PE2A: PUBLIC ENCRYPTION WITH TWO ACK APPROACH TO MITIGATE WORMHOLE ATTACK IN WSN

P. V. Khandare[1], N. P. Kulkarni[2]

[1] *P. G. Scholar, Department of Information Technology, SKNCOE, Maharashtra, India*
[2] *Professor, Department of Information Technology, SKNCOE, Maharashtra, India*

Abstract

Wireless Sensor Network provides a solution for various applications like nuclear power plant, military. This type of application required continuous monitoring. WSN is unprotected by various attacks; wormhole attack is one of among them. In this attack an attacker able to receive a packet from one location and drop it into another location. We propose an algorithm to defend wormhole attack, which is based on public key encryption and acknowledgement based. Proposed algorithm provides secure communication and detects misbehaving nodes.

Index Terms: *Wireless Sensor Network, wormhole Attack*

----------***----------

1. INTRODUCTION

Wireless Sensor Network (WSNs) consists of distributed autonomous small devices that cooperatively monitor environmental or physical conditions in remote and often hostile environment. WSN provides solutions for various applications like nuclear power plant, military applications etc., but now a day WSN can be used in many daily uses, including home automation, healthcare, traffic control or environment monitoring. WSN has several distinguishable characteristics that make them different from previous one wireless network. WSN is generally used in unnoticed areas and have a large number sensor node. These sensor nodes have limited source of energy, memory, communication and computation.

Security is another unique characteristic of WSN; it is an important factor to provide secure and authenticated communication between an authentic node in a critical application. The Basic security services of WSN include authentication, confidentiality, integrity, anonymity and availability. Figure 1 shows the Wireless Sensor Network architecture. It consists of sensor nodes, gateway sensor node and sink or base station. WSN is caused by various types of attacks. WSN based application required continuous monitoring and real time response, hence to provide security in WSN is challenging task.

Wormhole is one of the most severe attack in WSN. In this attack, the goal of an attacker is to drop the packet another location which is not a proper place. By using wormhole attack, the attacker can reduce the performance of the network. We propose an approach which is used to defend wormhole attack in the network. Proposed mechanism use encryption technique, decryption technique. For our better communication we use the public key cryptography technique and 2Ack scheme to find the misbehaving nodes in the network. Data security is provided by using encryption and decryption, the encryption is done by using the public key of the sender and the public key of the receiver. The decryption can be done with the help of the public key of itself that is receiver and public key of the sender. By taking the acknowledgement from two successive nodes we can predict that secure communication is done or not.

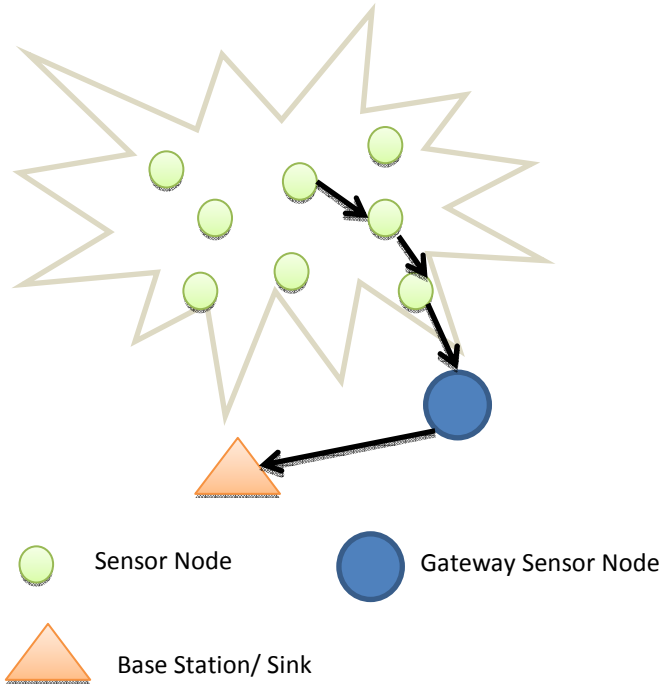

Fig-1: Wireless Sensor Network Architecture

We can say that about wormhole attack, an attacker is transmitting data between two authorized nodes. An attacker records a packet at one location transmit through and releases to another location. By using accurate location verification and clock synchronization we can prevent wormhole attack [1, 6, 8, 11, 13, 15, 16]. Following figure can illustrate the wormhole attack.

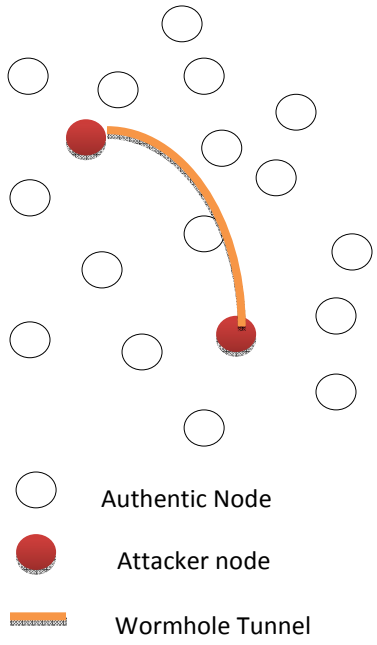

Fig-2: Illustration of wormhole attack.

2. SENSOR NODE ARCHITECTURE AND SECURITY REQUIREMENTS

2.1 Sensor Node Architecture

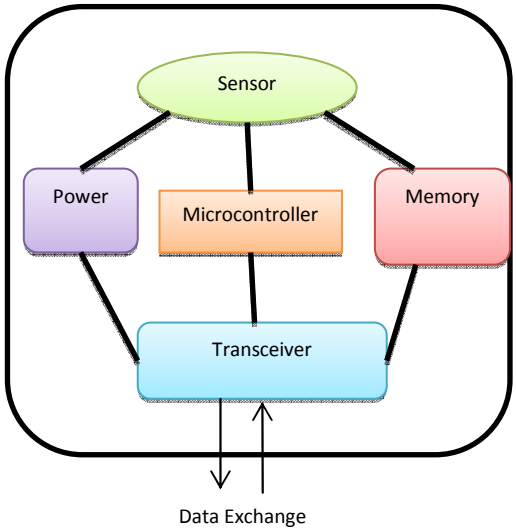

Fig-3: Sensor Node Architecture [1]

Verdonnel describes the sensor node device as the simplest tool in WSN. It consists of elements like sensor, memory, battery, microcontroller and radio tranreceiver. Microcontroller is used to control all task. It is equipped with the memory which is used to store environment sensed data. Battery is energy source for the sensor node device. Figure 3 explain the architecture of sensor node.

2.2 Security Goals or Security Services for Sensor Network

The sensor network operates in an ad-hoc manner, due to these security goals for this type of network cover both those of traditional network and suited to ad-hoc sensor network [2]. Security is an essential factor for every network to defend again security attacks [3]. The security goals are classified as primary goals and secondary goals. The primary goals are also known as standard security goals. Primary goals include authentication, confidentiality, integrity, and availability (CIAA). The secondary goals include data freshness, self-organization, secure localization and time synchronization.. In order to have a secure system the following criteria must be followed [2, 3, 4, 5].

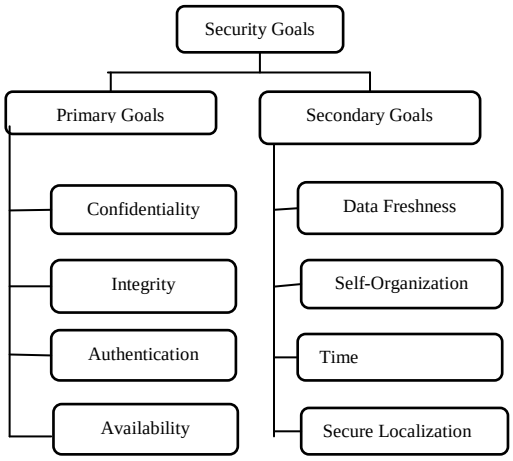

Fig-4: Security Requirement for Sensor Network

1) Authentication:

Authentication gives the consistently best performance of a message identifying its original source [2]. WSN have large amount of nodes in the network. The sensor node collects sensitive data which help to take many decisions. Authentication ensures that the received message is coming from origin [4]. An attacker not only going to modify the packet but also can change the whole packet stream by adding additional packet. Due to this, the receiver should have a decision making process to take decision for received packet is came from authenticate node. During the deployment of networks, authentication is required for many administrative tasks; it allows a receiver to verify that received data is coming from claiming sender. It can be achieved through symmetric or asymmetric mechanisms. To provide a secure communication in hostile environments, it is challenging task to ensure authentication [2, 4].

2) Integrity:

WSN consist of a large number of nodes which communicates with the help of certain communication range. In this type of network adversaries may be present,

hence during transmitting of data, data may be altered or loss by adversaries [6]. Data integrity ensures that reliability of data and it refers to the ability to confirm that message has not been tampered with, altered or changes. Even if the confidentiality of network measures, but there is a possibility that data integrity has been compromised by alterations [2]. The data integrity of the network disturbed, if the attacker is present in the network and inject false data and some undesirable conditions due to wireless channel cause damage [4].

3) Data confidentiality :

Data confidentiality is important for communication in WSN. WSN provides solutions for various types of applications like military, industry etc. Hence data confidentiality is important. An encryption is a standard procedure or approach through which we can get data confidentiality during communication [6]. Data confidentiality is an ability to keep secret communication from an attacker so that communication via the sensor network remains confidential. A sensor node should not make known its data to its neighbor [2] because sensor node stored highly sensitive data like military application [4]. There is need to build a secure channel in WSN for communication purposes. Information of sensor node like identity and its key must keep in encrypted format to protect against various attacks [4].

4) Availability:

Data availability ensures whether a node has the ability to use the resources and whether the network is available for communication. The failure of the base station or cluster head loss data availability. It is an important factor to maintain an operational network [2].

The secondary goals or security services are as follows:

5) Data freshness:

Even if confidentiality and data integrity is maintained but there is a need to ensure that the freshness of the each message [2]. It gives an idea about data i.e. it is recent or old. To ensure about data time stamp, a nonce or other time related counter can be added, which gives idea that no old messages or data replayed that is ensures about data freshness [2, 6].

6) Self-Organization:

Each and every node in the network is independent and flexible through to self-organizing and self-healing according to different versatile environment or conditions. The network should be self-organize to support multi-hop routing and also self-organize to support the trust relation among sensors. There is no particular infrastructure available for sensor network, if there is no availability of self-organization then damage cause it into an attack [2, 6].

7) Time Synchronization:

Most of application based on WSN depends upon some form of time synchronization. Sensor node has a very limited amount of energy, to save energy each sensor node radio may be turned off periodically. Some collaborative type sensor network required group synchronization for applications like tracking applications [2, 6].

8) Secure Localization:

Each sensor node must require location information accurate and automatically [6]. The ability of sensor network will depend on its ability to accurately and automatically locate each sensor in the network. An attacker can easily find unsecured location information by reporting false signal strength, replaying signals [2].

3. RELATED WORK

Ali modirkhazeni, Sadeedeh Aghamahmoodi, Arsalan Modirkhazeni and Nagrneh Niknejad [1] proposed approach to motigate the wormhole attack in WSN. It find the wormhole in network based on HELLO message and RESPONSE message. It uses shared secret key for communication purposes. Dhara butch and Devesh Jinwala[7] proposed a method to detect wormhole in the network. It is based on statistical analysis of sent and received packets. It requires strong synchronization. Gunhee Lee, Dong-Kyoo Kim, and Jungtaek Seo [13] proposed method for mitigation of wormhole in wireless Ad-hoc network. It uses two hope correctness test based on this they mitigate the wormhole in network. Amar Rashid and Rabi Mahapatra [16] proposed a technique to mitigate wormhole in the wireless network. They detect wormhole based on unknown pairwise key or unknown data transmission channel in the network. Jakob Erikson, Shrikanth V.Krisnamurty and Michalis Falutos proposed a TrueLink protocol or defending wormhole in a wireless network.

TABLE- I
COUNTERMEASURES FOR WORMHOLE ATTACK

Sr. No.	Author	Proposed Scheme	Key Used
1	Ali modirkhazeni,Saeedeh Aghamahmoodi,Arsalan Modirkhazeniand Naghmeh Niknejad[1]	Distributed approach to mitigate wormhole attack in Wireless Sensor Network	Shared secrete key
2	Gunhee Lee, Dong-Kyoo and Jungtaek Seo[13]	Mitigate the wormhole attack in wireless Ad-hoc network	Session Key
3	Amar Rashid and Rabi Mahapatra[16]	Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks in Wireless Sensor Networks	Use polynomial key management scheme
4	Jakob Erikson, Shrikanth V. Krisnamurty and Michalis Falutos	Proposed Truelink Protocol	None

5	Phuong Van Tran, Le Xuan Hung, Young Koo Lee, Sungyoung Lee, Heejo [15]	Transmission Time based mechanism	None
6	Dhara Butch and Devesh Jinwala[7]	Detection of wormhole attack in wireless network based on statistics of sent and received packet	None

4. PROPOSED SYSTEM

Wireless Sensor Network consists of a number of sensor node devices which are placed in unnoticed area. WSN is unprotected from various attacks. Wormhole attack is one of attack in WSN. In this attack, an attacker forms tunnel which drop the packets to another location. Here we proposed a mechanism which is used to defend a wormhole attack in the network. It uses public key cryptography and 2Ack scheme. We can find the misbehaving nodes in the network.

4.1 Mathematical Model

In [1], it is assumed that the attacker is not present at the time of neighbour discovery, whereas if attackers are present at time of neighbour discovery and able to get shared secret key.

An attacker with *m* neighbors can send data with the identity of each neighbor node with probability

$$P(A) = 1/m \quad (1)$$

Where, m is the number of real neighbors to attacking node and not able to detect wormhole attack

In proposed algorithm we use public key cryptography as opposed to shared secret key in existing algorithm. In neighbor discovery phase every node lets the neighbor node know its public key. Data Transmitted by a node is as

$$ED= E(K_{Sprivate}, E(K_{Rpublic}, D)) + E(K_{Sprivate}, Di)$$

Where

ED Encryption of data

E is a public key encryption function

$K_{Sprivate}$ is private key of sender node

$K_{Rpublic}$ is public key of Receiving Node,

which eliminated pretending identity of the neighbor node completely even if the attacker in present at time of neighbor discovery

In case of 2ACK,

Let probability of successful transmission as P(S), so probability of successful reception of 2Ack is

P (2Ack) = P (data send successfully)*P (probability successful Acknowledgement)^2

$$= P(s)^3$$

If acknowledgment received less than µ, Then node is the attacker or misbehaving.

4.2 System

Each node in the network has a public key and a private key and every node shared its public key at the time of neighbor discovery. The proposed system is starting with every node, every node sends HELLO message to all nodes. This forwarded message has source address and its own public key, which is broadcasted to all the nodes. To reply this message, every authentic node sent their public key to that node. Suppose when a node P want to send data to Q then P encrypt the data with public key of Q and then again encrypted with the help of the private key of sender that is P. When Q receives the data then it can be decrypted with the help of the public key of the sender that of P and its private key of Q. For the encryption and the decryption purposes we use the ECC algorithm. To check the successful transmission we use 2Ack scheme that are we taking the acknowledgement from two successive nodes in the network. By using this technique we can easily find the misbehaving or malicious node in the network. For the consideration of two next authenticate node we find the path to the base station. If the attacker able to receive messages but he could not able to decrypt messages. With this approach we consider that an attacker cannot be going to do the acknowledgement spoofing attack. If R is successive node then Q forward message to R. Node P is waiting for acknowledgement from Q and R. If P received acknowledgement from Q and R then data transmission is done successfully is assumed by P. If P hasn't received acknowledgement from Q and R then it's considered that Q is a misbehaving node. If acknowledgement is not coming from R then it assumes that R is misbehaving node in the network. Misbehaving node is nothing but node which has only accepted the data but could not forward to next node. Hence sensed data by other nodes cannot receive to base station and loss of data is done. The 2Ack can be used when the data is lost. The proposed approach provides secure communication and finds misbehaving nodes.

5. SIMULATION RESULT AND ANALYSIS

In the setup of Omnet++ simulation, 20 sensor nodes are deployed in the area of 200mX200m.Figure7 shows comparative results for both the systems at time t=200s. Instead of shared secret keys in **our proposed system** we are using public key cryptography for secure communication. It results in an increase in the security of the network.

Table II. Simulation Parameters

Parameter	Value
Simulation time	200 Sec
Simulation area	200 * 200 meter
Number of Nodes	20
Communication Range	Default 50 meter

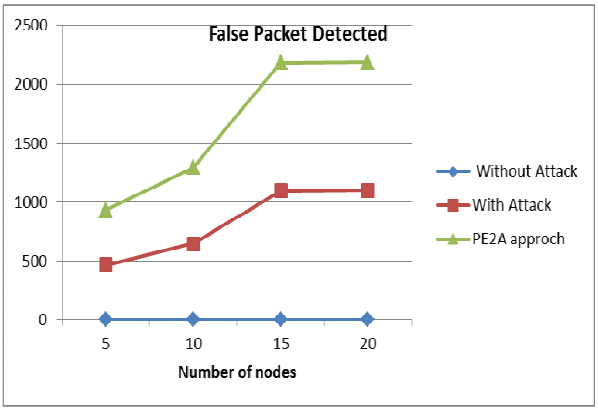

Fig.5 :False packet detected

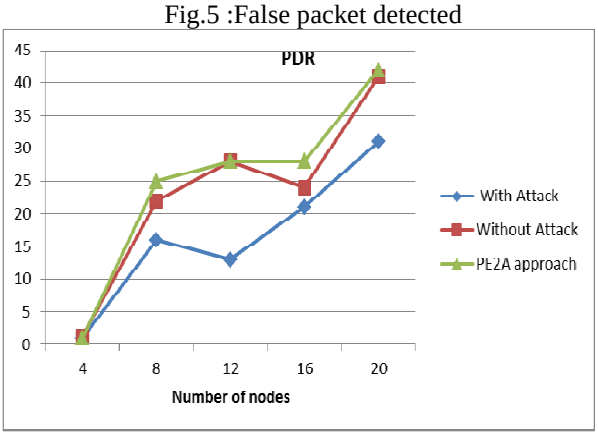

Fig.6 : Packet Delivery ratio

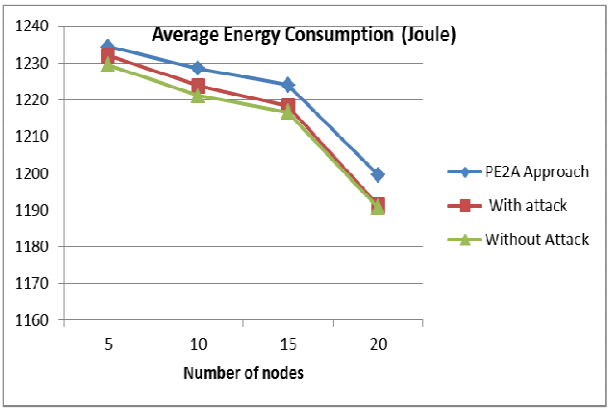

Fig.7 :Energy consumtion in a network

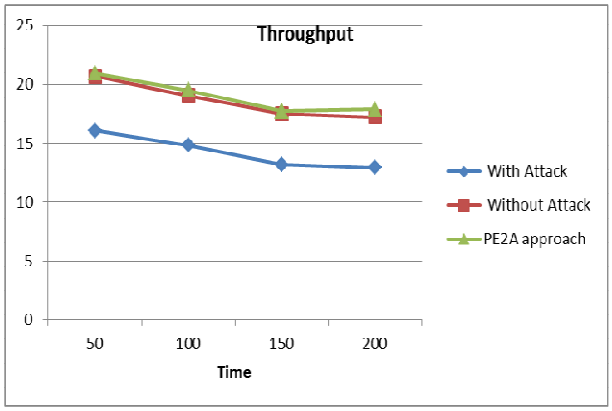

Fig.8: Throughput

CONCLUSIONS

To provide a security in WSN is a challenging task. Here we implement the system to mitigate the wormhole attack in WSN called public key encryption and 2ACK based approach. Our proposed approach provides secure communication. The ratio of proposed approach for received packet is more than the existing system. Using our approach we mitigate wormhole attack in WSN. If this approach is used for WSN then secure communication will be possible.

REFERENCES

[1] Ali modirkhazeni, Saeedeh Aghamahamoodi, Asarlan Modirkhazeni and Naghmeh Niknejad,"*Distributed Approach To Mitigate Wormhole Attack in Wireless Sensor Network* ",2011IEEE , page no. 122-128

[2] Dr. G. Padmavati, Mrs. Shanmungapriya, "*A survey of attacks, Security Mechanism and challenges in Wireless Sensor Network*", International Journal of Computer Science and Information Security (IJCSIS), volume 4 no. 1 & 2, 2009, ISSN 1947-5500, Page no. 291-296

[3] Hind Annahidh, Soha S. Zaghul, "*A Survey on Security Solutions in Wireless Sensor Network*", ISBN: 978-0-9853483, Page no. 94-98

[4] Dr. Banta Singh Jangra, Vijeta Kumavat, " *A Survey on Security Mechanisms and Attacks in Wireless Sensor Network*", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 3, September 2012, Page no. 291-296

[5] Yang Wang, Garhan Attebary, Burav Ramamurty, "*A Survey of Security Issues in Wireless Sensor Network*", IEEE Communications Survey and Tutorials, 2nd quarter 2006, Volume 8, No.2-23.

[6] P. Mohanty, S. Panigrahi, N. Sarma, S. Satapathy, " *Security issues inWireless sensor Network Data gathering Protocols: A Survey* ", Journal of Theoratical and Applied Infromation Technology, 2005-2010 JATIT, Page no. 14-27

[7] Dhara Buch, Devesh Jinwala "*Detection of wormhole attack in Wireless Sensor*", Proc of international

conference on Advances in Recent Technologies In communication computing 2011, Page no. 7-14

[8] Al-Sakib Khan Pathan, Hyung –Woo Lee Choong Seon Hong, " *Security In Wireless Sensor Networks : Issues & Challenges*" Feb 20-22, 2006 ICACT 2006 , ISBN 89-5519-129-4, Page no. 1043-1048R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[9] Xiaujiang Dv, Hsiao-HWACHEN, "*Security In a Wireless Sensor Network* ", IEEE Wireless Communication, August 2008, Page no. 60-66

[10] Abhishek Jain, Kamal Kant, M. R. Tripathy," *Security Solutions For Wireless Sensor Networks* " Second International Conference In Advanced Computing and Communication Technologies, 2012 IEEE, Page no. 430-433

[11] Sanzgiri , Kimaya, " *A Secure Routing Protocol For Ad Hoc Networks* " ,2002, 10th IEEE International Conference, Page no. 78-87

[12] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, "*An Approach To Mitigate Wormhole Attack In Wireless Ad Hoc Networks*",International Conference On Information Security & Assurance, 2008 IEEE, Page no. 220-225.

[13] Marianne A. Azer, Skeriff M.El-kassas, Magdy S. El-soudani, " An Innovative Approach For Wormhole Attack Detection & Prevention In Wireless Adhoc Networks", 2010 IEEE

[14] Amar Rasheed, Rabi Mahapatra, " Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks In Wireless Sensor Networks " ,2009 IEEE, Page no. 216-222

[15] Phoung Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoun Lee, Heejo Lee, "*TTM: An Efficient Mechanisms To Detect Wormhole Attacks In Wireless Adhoc Networks*" 2007IEEE

[16] Vijaya K., "*Secure 2ACK routing protocol in Mobile Ad Hoc Networks"*,TENCON 2008-2008 IEEE Region 10 conference, Page no. 1-7

[17] P. V. Khandare, Prof. N. P. Kulkarni "Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack ", International Journal of Computer Trends and Technology, Volume 4 issue 3-2013, Page no.247-252