IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 06-09
www.iosrjournals.org

Enhancing Security in Wireless Sensor Network Using Cryptography Techniques and To Increase the Network Life Time

C. Naveeth Babu[1], Dr. K. Karthikeyan[2]
[1]*Research Scholar, Department of CT, Dr.SNSRCAS, Coimbatore, Tamilnadu, India*
[2]*Head - Department of CS, Government Arts & Science College, Palladam, Tiruppur(Dt), Tamilnadu, India*

Abstract: *Wireless sensor network, which are basically spatially spread sensor nodes that disseminate the data throughout the network by using supportive environment. Security is an important factor that is needed to protect information and its availability, integrity and privacy. WSN protocol stack contains the physical layer, datalink layer, network layer, transport layer and application layer. In wireless network, deception attack will damage the network data and its integrity. This paper presents a symmetric key cryptographic technique engaged on the O-LEACH routing protocol which enhances and establish the security of wireless sensor networks. This protocol is chosen for this study as it is free from all threats which are based on the identity crisis. Threats such as sinkhole, selective forwarding, hello floods etc. can be identified and resolved as per the proposed scheme. In this paper the proposed scheme utilize the parameter such as network lifetime will increase to make the performance analysis.*

Keywords: *wireless sensor network, O- leach protocol, symmetric key cryptographic technique, network security, threads, network lifetime*

I. Introduction

A Wireless Sensor Network is one kind of the wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes. These networks positively cover a huge amount of spatially distributed, little, battery-operated, embedded devices that are networked to delicately collect, process, and transfer data to the operators, and it has forbidden the capabilities of computing & processing. Nodes are the tiny computers, which effort jointly to form the networks.[5]

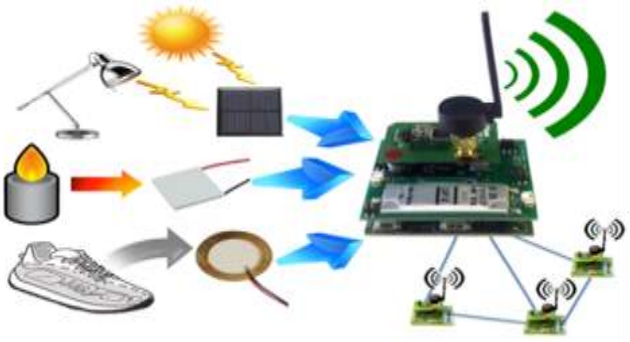

Fig 1: wireless sensor network

The sensor node is a multi-functional, energy efficient wireless device. The applications of motes in industrial are widespread. A collection of sensor nodes collects the data from the surroundings to achieve specific application objectives. The communication between motes can be done with each other using transceivers. In a wireless sensor network, the number of motes can be in the order of hundreds/ even thousands. In contrast with sensor n/w s, Ad Hoc networks will have fewer nodes without any structure.

Wireless Sensor Network Architecture

The most common Wireless Sensor Network architecture follows the OSI architecture Model. The architecture of the Wireless Sensor Network includes five layers and three cross layers. Mostly in sensor network we require five layers, namely application, transport, network, data link & physical layer. The three cross planes are namely the power management, mobility management, and task management. These layers of

the Wireless Sensor Network are used to complete the network and make the sensors work together in order to raise the absolute efficiency of the network.[8]

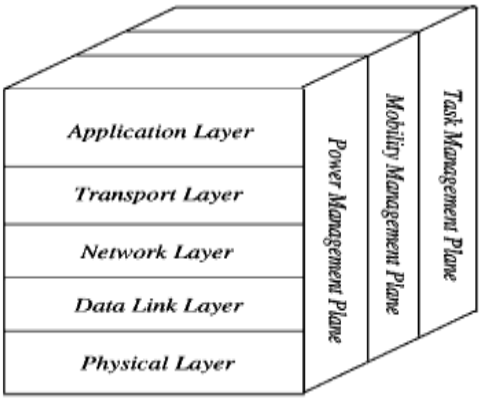

Fig 2: Wireless Sensor Network Architecture

II. Related Work

Sahabul Alam et al. "Analysis of Security Threats in Wireless Sensor Network" This paper provides the Security scheme and the threat attacks in wireless sensor network. Security schemes like: Cryptography, Steganography and Physical layer Secure Access. Threat attacks like: Collisions, Tampering, Jamming, Unfairness, and Flooding etc. They also propose a solution for the attacks in the wireless sensor network. One possible solution is the use of cryptography techniques.[1]

Jyoti Attri et al. "Study on cryptographic techniques in computer network security" provide the impression of cryptography techniques like Symmetric and asymmetric key. In symmetric key cryptography, single key is used for the encryption and decryption process i.e. using same key data can be encrypted and decrypted. Symmetric key are the very best one as compare to asymmetric key. Symmetric key cryptography is more sufficient for security in wireless sensor network.[2]

Ibriq J. et al. "A secure hierarchical routing protocol for wireless sensor networks", proposed a secure hierarchical energy efficient routing protocol (SHEER) which provides the secure communication at the network layer. To secure the routing, it implements the HIKES as a secure key transmission protocol and symmetric key cryptography.

Oliveira L. B. et.al, "Secleach - a random key distribution solution for securing clustered sensor networks" provides an efficient resolution for securing communications in LEACH. It used the random-key pre distribution and μTESLA for secure hierarchical WSN with active cluster formation. It has the fixed key pool and key distribution is static. So that keys can be identified after some certain time by the outsider and they can misuse the keys.[6]

Yih-Chun Hu et al. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" ARIADNE is an on-demand secure the ad hoc routing protocol based on DSR. It relies on the highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two parties of communication.[3]

III. O- Leach Protocol

O-LEACH is the optimization LEACH protocol. It works better than the LEACH and LEACH-C. In this protocol energy model is used. In this algorithm a new technique is proposed for the choice of sensors cluster heads based on the amount of the energy remaining after each round. In this sensor nodes are taken into the M×M square region. Uniform nodes are in it and we assume the base station is in center Sand in second simulation it will be in top or square. In this the cluster head can be select in each round with an energy value better than the ten percent of the residual value at each sensor. Then after this it will works as simple LEACH. It perform improved than LEACH and LEACH-C protocol. It increase the network lifetime and also have ability of extending the existence span of network.

IV. Proposed Schemes

We proposed a hierarchical protocol, which deals with the wireless sensor network security heterogeneity, based on O-LEACH. In the sensor network there are a number of sensor nodes (SN1) and a base station (BS1). Symmetric key scheme is used. In that there is a pair wise key is assigned to each node pair called

Two_way_keys. An associate will use the key common with corresponding CH1 to communicate with it. CH1 will use MC1 (manufacturing code) to communicate with BS1.

Assumption
• BS has no constraint regarding memory, computations and energy. It is BOSS for all SNs.
• Network is homogeneous with esteem to memory, communicational ability and computational ability of each sensor.
• Heterogeneity in Security: There are two types of nodes-Normal nodes and High Security Nodes. All the high security nodes are trusted and are implicit to be temper proof. They can always be relied upon during the entire network lifetime.
• Every SN1 is imprinted with a unique code called Manufacturing Code (MC1) and a Hash code .MC1 is used as the private key for the sensor node. It is 64 bits in length. Hash code is used to generate the new keys for the SN1.

We talk about the type of threats-Threat0, Threat1 and Threat2
• Threat 0 is a malicious node that does not had any valid data and wants to start the communication. It can be identified and banned at the time of the validation process of hello packets received by BS1 from each SN1.
• Threat1 is a malicious node that has a valid id but code and keys are invalid. It can be identified and banned at the allocation time of CH1.
• Threat2 node has a valid id and valid code. So, it can be identified and can be banned. Such nodes send alerts against their associates if they are the CH1 in present round otherwise it tells the wrong data to their corresponding CH1. Once BS1 receives any alerts from the network, it asks the concerned node to prove its authenticity by sending its key ring which is already stored with the BS. If the sent key ring does not match to that with BS, the node is destined to be banned.

V. Simulation And Result

5.1 Simulation Scenarios:

At the setup time of the wireless sensor network, some malicious nodes are identified:
Δ Malicious node * cluster head link between CH1 and associate
O Normal nodes O High security nodes O A node sending alert message

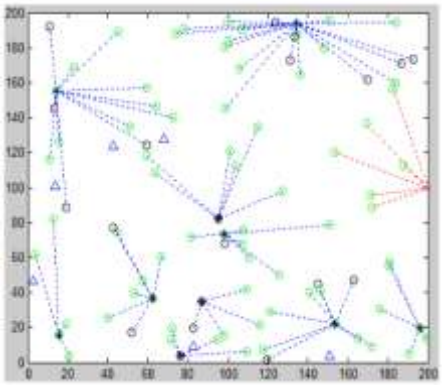

Fig 3: scenario1

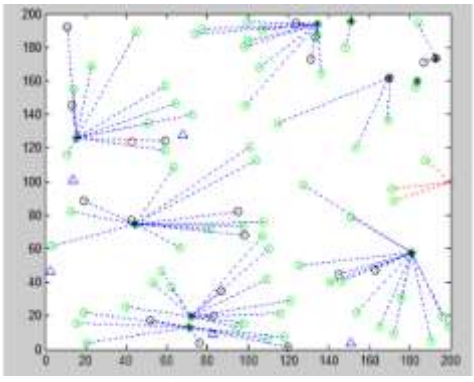

Fig 4: scenario2

In senario1, all malicious nodes are identified with their valid id, code and keys. Black circle shows the high security nodes
In senario2, the malicious node gets correct id, code and keys. The node sends the alert message for other nodes in the network

5.2 Performance Metrics: Network Lifetime :
The time unless the last node is dead is called the lifetime of network. It is the time span from the deployment to the instant when the network is considered non-functional.

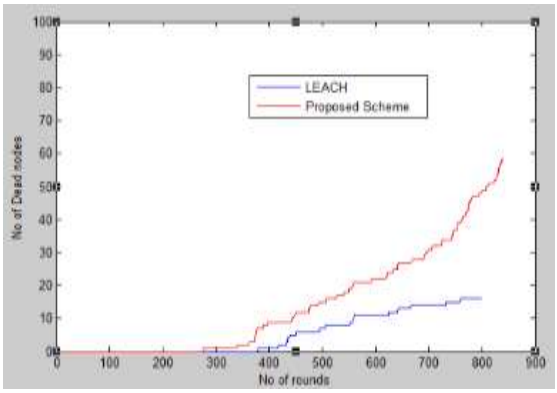

Fig 5: Network Lifetime

VI. Conclusion

In this paper the efficiency of the wireless sensor networks is enhanced by using a new proposed scheme which is employed using O-Leach protocol as the routing protocol for data transmission in the network. A Symmetric key cryptographic management technique had been utilized in order to enhance the security of wireless sensor network. The lifetime of nodes is also enlarged using the above technique, as malicious nodes are banned on initial stage and thus the less power is consumed in network.

References

[1]. Sushma .et. al., "Security threats in wireless sensor networks", International journal of computer Science & Management studies, ISSN: 2231-5268. Vol.11, Issue 01, may 2011.
[2]. Jyoti Attri.et al., "Study on cryptographic Techniques in computer network security'', Asian Journal of Advance Basic science.: 2(3) , 98-102 ISSN (online):2347-4114
[3]. Chun Hu Y. et al. ,"Ariadne: A Secure On-Demand Routing protocol for Ad Hoc Networks", Wireless Networks, Springer Science Business Media, Inc. Manufactured in the Netherlands, 2005.
[4]. Vikash Kumar1.et al., "Wireless Sensor Networks : Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 8, Apr 2014
[5]. Abhishek Pandey. et al., "A Survey on Wireless Sensor Networks security", International journal of computer Application (0975-8887) Volume 3-No.2, June 2010
[6]. Oliveira L. B. et. al, "Secleach - A random key distribution solution for securing clustered sensor network". proceeding of the Fifth IEEE International Symposium on Network Computing and Applications, pages 145–154, Washington, DC, USA, 2006. IEEE Computer Society.
[7]. Oliveira L.B. et.al," SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks", proceeding of the Fifth IEEE International Symposium on Network Computing and Applications (NCA'06) 2006, IEEE.
[8]. Heinzelman W., Chandrakasan Anantha P., Balakrishnan H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii. January 4-7, 2000.
[9]. Kun Zhang et al. "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management" 2008 IEEE Computer Society
[10]. Sahabul Alam .et al ., "Analysis of Security Threats in Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 2, April 2014