Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack

Pravin Khandare [#1], Prof. N. P. Kulkarni[*2]

[#]*Department of Information Technology, SKN College of Engineering*
Pune-41, India

***Abstract*— Wireless Sensor Network provides various applications like military, healthcare etc. These types of applications required a certain level of security. WSN is exposed by various types of attacks; wormhole is one of severe attack on WSN. In wormhole attack, an attacker receives packet from one location pass them through the tunnel and release to them another location. We propose an algorithm which defends wormhole attack in WSN called public key encryption and 2Ack based approach. Proposed approach provides security and finds misbehaving nodes in the network.**

***Keywords*— Wireless Sensor Network, wormhole attack.**

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of a large number of limited sensor devices which communicates through wireless media. In hostile environments like military battlefield, hospital, monitoring nuclear power plant, target tracking required constant monitoring and real time response, the solution to it provided by WSN. It consists of the sensor node device, which integrates a number of microprocessor component into a single chip. The sensor node device consists of elements like sensor, battery, memory, microcontroller and radio transceiver. The microcontroller controls all tasks, memory is used to store the environment sensed data. The battery is the energy source to sensor node device [1, 2].

Many applications based on WSN such as military and healthcare are critical and required a certain level of security. As sensor devices restricted hence security in WSN is challenging task [1, 2]. There are various attacks in WSN like a blackhole, selective forward attack, Sybil attack etc., a wormhole is one of severe attack on WSN, in which an attacker form a tunnel and its releases data into another location [3, 4, 5, 6, 7]. To prevent wormhole attack, we propose "public key encryption and 2Ack based approach to defend wormhole attack" in WSN. In the proposed approach, data is encrypted with the public key of the receiver and only decrypted by receiver private key, in this way security is provided. Data security is a more important factor than data are transreceives between two authentic nodes. A public key encryption system has permit nodes to transmit data to one another in a secure way. Public key encryption has a number of advantages over a symmetric key system, for example DES. By using 2Ack we can find misbehaving nodes which are only received data but cannot forward to next node. The rest of the paper is organized as follows: Section II discusses about the attacks in WSN. In Section III we discuss about different approaches to defend wormhole attack. Section IV explains proposed system and finally the Section V concludes the paper.

II. SECURITY ATTACKS IN WSN AND CLASSIFICATION OF WORMHOLE ATTACK

A. Attacks in WSN

Selective forwarding attack:

In this attack, an attacker may refuse to forward certain messages and simply drop them, ensuring that they do not propagate any further. The solution to this type of attack is the sequence number of each packet checked properly. Addition of data packet sequence in packet header can reduce this attack [3].

Sybil Attack:

In this attack, an attacker creating fake identities of nodes which is located within communication range. In simple word we can say that an attacker can appear in multiple places at the same time. Authentication and encryption techniques can prevent this attack [3, 4, 6].

Sniffing Attack:

This attack is related to military or industrial secrets. An attacker is located in proximity of the sender grid to capture data. We can prevent this attack by using proper encryption techniques for communication purposes [3].

HELLO flood Attack:

The main goal of this attack is a waste of sensor node energy in networks. An attacker sends HELLO packet to all nodes which are within a communication range, authentic nodes give reply this messages and waste their energy. Due to this Performance of the network is reduced; the solution to this attack is verifying the bidirectionality of link before using them [3, 4].

Data integrity Attack:

The goal of this attack disturbs the sensor network normal operation by injecting false data. Use of asymmetric system or use of digital signature can prevent acknowledgement spoofing attack [3].

Acknowledgement Spoofing:

The goal of this attack is convincing sender that weak link is strong or dead or disabled node is alive and sent packets are lost [3].

Energy Drain Attack:

In this attack, an attacker can do attack through the compromised node. The attacker injects fabricated report on network and generates traffic in the network. It causes false alarm and waste real world response effort, due to this sensor node in network are destroyed which is aim of an attacker [3].

Spoofed, Altered or Replayed Information:

In this attack, an attacker's target routing information exchanged between two authenticate nodes. It creates routing loops, attract or repel network traffic. The solution to this attack is authentication in a network that is receiver only accept routing information from authenticate or valid sender [3, 4].

Blackhole Attack:

In this, an attacker does attack through malicious node, which shows which shortest route is and attract entire traffic through it. This attack separates nodes from sink [3, 4, 7].

Node Replication Attack:

In this attack, an attacker tries to mount several nodes with the same identity at different places in the network. This clone node tries to disturb normal operation. It can be detected by verifying the identities of the node by trustworthy node [3, 4].

Sinkhole Attack:

In this attack, an attacker tries to attract all traffic from a particular area through malicious node. Use of unique key for neighbor node discovery or use of spread spectrum communication can prevent this attack [3, 4, 7].

Wormhole Attack:

In simple word we can say that, malicious node is transmitting data between two authentic nodes. An attacker records packet at one location transmit through a tunnel and releases to another location. By clock synchronization and accurate location verification we can prevent wormhole attack [3, 4, 8, 9, 10, 11, 12].

B. Classification of Wormhole Attack

In wormhole attack, a malicious attacker receives packet from one location of network and pass them through a tunnel and release to another location. Wormhole attack is classified based on different criteria. Khalil is classified on the technique which is used to launch wormhole attack. Classification made by Khalil is as wormhole using encapsulation, wormhole using out of band channel, wormhole with high power transmission, wormhole using a packet relay and wormhole using protocol deviation. Graaf classifies attack as active and passive attacks. Inactive attack end point of wormhole tunnel is from the network. In the passive attack end points don't belong to the network. Wang classified the wormhole attack in closed, half opened and open attacks. These classifications differ from each other as they made based on different criteria [1].

III. RELATED WORK

Ali modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni, and Nagrneh Niknejad [1] proposed approach to mitigate the wormhole attack in Wireless Sensor Network. Some assumptions are made; two neighbor nodes have 'secret key' which has been shared after deployment of network and cannot captured by an attacker. This approach starts with every node, say C sends message to all one hope neighbors. This message is encrypted with a secret shared key between each node. We can say that Kcd. The encrypted message contains the ID of the sender, a random number as nonce and message digest. They used MD5 algorithm to generate hash values. When D received HELLO message, it decrypted by using shared key, the sender of a message and compute the hash value of 'sender ID' concatenation of nonce. If the result is matched then HELLO message is authenticated from an authorized neighbor. The RESPONSE message is used to send back. It contains the identity of 'sender ID', nonce under a simple function F and a message digest of sender ID concatenation of 'Fnonce'. RESPONSE message decrypted by node C and verified node D through authenticate steps. It checks the hash value of 'IDd' and 'Fnonce' is similar to hash value in RESPONSE. Secondly, it checks for value of Fnonce. These two tests are successfully achieved then the neighbor is authenticated. In this way mitigation of wormhole attack in WSN can be achieved.

Dhara Butch and Devesh Jinwala [2] proposed method to detect a wormhole attack in WSN. This approach is based on analysis statistics of sent and received packets by each node in the network, with to generate a unique key between node and base station. It includes, mainly two phases that are, key generation phase and detection of the wormhole. In the first phase, it derives a key for data protection and in second phase detect wormhole. In this, each node finds its geographical location first. Each node gets information about one hope neighbors by using HELLO message and calculate four values Ka, Kb, Kc and Kd. Where Ka is the total numbers of neighbors, Kb is the sum of neighbors ID's, Kc is the X coordinate of the node and Kd is the Y coordinate of the node. By applying the multiplicative based function of these four keys an Intermediate Key IK is derived. This same information like Ka, Kb, Kc, Kd and Ik about all nodes is known to 'n' to base station. The next step is the distribution of the unique key, it is done by the base station. The Base station broadcast message which has two fields i.e. Intermediate Key and unique ID. If the unique ID's for all the nodes broadcasted then base station broadcast MSG_OK, by receiving this message nodes starts normal communication. In wormhole detection phase, it focuses on number of sending and received packets from and to each of the nodes in the network by checking the authenticity of gathering data.

Statistics are maintained by two tables at each node A and B, when A sent packet to B then the counter value of A incremented in sending value table. If A received packet then received packet counter is increased. It required synchronization, this can be done with the help of START and STOP message. Communication can start, only when the duration is bounded by messages and broadcasted by the base station, sometime duration is in between STOP and next START message so that each transmitted message may reach to destination before next interval start. When table's data are sent to base station it can be altered by malicious node, for secure communication data of tables is encrypted with the help of the AES algorithm. During this process unique ID allocated to each node in the initial phase used as key for AES. Total number of packets sent to node n with a total number of neighbors Na and total number of packets received by node i from n nodes compared. The total number of sent packets to neighbor A to destination node B must be equal to the total number of packets received by its one hope neighbor i.e. B. If this value not satisfied then wormhole can be detected.

Gunhee Lee, Dong-Kyoo Kim and Jungtaek Seo [8] proposed method to mitigate the wormhole attack in Wireless Ad-hoc network. It is an effective wormhole attack defense method that can properly detect wormhole attack and respond to them. Each node in the network maintains its neighbor information by using each node can identify replayed packet that forwarded by attackers. It worked in four stages that are one hope or two hop neighbors, building a neighbor list, detecting wormhole and responding wormhole. In first step focused on indication that check whether a node that forward a packet is a real neighbor or not because, it's not required accurate time synchronization and no monitoring burden that checks every packet. It gathers two types of neighbor such as one hope neighbor and two hop neighbors. The second phase is building a neighbor list process, each node newly joined in network broadcast an announcement being valid until next two hope nodes. When a node receives broadcast message, it forward message to its neighbors if the TTL value is 1. Every node which receives announcement should return acknowledgements to the new node. When acknowledgement returns back to new node then it registers responder as neighbor of it only if acknowledgement is valid. During this process it will set up a new session key for further communication. In detecting wormhole phase, it performs two tests for packet such as one hope correctness and two hop correctness. In fourth stage that is responding to wormhole, these two tests are not successful then wormhole exist in route.

Amar Rasheed and Rabi Mahapatra [10] proposed a technique to minimize wormhole attack in Wireless Sensor Network. Some assumptions are considered, it assumed that each physical device has only one radio and it's incapable of sending or receiving on more than one channel. When network established, every node is reloaded with a share of a randomly selected subset of polynomials and Mobile Sink [MS] is loaded with a randomly selected subset of polynomials. All sensor nodes including MS have radios tunnel preselected common channel called discovery channel. The MS sent a beacon message over discovery channel, it has MS ID. All nodes in the network use polynomial key management scheme and establish pair wise key with Mobile Sink. Mobile Sink assign channel F to every node in the network which has pair wise key say Ka and sent an encrypted message assigning frequency F to node which have a corresponding Key ‘ Ka’. This frequency F used to transmit data. In this approach if Mobile Sink receives data from node containing the unknown pair wise key or unauthenticated data transmission channel in the network then wormhole can be detected.

Jakob Erikson, Shrikanth V. Krishnamurty and Michalis Faloutos [11] proposed a countermeasure for wormhole attack in a wireless network. They proposed TrueLink Protocol for defending wormhole attack. It checks bidirectionality of links. It enables a node to verify adjacency of apparent neighbor. It uses a combination of timing and authentication. It uses together with secure routing protocol. A TrueLink protocol performs link verification between two nodes say A and B in two phases that are rendezvous phase and authentication phase. In the first phase ‘A’ and ‘B’ exchanges nonce’s αB and βA, where subscript shows node that generated nonce. This exchange proves adjacency of responding node through the use of strict timing constraints, due to this only a direct neighbor is able to respond a time. In the second phase ‘A’ and ‘B’ each sign and send a message (αB, βA), by mutual authentication themselves gives origin of their respective nonce. Due good time synchronization in first phase makes TrueLink immune to capture and reply style wormhole attack and strictly limits range of attacks based on bit by bit or “cut through” forwarding. In this way TrueLink provide countermeasures to wormhole attack in a wireless network.

Phuong Van Tran, Le Xuan Hung, Young Koo Lee, Sungyoung Lee and Heejo[12] proposed a transmission time based mechanism(TTM) to detect wormhole attack. It has a four stage AODV route setup, TTM, sending RTT value back to the source node. In phase one, when a node tries to send data to another node and there do not exist a valid route in a table then it broadcast a route request packet (RREQ). By receiving this message node setup a reverse route to the source node in its routing table. In a second phase, when a node establishes a path to another node, it tries to check whether there a wormhole link in that path or not by calculating every RRT (Round Trip Time) between two successive nodes along the path. In this phase each node establishes its path and calculate RRT between it and destination node. In the third phase, every intermediate node along the path needs to send the RTT between them and destination back to the source node with a RREP. The fourth phase is used to detect wormhole, based on the RREP threshold value they detect wormhole attack.

IV. PROPOSED SYSTEM

In wormhole attacks, an attacker tries to establish tunneling link in Wireless Sensor Networks. Different methods are proposed by the different researcher for detection and prevention of wormhole attack.

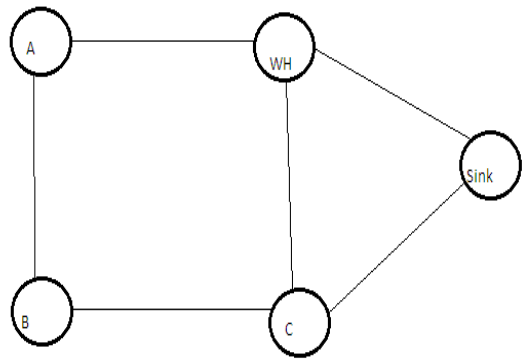

Fig.1: Illustration of Wireless Sensor Network

Fig. 1 shows all valid or authenticate nodes and the malicious node in WSN. A, B and C are authentic nodes in the network, where WH is a malicious node in the network. Sink collect all the data in the network. The actual neighbors of 'B' are A and C, similarly actual neighbors of 'C' are 'B' and sink. A has neighbor B which is an authentic node in the network. Where WH is malicious node, tries to make a tunnel in networks. For our proposed system we consider some simulation parameter, that are the number of nodes, the number of attackers or misbehaving nodes, network area and data packet rate. For our simulation result we vary the number of nodes like 10, 20,50,100. The number of attacker consideration is 1%, 2%, 5%, 10%. Similarly consider data packet rate 1pps, 2pps, 5pps.

A. Mathematical Model

In [1], it is assumed that the attacker is not present at the time of neighbor discovery, whereas if attackers are present at time of neighbor 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

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

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.

B. System Assumptions

It has been assumed that each node has a set of public key and private key. Also assumed every node shared his public key with another node at the time of neighbor discovery. Data collected by each node is sent to authenticate neighbor. Data should be forwarded with constant bit rate.

C. System

The proposed method starts with every node in network, say 'A'. It sends a HELLO message to the all one hope neighbors in the network. This broadcasted message contains source address and its own public key, which is broadcasted to all nodes. In response to this message, every authentic neighbor sent their own public key to 'A'. Receiver public key of one hop neighbor sent in the encrypted message format. This message contains source ID, public key of 'B' encrypted with the public key of A and destination address.

When the node 'A' want to send data to 'B' then 'A' encrypt data with public key of 'B' and this data again encrypted with the private key of sender i.e. 'A'. When receiver 'B' receives data from the sender 'A' then first 'B' decrypt data with public key of sender A and remaining data is decrypted with its own private key. In this way secure communication is done. For encryption and decryption purposes we use the RSA technique. To check data is reached to authenticate nodes we propose 2Ack scheme. By using 2Ack scheme we can find misbehaving node. In this scheme we take acknowledgment from one hope and two hop nodes.

For consideration of next two nodes we calculate a route toward the sink node and maintain information for route selection. Fig. 2 shows the flow of the proposed system. If attacker got messages from authenticate node, then it do not forward to the next node and tries to drop them into another location. By using 2Ack scheme we can prevent this by taking acknowledgments from next two nodes. If the malicious node able to accept messages but he could not able to decrypt messages. Our proposed 2Ack scheme is able to detect misbehaving or malicious node in networks. Fig. 3 shows illustration of 2Ack.

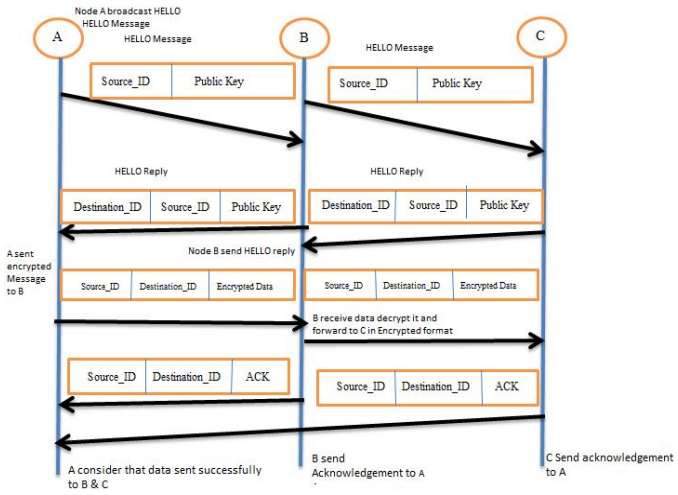

Fig. 2: Flow of proposed system

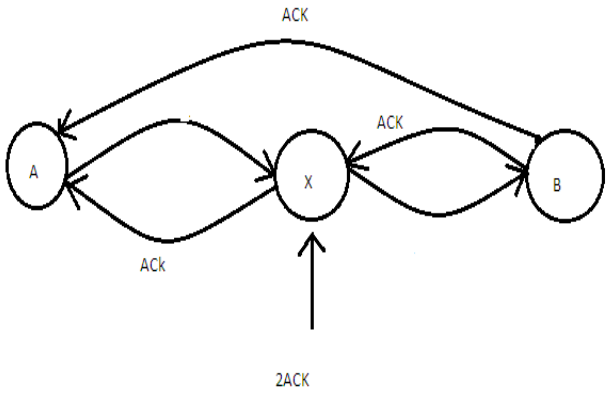

Fig. 3: Illustration of 2Ack

In this method we assume that attacker not going to spoof acknowledgement. If A sends message to X, then X only receives messages and do not forward to next authenticate node i.e. B. A is waiting for acknowledgement from X and B. If B receives the message from X then it sends two acknowledgement to node A and X, then A conforming that data forwarded successfully to next two authenticate nodes. If A cannot receive acknowledgment from X and B then it assumes that X is only receiving information and it do not forward to next node. In this way we find that X is a misbehaving node in the network. If X sends an acknowledgement to A and B does not send acknowledgement to node A then it assumed that B is a misbehaving node in the network. In this way we can determine all misbehaving nodes in the network.

D. Proposed Algorithm

Begin
INPUT: Encrypted Message
1: If A sends message to X
2: If X receives the message and forward to B
3: then B sends an acknowledgement to A
4: X forward acknowledgement to A
5: Node A consider that message forwarded successfully
6: Else
7: If X sends an acknowledgement to A
8: B do not send acknowledgement to A
9: Node A classified to B as a misbehaving node in the Network
10: Else
11: If X does not send acknowledgement to A
12: If B does not send acknowledgement to A
13: then A classified as X as a misbehaving node in networks
14: End.

We can use this 2Ack when a packet is lost. By using proposed scheme we provide secure communication and prevention from wormhole attack. The advantages of our proposed system are,

- It provides a secure communication
- An attacker or misbehaving node easily detected.

The disadvantages of our proposed system may be are

- Energy consumption may be more
- It will require more time

V. CONCLUSION

In this paper, we explained various attacks in WSN, classification of wormhole attack and various approaches for wormhole attack. Our proposed approach that is public key encryption and the 2ack based approach provides secure communication in WSN and defend it from wormhole attack. This approach will be implemented by using OMNET++ and Castalia framework. This approach will be suitable for Wireless Sensor Network.

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] 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

[3] Prabhudatta Mohanty, Sangram Panigrahi, Nityananda Sharma and Siddhartha Sankar Satapathy,"*Security Issues In Wireless Sensor Network Data Gathering Protocols : A Survey* "Journal of Theoretical & Applied Information Technology 2005-2010 JATIT, Page no. 14-27

[4] 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.

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

[6] 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

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

[8] 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.

[9] 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

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

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

[12] 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

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