International Journal of Technology and Engineering System (IJTES)
Vol 7. No.4 2015 Pp. 420-426

available at : www.ijcns.com
ISSN: 0976-1345

DETECTING STRUCTURE-BASED SYBIL NODES USING SYBIL BELIEF

PRABAVATHI.K and SANTHIYA.S
UG Students,
Department of CSE M.R.K Institute Of Technology,Kattumannarkovil Tamilnadu, Indi

ABSTRACT

Sybil attacks are a fundamental threat to the security of distributed systems. Recently, there has been a growing interest in leveraging social networks to mitigate Sybil attacks. However, the existing approaches suffer from one or more drawbacks, including bootstrapping from either only known be nignor known Sybil nodes, failing to tolerate noise in their prior knowledge about known benign or Sybil nodes, and not beings calable. In this paper, we aim to overcome these drawbacks. Toward this goal, we introduce SybilBelief, a semi-supervised learning framework, to detect Sybil nodes. Sybil Belief takes asocial network of the nodes in the system, a small set of known benign nodes, and, optionally, a small set of known Sybilsasinput. Then, SybilBelief propagates the label information from the known benign and/or Sybil nodes to the remaining nodesin the system. We evaluate SybilBelief using bothsynthetic and real-world social network topologies. We show that SybilBeliefis able to accurately identify Sybil nodes with low false positive rates and low false negative rates. Sybil Belief is resilient to noise in our prior knowledge about known benign and Sybil nodes. Moreover, SybilBelief performs orders of magnitudes better than existing Sybil classification mechanisms and significantly better than existing Sybil ranking mechanisms. Index Terms— Sybil detection, semi-supervised learning, Markov random fields, belief propagation.

I . INTRODUCTION

SYBIL attacks, where a single entity emulates thebehaviorof multiple users, form a fundamental threat to the securityof distributed systems [1].

Example systems include peer-topeer networks, email, reputation systems, and online socialnetworks. For instance, in 2012 it was reported that 83 millionout of 900 million Facebook accounts are Sybils [2]. Sybilaccounts in online social networks are used for criminaactivities such as spreading spam or malware [3],stealingother users' private information [4], [5], and manipulating webearch results via "+1" or "like" clicks [6].raditionally, Sybil defenses require users to present trustedidentities issued by certification authorities. However, suchapproaches violate the open nature that underlies the successManuscript received December 17, 2013; revised February 6, 2014 andMarch 31, 2014; accepted April 4, 2014. Date of publication April 11, 2014;e of current version April 30, 2014. This work was supported in part byntel through the Intel Science and Technology Center for Secure Computingnd in part by the Swiss National Science Foundation under Grant 138117.The associate editor coordinating the review of this manuscript and approvingit for publication was Dr. AthanasiosVasilakos.N. Z. Gong and M. Frank are with the Department of Electrical Engineeringd Computer Science, University of California at Berkeley, Berkeley, CA94720 USA (e-mail: neilz.gong@berkeley.edu;mail2mf@gmx.de).. Mittal is with the Department of Electrical Engineering, PrincetonUniversity, Princeton, NJ Color versions of one or more of the figures in this paper are availableonline at http://ieeexplore.ieee.org.0.1109/TIFS.2014.23169 75of these distributed systems [7]. Recently, there has beengrowing interest in leveraging social networks to mitigateSybil attacks [7]–[15]. These schemes are based on the observation that, although an attacker can create arbitrary Sybilusers and social connections among themselves, he or shcan only establish a limited number of social connectionsto benign users. As a result, Sybil users tend to form a community structure among

themselves, which enables a largenumber of Sybil users to integrate into the system. Notethat it is crucial to obtain social connections that representtrust relationships between users, otherwise the structure-basedSybil detection mechanisms have limited detection accuracySee Section II-A for more discussionsHowever, existing structure-based approachessufferfromone or more of the following drawbacks: (1) they can bootstraprom either only known benign [8]–[10], [12] or known Sybilnodes [14], limiting their detection accuracy (see Section VI),2) they cannot tolerate noise in their prior nowledgeaboutkown benign [13] or Sybil nodes [14], and (3) they renotcalable [7]– [12].To overcome these drawbacks, we recast the problem ofinding Sybil users as a semi-supervised learning problemwhere the goal is to propagate reputations from a small setf known benign and/or Sybil users to other users alongthe social connections between them. More specifically, wefirst associate a binary random variable with each user in the system; such random variable represents the label (i.e., benignor Sybil) of the user. Second, we model the socialnetworMarkovRandoField, which defines a joint binary random variables. Third, given a set of known benignand/or Sybil users, we infer the posterior probability of a userbeing benign, which is treated as the reputation ofthe user. Foefficient inference of the posterior probability, couple ouframework with Loopy Belief Propagation [16], an iterativelgorithm for inference on probabilistic graphical models.We extensively evaluate the influence of variousfactorsincludingparametersettings in the SybilBelief, the numberof labels, and label noises on the performancofSybilBeliefFor instance, we find that SybilBelief is relatively robust toparameter settings, SybilBelief requires one label per community, and SybilBelief can tolerate 49% of labels to be incorrectin some cases. In addition, we compare SybilBelief with stateof-the-art Sybil classification and ranking approaches on realworld social network topologies. Our results demonstrate that

SybilBelief performs orders of magnitude better than previous Sybil classification mechanisms and significantly better

- than previous Sybil ranking mechanisms.

  Finally, SybilBelief 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].
- 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].
- 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: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].
- 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].
- 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].

1.1.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 passive attack endpoints are not 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].

II .RELATED WORK

Ali modirkhazeni, SaeedehAghamahmoodi, ArsalanModirkhazeni, and NagrnehNiknejad [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 DeveshJinwala [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 calculates 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.

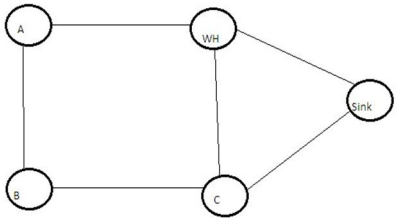
Gunhee Lee, Dong-Kyoo Kim and JungtaekSeo [8] proposed method to mitigate the wormhole attack in Wireless Ad-hoc network. It is an effective wormhole attack defense method that can properly detect wormhole attack and respond to them. Each node in the network maintains its neighbor information by using 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 checks whether nodes 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 MichalisFaloutos [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, Sungyong Lee and Heejo Lee [12] proposed a transmission time based mechanism (TTM) to detect a wormhole attack in networks. This detects wormhole attack using route setup procedure by the transmission time between two successive nodes along setup path. Wormhole attack is determined based on transmission time between two malicious nodes. This scheme works in four phases AODV route setup, Transmission Time based mechanism, sending the RTT value back to the source node and wormhole detection. During AODV procedure when the node 'A' wants to communicate B then it will check route in the table. After receiving RREQ at B first



time set up a reverse route to source node in its routing tables. If the B node is the destination or has a valid route to destination, it will send a reply back to A. At a transmission time based mechanism, when a node set up route to other nodes, if check whether their wormhole link or not by calculating RTT (Round Trip Time) between two successive nodes along route. Each node in the network setup route which computes RTT between it and destination and send back this value to source node and identify wormhole on RTT between two malicious neighbors or two wormhole links considered higher than between two authenticate neighbors. In the third phase, every intermediate node in route need to send RTT between them and destination back to the source node. In case to reduce overhead, after receiving a RREP, the intermediate node will calculate the RTT and send the result

III . 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.

Figure1. Illustration of Wireless Sensor Network

Figure 1 show 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. 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, and 100. The number of attacker consideration is 1%, 2%, 5%, 10%. Similarly consider data packet rate 1pps, 2pps, 5pps.

3.1.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 (KSprivate, E (KRpublic, D)) +E (KSprivate, 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.

3.2. 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.

3.3.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. Figure 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. Figure 3 shows illustration of 2Ack.

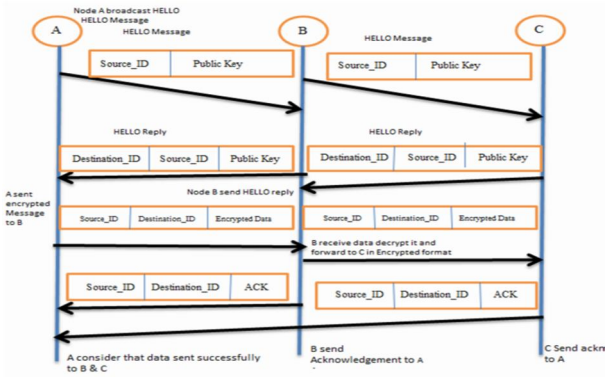


Figure2. Flow of proposed system

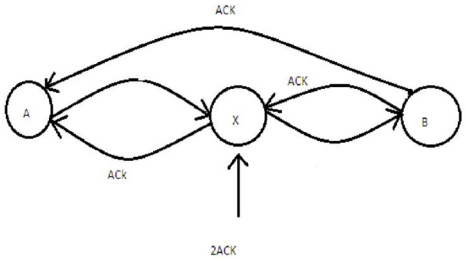


Figure3. Illustration of 2Ack

By using this method we can find malicious nodes or misbehaving nodes in WSN. Here we take two acknowledgements from one hope and two hop neighbors toward the sink node to check to check whether node send and receive messages in the network.

Here A and B are authenticate nodes, where X is misbehaving node, which is only receive data and do not forward data to next authenticate node. To detect this misbehaving node we used 2ACK scheme.

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 acknowledgements 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.

3.4.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 can be easily detected.

The disadvantages of our proposed system may be are

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

IV .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 provide 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, SaeedehAghamahamoodi, Asarlan Modirkhazeni and NaghmehNiknejad, "Distributed Approach To Mitigate Wormhole Attack in Wireless Sensor Network ",*2011IEEE* , page no. 122-128

[2] DharaBuch, DeveshJinwala, "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] PrabhudattaMohanty, SangramPanigrahi, Nityananda Sharma and Siddhartha SankarSatapathy,"*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 ChoongSeon Hong, " Security In Wireless Sensor Networks : Issues & Challenges" Feb 20-22, 2006 ICACT 2006 , ISBN 89-5519-129-4, Page no. 1043-1048

[5] XiaujiangDv, 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 " , *10th IEEE International Conference2002*, Page no. 78-87

[8] Gunhee Lee, Dong-kyoo Kim, JungtaekSeo, "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, SkeriffM.El-kassas, Magdy S. Elsoudani, " 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] Jakob Erikson, Shrikanth V. Krishnamurthy, Michalis Falotsos, "TrueLink : A Practical Countermeasure to the Wormhole Attack In Wireless Networks",*2006 IEEE* Page no. 75-64

[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