Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Data Confidentiality for Providing High Security in Wireless Sensor Network

Sneha Ghormare*, Vaishali Saharel, Anil Jaiswal

Computer Department, Nagpur University Nagpur,

Maharashtra, India

Abstract— In Wireless Sensor Network, the security of data and confidentiality of data is an important aspect. Hence the data cannot be interrupted by the intruder. For updating configuration parameters and distributing management commands, data discovery and dissemination protocol for wireless sensor network is responsible. But, it has drawback is that, some protocols were not designed with security. For this reason, The DiDrip protocol i.e. first secure and distributed data discovery and dissemination protocol is proposed. The main function of this protocol is for authorized multiple network user. So, with the help of different security parameters the system provides a high security to the wireless sensor network. Energy efficient new algorithm is also used because it is difficult to crack.

Keywords: Wireless sensor network, data discovery and dissemination protocol, security, data, neighboring sensor node, AP algorithm etc

I. INTRODUCTION

Wireless sensor network are highly distributed network of all small and light weighted nodes, which are spread over the system in large numbers by the measurement of physical parameters such as temperature, pressure, relative humidity. Each node of the sensor network consists of three subsystem i.e. sensor subsystem which sense the environment, processing subsystem which performs local computation on the sensed data, and communication subsystem is responsible for message exchange with neighboring sensor node. WSNs have a wide range of applications, ranging from monitoring environments, military zones, sensitive installations and remote data collection and analysis. The most important operation in sensor network is data dissemination. In the sensor network, queries or data are routed. Any other node, which is interested in the data or base station, has to be communicated by sensor node for collection of data. Working of source is to generate the data and event can be performed when information to be reported. The working of sink is that, a node which is interested in an event and it will seek some information.

DiDrip consists of four phases, system initialization, user joining, and packet pre-processing and packet verification. For our basic protocol, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters to the network and wants to dissemination some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet.

After a wireless sensor network (WSN) is deployed, there is usually a need to update buggy/old small programs or parameters stored in the sensor nodes. This can be achieved by the so-called data discovery and dissemination protocol, which facilitates a source to inject small programs, commands, queries, and configuration parameters to sensor nodes. For updating configuration parameters distributing management commands, data discovery and dissemination protocol is responsible.

II. LITERATURE SURVEY

D. He, S. Chan, Mohsen Guizani, H. Yang [1], they proposed the first secure and distributed data discovery and dissemination protocol. To simultaneously and directly disseminate data items, it will allow the network owner to the authorized multiple network user with the different privileges to the sensor node and it addresses number of possible security vulnerability.

Archana Tayal, Prachi [2], in this research, they proposed Applications of wireless sensor network are increasing day by day. Data nodes in sensor network are easy to capture and confidential data of sensor nodes can be accessed by eavesdropper. Security has always been troublesome in the wireless communication. Cryptography algorithms are kernel of the WSN security. They present a new symmetric key algorithm based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack. The features are time taken by algorithm for different key size and number of rounds along with the comparative analysis of proposed algorithm with AES on various parameters to prove its efficiency.

D. He, C. Chen, S. Chan and J. Bu [3], they used a secure and distributed code dissemination protocol named DiCode. Ability to resist denial of service attack is the salient feature of this proposed protocol. Theoretical analysis

gives demonstration about the security properties of this protocol. For verification of the efficiency of the proposed approach, they need to implement proposed mechanism in the network of resource constrained sensor node.

D. He, S. Chan, S. Tang, and M. Guizani [4], the identification of the security vulnerabilities in data discovery and dissemination when used in WSNs had been proposed. It allows an adversary to update a network with undesirable values, erase critical variables. For addressing these vulnerabilities, this research presents the design, evaluation of a secure, implementation, for WSNs data discovery and dissemination protocol named SeDrip. The limited resources of sensor nodes, packet loss and out-of sequence packet delivery; this protocol takes into the consideration. It can provide instantaneous authentication and without packet buffering delay and tolerate node compromise.

John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary[5], Wireless Sensor Network need for effective security mechanism, these types of researches they had done. Sensor network may interact with sensitive data and operate in hostile unattended environment, from the beginning of the system design, these security concerns to be addressed. The Wireless Sensor Network security presents the obstacles and the requirement in the sensor security, they had proposed.

Ritu Sharma, Yogesh Chaba, Yudhvir Singh [6], the Wireless Sensor Networks has low power, low-cost smart devices which have limited computing resources. The security mechanisms are also be a rising big issue because there is a widespread growth of application of Wireless Sensor Network. Based on Wireless Sensor Network, a lot of real world application has been already deployed. Geographical monitoring, medical care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring, and surveillance systems these are the applications. Typical constraints, security goals, threat models and typical attacks on sensor networks and their defensive techniques or countermeasures relevant to the sensor networks on the basis of these parameters researches had done.

III. PROPOSED WORK

Existing System

Comparative Analysis

Table of comparison between existing system and proposed system.

TABLE I COMPARISON OF ALGORITHM

S Sr. No.	**Algorithm / Parameter**	**AP**	**AES**
1	No. Of CPU Cycle	Less	High
2	Key Size	Low	High
3	Energy Consumption	Less	High
4	Throughout	High	Less

Proposed Algorithm

The proposed algorithm is new symmetric key AP algorithm, which is based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack. The algorithm for both encryption and decryption are as follows.

AP Encryption Algorithm

1. Given Plain Text.
2. Randomly generate key k
3. Calculate key K2 and key 3 from the key k.
4. Repeat
5. Divide the n bits of plain text P into r multiple blocks of key size k such that n = k * r + m where m is mod (n, k)
6. Shuffle r blocks using key k
7. Substitute the text (n bits) using key K2
8. Shift the text in circular left shift with k3
9. until all round done.

AP Decryption Algorithm

1. Given Cipher Text and key k
2. Calculate key k_inv, k2 & k3 from the key k.
3. Repeat
4. Shift the text in circular right shift with k3
5. Substitute the text (n bits) using key k2.
6. Divide the n bits of plain text P into r multiple blocks of key size k such that n = k * r + m where m is mod (n, k)
7. Shuffle r blocks using inverse key k_inv
8. until all round done.

Module A: Wireless Sensor Network Formation and Communication in Wireless Sensor Network

In this module designing of complete wireless sensor network will be done, and the number of Sensor Nodes, Storage Node and Sink node, and then interrelate them to form the network.

Once, designing of Wireless Sensor Network is completed, then the next step is to have the communication between all the nodes, storage node and sink node. The communication in the sense there will be transmission of the data amongst different nodes in the node

Module B: Data Discovery and Dissemination Protocol and Parameter Requirements

The proposed module will emphasize on distribution of data discovery and dissemination protocols and the functional requirements of such protocols, it sets their design objectives. It identifies the security vulnerabilities in existing data discovery and dissemination protocols.

Module C: Providing the Security to WSN

The proposed module is a block cipher symmetric key algorithm. The set of operation known as 3S are shuffling, substitution and shift left those are to be applied to the plain text in each round. Rounds can vary from 2^0 to 2^10. Plain Text could be of any length. Though it is a block cipher but no padding is required in the proposed algorithm.

Shuffling:

In this module, algorithm initially generates a permutation table using P-box of size 48 bits to shuffle the plain text. Thus, creating a key space of size 48 bits i.e.1.2414e + 061 which is sufficiently large enough for the intruder to crack. To elaborate working of algorithm an example is considered with key of 16 bits.

Substitution:

Substitution is performed by using Vigenere Cipher. Vigenere Cipher is a poly alphabetic substitution where text is encrypted using a series of additive cipher. An additive cipher is a traditional cipher where text is shifted ahead to a particular number. Text 'M 'is substituted to 'U' for additive key = 8.

Shift:

Cipher text created in previous step is applied a circular shift by a certain number of times, and this number of shift depends upon the key K2 used by Vigenere cipher. Key k3 for circular left shift is the leftmost digit of key k2.k3 = left most (K2). In the given example k3 = 9 and generated final cipher text.

Requirements for Security

Data confidentiality:

A sensor network should not leak any sensor readings for surrounding networks. In many applications nodes can communicate highly sensitive data. For achieving confidentiality, it keeps sensitive data with a secret by encrypting the data with a secret key that only intended for receivers' posses.

Data authentication:

In sensor network, message authentication is very important for many applications. In any decision making process, the data originates from trusted source, that is to be ensured by receiver. Since, an adversary can easily inject messages. Informally, the data authentication is allows a receiver to verify that the data really was sent by the claimed sender.

Data integrity:

The receiver that the received data is no change in transit by an adversary can be ensured by data integrity in the communication. A sensor should be able to ensure that received data items have not been modified during the data dissemination process.

IV. CONCLUSION

In this paper, considering such a problem with wireless sensor network in accordance with the security is more complex and challenging in nature also the security vulnerabilities in data discovery and dissemination when it is used in WSNs. An energy efficient new AP algorithm has been proposed. Thus we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols and AP algorithm and the system will maintain the integrity of the data also ensure the performance of the system.

Here we can conclude that the proposed system will provide the high security. Then by applying energy efficient new algorithm we can encrypt and decrypt the message for the security purpose. We proposed a new symmetric key AP algorithm based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack. In this research we will not only going to detect the malicious node from the network, but we will also remove the attacker node from the network, which will make the system much more secure and reliable. This will provide us a high security to the wireless sensor network by detecting and removing the attacker from the network.

REFERENCES

[1] D. He, S. Chan, Mohsen, Guizani, H. Yang, "Secure and distributed data discovery and dissemination in Wireless Sensor Network", IEEE Trans. Parallel and distributed system, 2014.

[2] Archana Tayal, Prachi, "Energy Efficient New Symmetric Key Algorithm (AP) for WSN", Research Notes in Information Science (RNIS) Volume13, May 2013 doi:10.4156/rnis.vol13.35.

[3] D. He, C. Chen, S. Chan and J. Bu, "DiCode: DoS resistant and distributed code dissemination in wireless sensor networks", IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.

[4] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646, Sept. 2013.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Department of Computer Science Wayne State University, 2006 Auerbach Publications, CRC Press.

[6] Ritu Sharma, Yogesh Chaba Yudhvir Singh, **"**Analysis of Security Protocols in Wireless Sensor Network", Int. J. Advanced Networking and Applications 707 Volume: 02, Issue: 03, Pages: 707-713 (2010).

