ISSN:2231-0711

Amandeep Singh et al | IJCSET(www.ijcset.net) | 2018 | Volume 8 Issue 1, 4-7

Secure File Sharing in Wireless Sensor Network Using Kudos and Base64 Algorithm

Amandeep Singh[1]
[1]*Department of Computer Engineering, BBSBP College (Fatehgarh Sahib, Punjab), India*
[1]amanji6353@gmail.com
Maninder Kaur[2]
[2]*Department of Computer Science & Engineering, DIET (Kharar Campus, Punjab), India*
[2] maninderecediet@gmail.com
Prabhdeep Kaur[3]
[3]*Department of Computer Engineering, BBSBP College (Fatehgarh Sahib, Punjab), India*
[3]prabh_316@yahoo.co.in

Abstract: **- Wireless Sensor Network is an emerging and rapidly growing technology in today's time. Wireless sensor networks are increasingly being used to monitor habitats or environmental conditions such as temperature, sound etc, analyze traffic patterns, and gather data for reconnaissance and surveillance missions. Many wireless sensor networks require the protection of their data from unauthorized access and malicious tampering, motivating the need for a secure and reliable file sharing for sensor nodes. They are deployed in an open environment. Therefore they are prone to security threats. In a small network, nodes can communicate with each other in a simple manner because of less number of nodes. But in huge network it becomes challenge for sensor nodes to recognize all the sensor nodes present in a network. In this research work, the main base station keeps the record of all the sensor nodes and the Kudos and Base64 Algorithm have been applied to provide secured file sharing in a wireless sensor network.**

Keywords: **- Sensor, Nodes, Secure, Reliable**

I. INTRODUCTION

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network (WSAN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. There are different applications of wireless sensor network which is used in day to day life. Some of the applications are as follow:-

Motion tracking: Sensor nodes sense movements in a room. These nodes can install in the rooms which serves the purpose lights get automatically switched off when no one present in the room. Nodes installed in the vehicles which sense the automobiles disturbances [1].

Seismic sensing: Sensor nodes can provide more precise study on seismic activities than other studies. It provides aftermath of earthquakes on buildings very precisely. Sensor nodes deployed in different parts of a building which provides the effects of earthquake strength to the building [2].

Security: Sensor nodes can deploy for security purposes. Military can deploy sensor nodes on borders which can detect armed men while crossing the border and alarmed border patrolling team [3].

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting[4][10]. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network.

II. LITERATURE SURVEY

A sensor network is defined as composition of a large number of low cost, low power multi functional sensor nodes which are highly distributed either inside the system or very close to it. These nodes which are very small in size consist of sensing, data processing and communicating components. The position of these tiny nodes need not be absolute; this not only gives random placement but also means that protocols of sensor networks and its algorithms must possess self organizing abilities in inaccessible areas. However nodes are constrained in energy supply and bandwidth, one of the most important constraints on sensor nodes are the low power consumption requirements. These constraints combined with a specific deployment of large

number of nodes have posed various challenges to the design and management of networks. These challenges necessitate energy awareness at all layers of networking protocol s tack. The issues related to physical and link layers are generally common for all kind of sensor applications , therefore the research on these areas has been focused on system level power awareness such as dynamic voltages calling, radio communication hardware, low duty cycle issues , system portioning, and energy aware MAC protocols . At the network layer, the main aim is to find ways for energy-efficient route setup and reliable relaying of data from the sensor nodes to the s ink s o that the lifetime of the network is maximized. Sensor nodes not only carry limited but usually carry irreplaceable power sources and thus the main focus of sensor network protocol is primarily on power conservation. At the cost of lower throughput or higher transmission delay they must possess inbuilt trade-off mechanism that gives the end user the option of prolonging network lifetime. Realization of these and other sensor network applications require wire les s ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wire les s ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad -hoc networks are as follows

* Sensor nodes mainly us e broadcast communication whereas ad-hoc network uses point to point communication.
* The topology of a sensor network changes very frequently.
* Sensor nodes may not have global identification because of the large amount of overhead and large number of sensors.
* The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in Ad- hoc networks.

In this paper, we present a survey of protocols, design issues and outline the use of certain tools to meet the design objectives. The paper is organized as follows. In the first section we specify some of the sensor network applications, second section summarizes the system architecture design issues for sensor networks and there implications on data routing. In section three, classification and comparison of protocols have been discussed.[5]

Wireless Sensor Networks (WSN) are used in variety of fields which includes military, healthcare, environmental, biological, home and other commercial applications. With the huge advancement in the field of embedded computer and sensor technology, Wireless Sensor Networks (WSN), which is composed of several thousands of sensor nodes which are capable of sensing, actuating, and relaying the collected information, have made remarkable impact everywhere. This paper presents an overview of the various research issues in WSN based applications. [6]

Various traditional approaches proposed by various authors from years of research, but they are not optimal and secure transmission is still an interesting research issue in the field of wireless sensor networks. Nodes between the transmission is more while transmission of data between source and destination node , the performance and data confidentiality needs better solution[7][8].

Wireless Sensor Networks is one of the hottest topic and growing area now days. WSN have become popular due to its wide range applications. There are lots of problems in Wireless sensor networks related to Power, Cost, and Bandwidth etc. Power optimization is the main constraint in WSN and this limitation with a typical deployment of huge figure of nodes has added challenges to the design and management of WSN. They are typically used for remote environment monitoring in areas where providing electrical power is difficult. Therefore, the devices need to be powered by batteries and alternative energy sources. The energy of battery is limited in Wireless sensor Networks.

In WSN, limited transmission range, processing and storage capability as well as power resources are limited of sensor node. In this work, present a survey of new power saving and power optimization techniques for wireless sensor networks, which gives better result and increase the performance of WSN application areas.

III. METHODOLOGY OR ALGORITHM USED

The aim of the methodology is to increase the reliability of a network and improvised the secure file sharing. File sharing in this network is achieved by this algorithm. The framework is designed which consists of main base station, cluster heads, sensor nodes and database. The record resides at base station for every sensor node present in a network which gets updated with every transaction. The authentication of sensor nodes has done by main base station. The file sharing has been carried out between two sink nodes of different clusters. In this algorithm, we have taken two predefined stacks along with a logic based lookup concept. The first stack holds the information about the sequence counter implemented by the user. Whereas the other stack maintains the record for the data on which encryption has to be performed. The encryption process is of five steps; and four out of these five steps can be customized. Only step 2 cannot be altered by the user. The encryption process does a variety of binary operations like Shift Left Operation on the message for protecting it against unauthorized attacks. In this operation, bits are shifted left

to one place and Most Significant Bit (MSB) is placed to Least Significant Bit (LSB). The kudos and base64 algorithm consists of different steps which are discussed below:

The steps of encryption are given as follows:

1) The plain text is read from input file line by line i.e. separated by a full stop. The user has the option of choosing the sequence counter for transposition of characters. This sequence number must be a positive whole number. The shift-right operation is used here for transposing the characters. The first line characters are transposed using the sequence counter and the next line characters are transposed by incrementing the sequence counter by one. If the user opts not to choose the sequence number, the default sequence number 1 is selected. Suppose the value for first line is 1, for second line will be 2, and so on. If user specifies it as 5, value for first line will be 5, for second line it will be 6, for third line 7 etc. This step is categorized under block level encryption.

2) This part of encryption is user independent and is a block level encoding. Here, two strings of equal length are chosen from the text file and are shuffled. The shuffling takes place by placing one character of first string followed with one character from second string; and so on. For example: Following are the strings of length 20 characters selected:

Q W E R T Y U I O P A S D F G H J K L Z and q w e r t y u i o p a s d f g h j k l z;

Then the output of this phase is:

Q w E r T y U i O p A s D f G h J k L z and q W e R t Y u I o P a S d F g H j K l Z.

3) The next step is the stream encryption of the plaintext. The output from the previous step is taken as the input. Character by character is read and then transformed into ASCII code. The ASCII value of each character is then incremented by some random number (sequence counter). This is the second sequence counter that user can pick.

For example: The input is KUDOS,

Then ASCII value of each character is K – 97, U – 107, D – 90, O – 101 & S - 105.

The user chooses sequence counter 1 for 1st character, 3 for next, 5 for next and so on. KUDOS is encoded into LXIV.

4) Now, the input character from last step is converted into 8-bit binary number. Here a block of 64 bits are taken into account and then a dynamic sequence counter is decided by the user. Then shift-left operation is performed on this 64-bit data based on the opted sequence counter. For example: 1 shift-left operation for first block, 4 shifts for second block, 9 shifts for third block, and so on.

5) The encryption process is continued on next step on the base of compliment. A sequence counter is decided to work on the 8-bit level of intermediate cipher text. A sequence of bits will be complemented and the next block of same number of bits will remain unaffected. For example: First 2 bits will be complimented, then next 2 bits remain same; then next 4 bits are complimented and the next 4 bits remain unchanged. This sequence counter is also identified by the end user, hence customizing the whole encryption process according to his particular needs.

6) The steps 1 to 5 are repeated till the input plaintext is changed into the cipher text and public health, and are examples of operations research or management science methods.

IV. EXPERIMENTAL RESULTS

This section shows the results computed by this methodology. The result is calculated on the basis of client mobility speed, accuracy and computation cost.

Accuracy: - The accuracy of this is compared with paper [9] against 1000 number of transaction. As authentication of sensor nodes present in a network is given by the main base station which is based on the past interactions in a network. The average accuracy with 1000 transactions is 98.

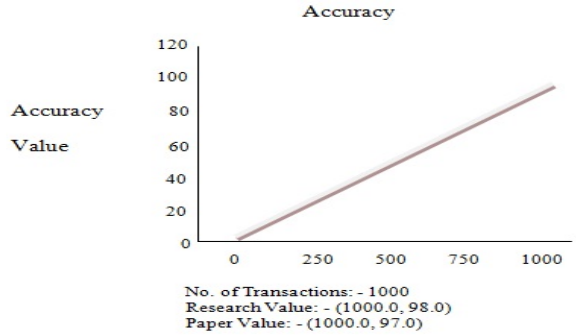

Fig 1: Graph showing the accuracy of proposed method as compared to paper [9]

Client Mobility Speed: - The improved interface allows a user to send file from different nodes with which it was not associated earlier. The user will get authenticated from the main base station and can send file. The mobility of user from one node to another node is the client mobility speed. The client mobility speed is compared with paper

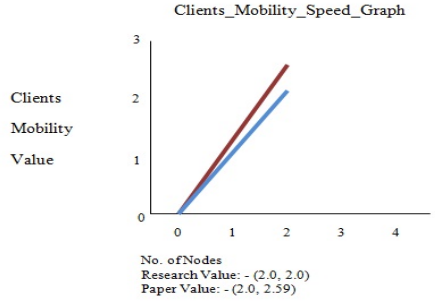

Fig 2: Graph showing the Client Mobility Speed using the proposed method as compared to paper [10]

Computation cost: Computation cost is the latency time which it take to encrypt and decrypt the file when it is send from one cluster to another cluster. Computation cost is decreasing in comparison with paper

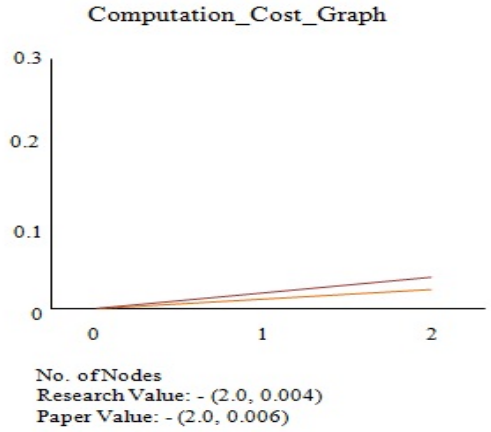

Fig 3: Graph showing the Computation Cost using the proposed method as compared to paper [10]

V. CONCLUSION

In this paper, we have been concluded that our research work provides a improved results as compared to base paper. Although security threats are there for wireless sensor networks as they work in an open environment. In this main base station authenticates the sensor nodes present in a network. After the node authentication by main base station the sharing of files between two different nodes can be done. The algorithms Kudos and Base64 are used for the authentication and encryption for sharing of file in a network. The proposed work increases the security of network by eliminating the entry of untrusted nodes in a network. The computation cost during file sharing has been decreased. The client mobility speed increases when it switches from one node to another node to share the file. In the future work, some more different algorithms can be applied to get improved results in terms of accuracy and enhancement.

REFERENCES

[1] Al-Turjman, Fadi M., Hossam S. Hassanein, and Mohamed A. Ibnkahla. Efficient deployment of wireless sensor networks targeting environment monitoring applications. Computer Communications 36. no. 2 . pp. 135-148. 2013

[2] Liu, Guojin, Rui Tan, Ruogu Zhou, Guoliang Xing, Wen-Zhan Song, and Jonathan M. Lees. Volcanic earthquake timing using wireless sensor networks. In Proceedings of the 12th international conference on Information processing in sensor networks. pp. 91-102. ACM. 2013.

[3] Pannetier, Benjamin, Jean Dezert, and Genevieve Sella. Multiple target tracking with wireless sensor network for ground battlefield surveillance. In Information Fusion (FUSION). 2014 17th International Conference on. pp. 1-8. IEEE. 2014.

[4] Mehdi Saeidmanesh, Mojtaba Hajimohammadi, and Ali Movaghar, “Energy and Distance Based Clustering: An Energy Efficient Clustering Method for Wireless Sensor Networks”, World Academy of Science, Engineering and Technology , USA, Vol 3, 2009, pp 212- 230.

[5] Swati Sharma, Dr. Pradeep Mittal,” Wireless Sensor Networks: Architecture, Protocols”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 1, January 2013

[6] Applications: A survey International Journal of Information and Electronics Engineering, Vol. 2, No. 5, September 2012 Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, and Elijah Blessing Rajsingh.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” Int. J. Comput. Applications, vol. 47, no. 11, pp. 23–28, 2012.

[8] Chris Karlof , David Wagner., “Secure routing in wireless sensor networks: attacks and countermeasures,” 1570-8705/$ - see front matter _ 2003 Elsevier.

[9] Zhang, Bo, Zhenhua Huang, and Yang Xiang. A novel multiple-level trust management framework for wireless sensor networks. Computer Networks 72 pp: 45-61,2014.

[10] Li, Celia, Uyen Trang Nguyen, Hoang Lan Nguyen, and Nurul Huda. Efficient authentication for fast handover in wireless mesh networks. computers & security 37 pp: 124-142,2013.