International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur, Tamilnadu, India.

DES ALGORITHM USING ENERGY CONSUMPTION IN MOBILE SECURED SENSOR NETWORK

P.Chitra,
Research Scholar
Department of Computer Science,
Erode Arts and Science College,
Erode, Tamilnadu, India.

Dr.T.R.Ranganayaki,
Associate professor,
Department of Computer Science,
Erode Arts And science college,
Erode, Tamilnadu, India.

Abstract: Mobile wireless sensor networks are the new generation of network and the networks are organized by the form of Double -layer which can adapt to the application of the sink node and the sensor node with mobility. The main objectives of this method are uniform distribution, increase of network life time, decrease of traffic load and load balance and security in data transfer in reliability of formed path. This starts from network architecture and is divided into high-end node layer, DEN (Data Encryption node) layer and low-end node layer. The high-end node are responsible for the data routing, DEN is used for secure the data and the low- end node is used for sensing and reporting data. This approach will be for data transfer in security and reduce the energy consumption.

Keyword: Sensor networks, Routing, Security lifetime, Sink node, Uniform distribution, DEN.

I.INTRODUCTION

Wireless sensor networks are collection of nodes where each node has its own sensor, processor ,transmitter and receiver and such sensors usually are low cost devices that perform a specific type of sensing task. A wireless sensor network consists of a number of sensor nodes with the capability of storing processing and relaying the sensed data and often has a base station called sink node [1]. Being of low cost such sensors are deployed densely throughout the area to monitor specific event. The wireless sensor networks mostly operate in public and uncontrolled area; hence the security is a major challenge in sensor applications. The traditional security mechanisms are authentication, symmetric key [6] for encryption and decryption cryptography. Five key features are used to develop WSN are scalability, security, reliability, self – healing and robustness. For each implementation, there are different type of attacks possible and demands a different security level. As WSN is mostly used for gathering application specific information from the surrounding environment, it is highly essential to protect the sensitive data from unauthorized access. Sensor nodes may also be physically captured or destroyed by the enemies. The uses of sensor network in various applications emphasis on secure routing. Various protocols are proposed for routing [3] and data gathering but none of them are designed with security as a goal. The resource- limitation of sensor networks poses great challenges for security. WSN are based on symmetric key cryptography [2]. Wireless Sensor Networks are being employed in various real time fields like military, disaster management, Industry, Environmental Monitoring and Agriculture Farming.I point out two approaches, first DES algorithm for security purpose and energy consumption using TABU search algorithm. First, DES requires sender and receivers to share a secret. Cryptographic key [7] anb this key is part of the input to the computation. The sender computes the DES over the packet and includes it with the packet using the secret key. A receiver sharing the same key re-computes the des and compares it with the DES in the packet. If the two are the same then the receiver accepts the packet or otherwise reject it. Authentication is done using the cipher block chaining with DES which creates a message integrity code using a block cipher in CBC mode and computes a DES over the packet and includes the length of the authenticated data. Second, energy consumption [1] is to calculate the total energy of every moment using the trace files for both kinds of mobile wireless sensor network with the same number of mobile sensor nodes - one is flat mobile wireless sensor node and another is two-end node wireless sensor network and then to compare total energy of both kinds of mobile wireless sensor network in the same moment. To calculate the energy TABU search algorithm is used. To make energy consumption and packet delay two - end node is used; they are high-end node [1], DEN and low-end node [1]. The high – end node keep connection each and are responsible for collecting and forwarding the sensing data from sensor node. The low – end node only responsible for sensing data and reporting of the data to the high – end node and they cannot communicate with the other sensor nodes. The high – end node: A large number of sensor nodes with poor resource are randomly deployed in the specified region and can randomly changed its location; they are responsible for sensing interesting data in the monitoring region and sense the sensing data to the static high – end node in the single-hop form, after the sensor nodes obtain the interesting data .then high – end node route the sensing data to sink by multi – hops in the high – end node after collecting data from sensor nodes. DEN: DEN (Data Encryption Node) is used for security purpose which unauthorized person can not access the authorized information. In this node encryption technique is used for both sender and receiver. Authentication is done using the cipher block chaining with DES which creates a message integrity code using a block cipher in CBC mode and computes a DES over the packet and includes the length of the authenticated data.

The Low – end node: This layer consists of a small number

of static. The high – end node and plays the role of gathering and forwarding the sensing data from sensor node, and their processing, communication, storage capabilities are stronger than mobile sensor nodes, even they can get continuous power supply. The data will be transmitted in multi – hop from between high – end node until it do not arrive sink.

II.SECURITY ANALYSIS

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system securitydesign,implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach is called threat and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk.Denial of service [5] attack results into making unavailable the resources to their intended users. As an example node A sends request to node B for communication and node B sends acknowledge to node A but A keeps on sending request to B continuously. As a result B is not able to communicate with any other nodes and thus becomes unavailable to all of them. Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization. most of denial of service attacks may be prevented by powerful authentication and identification mechanisms

Security Requirements: A sensor network is a special type of Ad hoc network. So it shares some common property as wired network. The security requirements of a wireless sensor network [3,4] can be classified as follows:

Authentication: As WSN communicates sensitive data and the receiver needs to make the data in any decisions making process originates from the correct source. Data authentication prevent unauthorized user to detect the message from unauthorized nodes and reject.

Integrity: Integrity ensures the receiver that the received data is not allowed in transit by adversary. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident.

Data Confidentiality: It means keeping information secret from unauthorized user. Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.

Secure Localization: The sensor network often needs location information accurately and automatically. However, an attacker can easily manipulate non-secured location information by reporting false signal strengths and replaying signals. The sensor network should be robust against various security attacks and should not break the security of the entire network.

III. KEY MANAGEMENT

Security provides key mechanisms that can be used for providing confidentiality and authentication in sensor networks. It supports the establishment of four types of keys for each sensor node [1,8] – an individual key shared with the base station, a pair-wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network.

Individual Key: Every node has a unique key that it shares pair-wise with the base station. This key is used for secure communication between a node and the base station. For example, a node may send an alert to the base station if it observes any abnormal or unexpected behavior by a neighboring node, then the base station can use this key to encrypt any sensitive information.

Cluster Key: A cluster key is a key shared by a node and all its neighbors, and it is mainly used for securing locally broadcast messages. Securing sensor messages which can benefit from passive participation. Passive participation are very important for saving energy consumption in sensor node [ ].For passive participation to be feasible, neighboring nodes should be able to decrypt and authenticate some classes of messages, e.g. sensor readings, transmitted by their neighbors. This means that such messages should be encrypted or authenticated by a locally shared key.

Pair-wise Shared Key: Every node shares a pair-wise key with each of its immediate neighbors. Pair-wise keys are used for securing communications that require privacy or source authentication. For example, a node can use its pair-wise keys to secure the distribution of its cluster key to its neighbors, or to secure the transmissions of its sensor readings to an aggregation node. Note that the use of pair-wise keys precludes passive participation.

Group Key: This is a globally shared key that is used by the base station for encrypting messages that are broadcast to the whole group. Note that from the confidentiality point of view can not separately encrypting a broadcast message using the individual key of each node.

All these keys are used in the Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results. Security Protocols in sensor Networks provides data authentication, replay protection, semantic security and load balance. Data Confidentiality, two party data authentication and authentication broadcast for severely resource constrained environments. Localized Encryption and Authentication Protocol is a key management.

IV.DES MECHANISM

In application layer, I use DES (Data Encryption Standard) algorithm transfers 64 bit input in a series of steps into 64 bit output in the same key 56 bit. The key is passed through the permutation function each has 16 rounds and a sub key is produced for a left circular shift and a permutation.

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key. A block to be enciphered is subjected to an initial permutation IP and then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}. Permutation is an operation performed by a function, which moves an element at place *j* to the place *k*. The key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function KS, called the key schedule. First, a description of the computation.

Let K be a block of 48 bits chosen from the 64-bit key. Then the output L'R' of an iteration with input LR is defined by:

L' = R

R' = L (+) f (R,K)

L'R' is the output of the 16th iteration then R'L' is the preoutput block.

At each iteration a different block K of key bits is chosen from the 64-bit key designated by KEY. Let KS be a function which takes an integer *n* in the range from 1 to 16 and a 64-bit block KEY as input and yields as output a 48-bit block K*n* which is a permuted selection of bits from KEY. That is

K*n* = KS (*n*, KEY)

Let the permuted input block be LR. Finally, let L0 and R0 be respectively L and R and let L*n* and R*n* be respectively L' and R' when L and R are respectively L*n*-1 and R*n*-1 and K is R*n*; that is, when *n* is in the range from 1 to 16,

L*n* = R*n*-1

R*n* = L*n*-1 (+) f (R*n*-1, K*n*)

The pre-output block is then R_{16} L_{16}.

This DES algorithm is used in the network layer. The main objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa.. In WSN, each node in the network acts as a router (because they use broadcast mechanism), so as to create secure routing protocol. Encryption and decryption techniques are used for secure routing in DES algorithm.

V. RESULTS

I will do in NS2 simulators. The messages that contain mobile code are very strong encryption and the energy consumption of the data. If the unauthorized user enters then the sensor nodes identify and the user can not access the message. This can be done by DES algorithm. Energy consumption can be done in TABU search algorithm is used to calculate the total energy of every moment.

VI. CONCLUSION

The security is going to play a pivotal role in WSN. Security describes the reliability to identify threads to the application class and introduce a new security protocol that operates in the base station made of sensor communication. We point out the two important approaches they are first, energy consumption is to calculate the total energy of every moment and second, security is used to design a security scheme and provide security services to each layer and services of sensor networks.

VII.REFERENCES

[1] Xuhui Chen and Peiqiang yu .Research On Hierarchical Mobile Wireless Sensor Network Architecture with Mobile Sensor Nodes. In proceedings of the IEEE International conference on biomedical Engineering and Informatics (BMEI) PAGES 2863 – 2867,2010.

[2] Ren Yueqing, XuLinin. A study of topological characteristics of wireless sensor network based on complex network. In proceedings of international conference on computer application and system modeling(ICCASM 2010) PAGES V15.486-V15.489.

[3] PRABHUDUTTA MOHANTY, SANGARAMPANIGRAHI, NITYANANDA SARMA and SIDDHARTHAR SANKAR SATAPATHY. Security issues in wireless sensor network data gathering protocols : a survey. In proceedings of journal of theoretical and applied information technology. PAGES 14-27 10

[4] Mayank Saraogi. Security in wireless sensor networks.

[5] Abhishek Pandey and R.C.Tripathi.In proceedings of international journal of computer application (0975-8887),Vol 3 No.2 PAGES 43-48, 2010.

[6] Kui Ren. Communication security in wireless sensor networks.

[7] David Boyle and Thomas newe. Securing wireless sensor network: security architectures in proceedings of journal of networks, Vol 3 PAGES 65-76 2008.

[8] Xiuli Ren,[1,2] and Hibin YU[1]. Security Mechanisms for Wireless Sensor Networks. In proceedings of international journal of computer science and network security (IJCSNS), Vol.6 No.3 PAGES 155-161, 2010.

[9] Kalpana Sharma, M.K.Ghose and Kuldeep, complete security frame work for wireless sensor networks. In proceedings of international journals of computer science and information security, Vol 3, No.1 2009.

[10] Dirk Westhoff, Joao GIRAO, Amardeo SARMA. Security solutions for wireless sensor networks.