt-II being called, it peruses the key from lowest part record to the top most record and unscrambles the information over and over. Once the first information is recovered the key table is deleted for future key stockpiling. The unscrambling might be composed as data[d]=decrypt(decrypt(decrypt(data,(key)_n), key_(n-1))… … ,(key)_1)

6. Experiments

The calculation is composed DOTNET schema 2010 and the proposed methodology is checked and the results are given in the advancing part comes about and talk. The front-end is outlined utilizing Asp.net and the code behind is composed in C#.net dialect. The look-n-feel of the GUI is great in Asp.net and the execution efficient and correctness of looking and capacity calling is immaculate in C#.net. Therefore the trial of this paper is actualized in DOTNET system 2010. In this execution the Nodes are expected as clients.

7. Results and Discussion

The GUI (Graphical User Interface) of the proposed methodology is produced in Asp.net and the pages

are given in this segment. The usage of this work begins with another client entrée to the cloud and it could be acquired by enlistment of client. For enrollment the client need to fill the significant data given in the enlistment structure like name secret key and some contact data of the client. When the subtle elements are submitted to the server, the server produces a programmed number as the client ID and allocate to the client, it is likewise put away with the client points of interest. Once the client is enrolled he can login with the client ID and the secret key.

Journal of Theoretical and Applied Information Technology
31st August 2014. Vol. 66 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

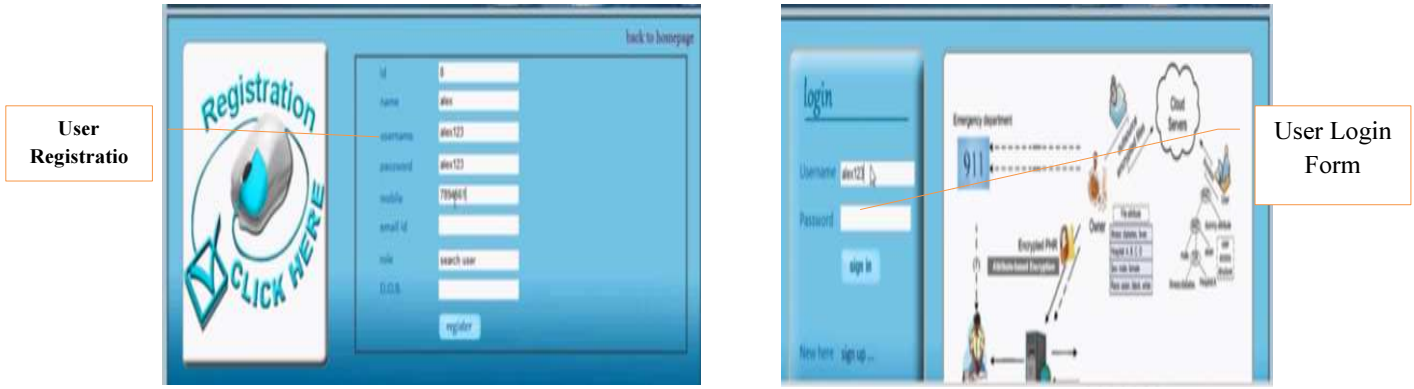

Figure-3: Registration Form

One the enlistment and login is achievement, the current client subtle elements are given in the left half of the board, and he will get a mystery key allocated by the server for encryption and decoding procedure of the specific client. While the client sends a record, it is must to enter the mystery key and give the document is delineated pictorially in Figure-4.

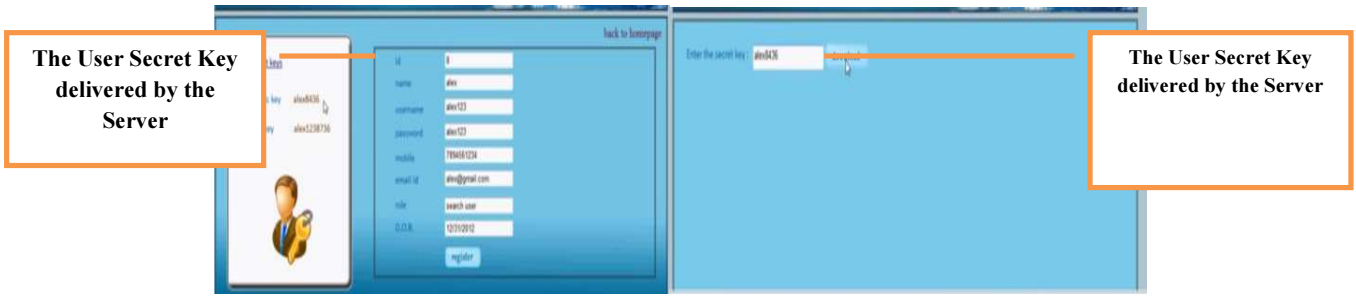

Figure-4: User Authentication

When the record sent by the sender the document will be encoded N number of times as per the moderate clients around the sender node and the end node. In our framework there are two middle of the road nodes are accessible, so including sending node three times the record is getting encoded more than once lastly the N-Crypt-II will unscramble the document and submit to the objective is demonstrated in Figure-5 plainly.

Journal of Theoretical and Applied Information Technology
31st August 2014. Vol. 66 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

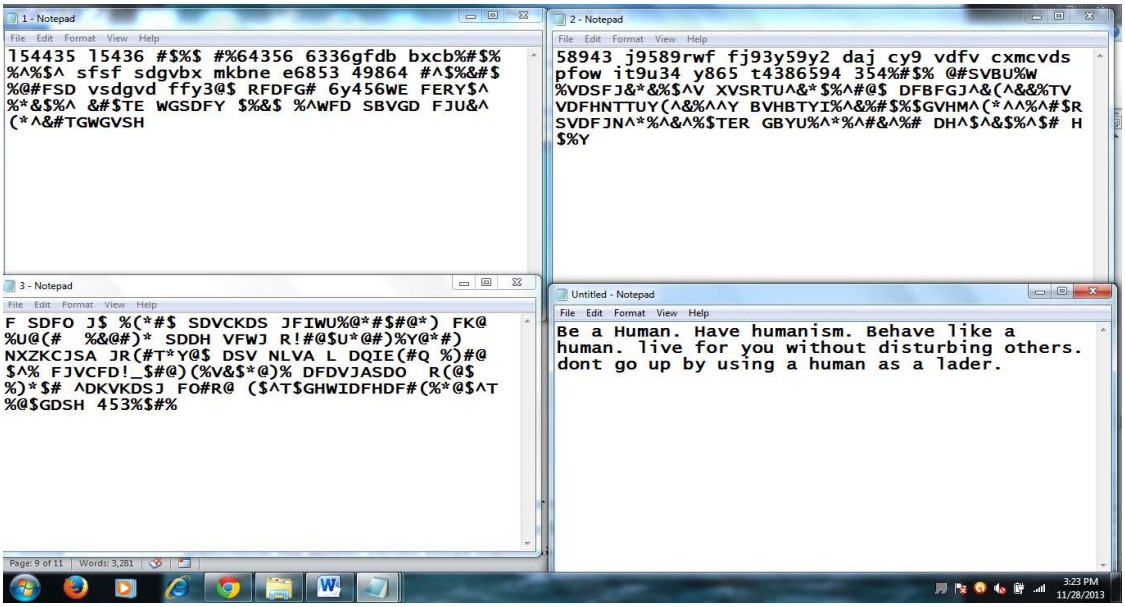

Figure-5: File Encryption & Decryption

The first record name is sample.txt, and the first run through encoded document named as 1.txt, the second time scrambled record named as 2.txt lastly the unscrambled record named as untitled.txt. On the off chance that the client needs to spare the unscrambled record while downloading itself they can select their nearby framework area and give their document name.

From this usage the time taken to do the encryption unscrambling is nearly less, so cost is likewise less. Consequently this security N-Crypt focused around Data Level security is effective. The system proficiency and the discovery rate acquired utilizing N-Crypt is given in the accompanying Figures.

To process the productivity of N-Crypt approach regarding energy by changing the amount of frameworks changed as 10, 20, 30, 40 and 50 nodes in WSN. The remaining energy acquired utilizing VEBEK for 10 nodes is 96%, 20 nodes is 92.12%, 30 nodes is 89.45%, 40 nodes is 88.01% and for 50 nodes 87% where the remaining energy got utilizing N-Crypt for 10 nodes is 90.04%, 20 nodes is 98.98%, 30 nodes is 98.01%, 40 nodes is 97.49% and for 50 nodes 97.06%. The remaining energy examination around VEBEK and N-Crypt is indicated in Figure-6.

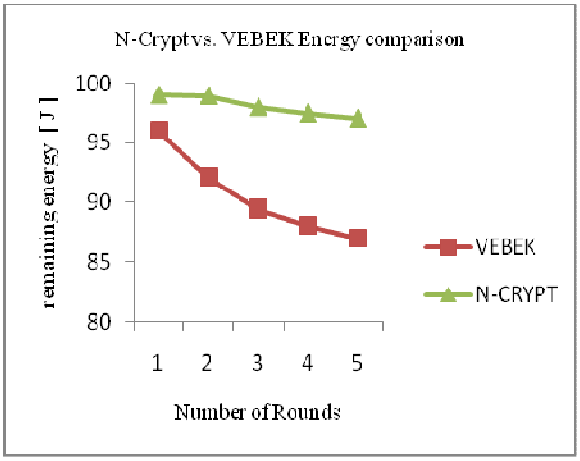

Figure-6: N-Crypt vs. VEBEK Energy Comparison

Journal of Theoretical and Applied Information Technology
31st August 2014. Vol. 66 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

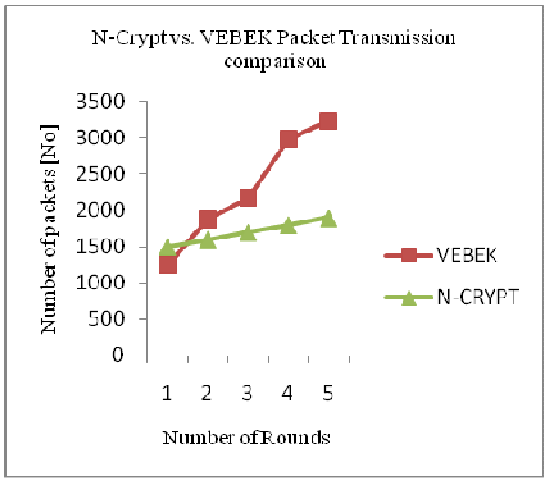

Figure-7: N-Crypt vs. VEBEK Packet Transmission Comparison

To register the proficiency of N-Crypt approach regarding number of parcel transmission by changing the amount of frameworks changed as 10, 20, 30, 40 and 50 nodes in WSN. The amount of bundle transmission utilizing VEBEK for 10 nodes is 1254, 20 nodes is 1876, 30 nodes is 2167, 40 nodes is 2984 and for 50 nodes 3230 where the parcel transmission acquired utilizing N-Crypt for 10 nodes is 1500, 20 nodes is 1600, 30 nodes is 1700, 40 nodes is 1800 and for 50 nodes 1900. The amount of bundle transmission examination around VEBEK and N-Crypt is indicated in Figure-7.

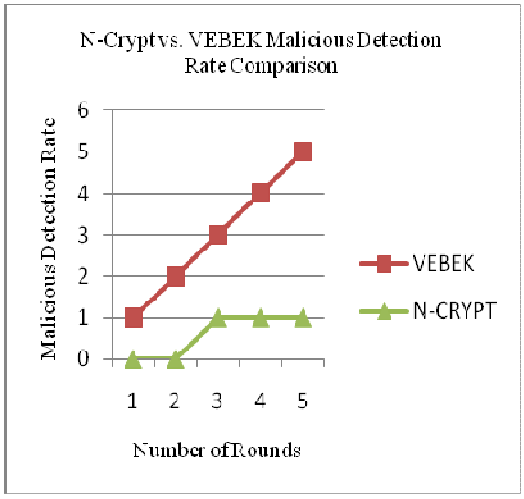

Figure-8: N-Crypt vs. VEBEK Malicious Detection Rate Comparison

To figure the effectiveness of N-Crypt approach regarding malevolent identification rate by changing the amount of frameworks changed as 10, 20, 30, 40 and 50 nodes in WSN. The amount of pernicious action acquired utilizing VEBEK for 10 nodes is 1, 20 nodes is 2%, 30 nodes is 3%, 40 nodes is 4 and for 50 nodes 5 where the identification rate got utilizing N-Crypt for 10 nodes is 0 20 nodes is 0, 30 nodes is 1, 40 nodes is 1 and for 50 nodes 1. The discovery rate correlation around VEBEK and N-Crypt is indicated in Figure-8.

8. CONCLUSION

This paper focuses on giving information security in the WSN.By sparing the energy, expanding the throughput, speed, security the expense might be upgraded. In the investigation based requisition the energy sparing based correspondence with high security is really vital. To conquer this anxiety, we offered a secured correspondence structure for sensor systems called N-Crypt and Keying. In this proposed scheme the energy consumption is greatly reduced to 60 percentage without the presumption of a dependable medium access control layer. In future, it could be stretched out as energy effective, secured convention might be actualized for remote co-agent systems.

REFERENCES

[1]. Aditya Shukla, Anurag Pandey, Saurabh Srivastava, " Virtual Energy Based Encryption & Keying on Wireless Sensor Network", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278- 727Volume 9, Issue 3 (Mar. - Apr. 2013), PP 34-43.

[2]. Y. Zhou and T.S. Ng, "Performance analysis on MIMO-OFCDM systems with Multi-code Transmission," IEEE Trans. Wireless Commun., vol. 8, no. 9, pp. 4426-4433, Sept. 2009.

[3]. Y. Zhou and T.S. Ng, "MIMO-OFCDM systems with joint iterative detection and optimal power allocation," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 5504-5516, Dec. 2008.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[4]. Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in Proc. 2013 IEEE Intern. Conf. Commun. (IEEE ICC 2013), pp. 1-5, Budapest, Hungary, Jun. 2013.

[5]. Y. Zou, X. Wang, and W. Shen, "Eavesdropping attack in collaborative wireless Networks: Security protocols and intercept behavior," in Proc. 2013 IEEE Intern. Conf. Comp. Supp. Cooper. Work in Design (IEEE CSCWD 2013), pp. 1-5, Whistler, Canada, Jun. 2013.

[6].Sudheer pembusani, abhishek gudipalli, saravanan mahadevan, "Challenges In Minimising Energy Consumption For Wireless Sensor Networks", Journal Of Theoretical And Applied InformationTechnology,28 February 2014, vol. 60. No. 3 -2014.

[7]. R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," IEEE Trans. Veh. Tech., vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[8]. J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[9]. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna twoway relay channels with analog network coding against eavesdroppers," in Proc. IEEE 11th Intern. Workshop Signal Process. Adv. in Wireless Commun. (SPAWC 2010), pp. 1-5, Jun. 2010.

[10]. Bletsas, H. Shin, M. Z. Win, and A. Lippman, "A simple cooperative diversity method based on network path selection," IEEE J. Select. Areas in Commun., vol. 24, no. 3, pp. 659-672, Mar. 2006.

[11]. Rahal Romadi, Hassan Berbia, B.Bounabat, " Wireless Sensor Network Simulation Of The Energy Consumption By A Multi Agents System", Journal Of Theoretical And Applied Information Technology, Vol 25. No. 1-2011.

[12]Abdessadeq fettouh, Abdelazizel fazziki, Najibel kamoun, "Quality Of Services Routing For Mobile Ad-Hoc Networks", Journal Of Theoretical And Applied Information Technology, December 2013 ,Vol. 58. No. 2-2013.

[13]Ganeshkumar.P and Thyagarajah.K "Balancing throughput and fairness for concurrent flows based on per flow scheduling in ad hoc networks", International Journal of Computers and Applications (ACTA Press), Vol. 32, No. 4, 2010, pp. 408-415.

[14]Gopalakrishnan.S. and P. Ganeshkumar "Intrusion Detection in Mobile Ad Hoc Network using Secure Routing for Attacker Identification Protocol", American Journal of Applied Sciences, ISSN: 1546-9239, Science Publication 2014.

[15] S.Sheeja, Dr.Ramachandra V.Pujeri, "Efficient Energy Based Congestion Control Scheme For Mobile Ad Hoc Networks" Journal of Theoretical and Applied Information Technology,10 June 2014 -- Vol. 64. No. 1 -- 2014