Threshold based scheme for isolation of Wormhole Attack in WSN

[1]Jasjit kaur, [2]Pratibha

[1]P.G. Student, [2]Assistant Professor
Department of Computer Science & Technology,
Shri Sukhmani Group of Institute, Derabassi, Mohali, India

***Abstract*: Out of many attacks in wireless sensor network, the wormhole attack is pretty dangerous one as it is launched using two pairs of malicious nodes with create a tunnel by skipping few nodes in between source and destination node. The existing scheme considers the wormhole attacks when there are no intermediate nodes present between destinations. This technique is suitable for scenarios where the path length between source and destination is two hops only. This scheme cannot be used for networks with layer hops between source and destination node. In this research work, we are proposing a threshold based scheme for the detection and isolation of malicious nodes in the network. The malicious nodes are responsible to trigger wormhole attack in the network. As per hop delay is already calculated in the network and node which is increasing the per hop delay than defined value is detected as the malicious node. When the malicious node is detected from the network then the source node will send alert message to each node in the network. When the node receives the alert message, it will remove the malicious node from the path. The technique is efficient in terms of complexity and also various congestion values are included for the detection of malicious nodes. In this phase, the malicious nodes get isolated from the network with the approach of multipath routing. The sensor nodes which increase per hop delay is detected as the malicious nodes. The proposed technique is implemented in NS2 and simulation results shows that proposed technique performs well as compared to other techniques.**

***Index Terms*: Wireless Sensor Network, WSN Security, Wormhole Attack, Availability**

I. INTRODUCTION

The wireless sensor network (WSN) can be described as a combination of various sensing devices or nodes for getting the information about the contiguous situations of a particular area [1]. Nowadays, wireless sensor networks are being used in various applications. These networks can perform several tasks like sensing, processing and sharing of information inside the areas. The wireless sensor network deploys the monitoring area for the random distribution of sensor nodes within the area. Because of the broad and unfriendly applications of wireless sensor networks, several issues raise.

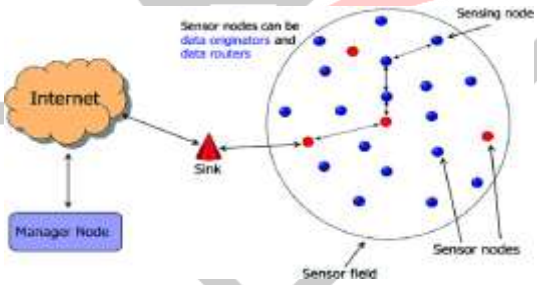


Figure 1.1 Wireless Sensor Network

Due to the small size, these sensor nodes contain only limited battery energy. Wireless sensor networks are positioned in subversive applications. The activities of these regions cannot be monitored because of their inaccessibility for human beings. The nodes deployed in these kinds of areas are more costly than the nodes deployed in worldly regions. The multimedia sensor networks install various microphones and cameras inside them with inexpensive sensor nodes. Larger bandwidth, power and quality of service are some important factors necessary for the appropriate processing of information. In auditory areas, sensor nodes are placed for the deployment of networks in order to create sparse environment. The wireless sensor network faces several constraints such as signal fading, delay and propagation [2]. The proper distribution of network within the definite region is necessary for the collection of information. In order to perform general scrutiny, the monitoring of such regions is imperative in mutual way for the collection of whole applicable information [3]. Aggregation and base station are the two significant mechanisms occurring inside the wireless sensor networks. The data is gathered from the sensor nodes present around the areas. This data is transferred to other nodes. These nodes forward this information to the dominion. The information sharing carried out inside wireless sensor networks is defenseless and not confidential. This is due to the fact that these networks are positioned in hazardous areas with only minimum amount of reserves. The employment of security practices inside these networks is very tricky. But, security is extremely imperative for the proper processing and transmission of data. Because of their properties, these networks face several issues in terms of security.

1.1 Security Requirements in Wireless Sensor Network

The security of wireless sensor networks is extremely essential. For this purpose, some necessities should be kept in mind. The sensor node needs several kinds of surrounded resources inside it for ensuring the complete safety of extremely responsive information. The performance keeps this network lively. A malicious node can easily trigger attack within these networks because of some susceptibilities and occasions. The clients can go through huge loss because of these attacks.

A. **Data Confidentiality** This property can be described as a procedure using which data can be concealed absolutely and does not remain visible to opponents. The information can be made absolutely imperceptible with the help of a secret key for the encoding of information. Merely authorized users can assist in the importation of information. A number of essential dynamics related to the secrecy are needed to be considered in wireless sensor networks.

B. **Data Authentication** In these networks, any types of illegitimate elements can be blocked. At the same time, the authentic nodes pay attention to identify any types of illegal nodes or clients. The attainment of information from a precise source is necessary. Also, the target must be guaranteed to be a fraction of communication for assuring that the information is not transmitted to any illegal users [4].

C. **Access Control** This property ensures the inaccessibility of information to illegal consumers. This feature does not allow any type of illegal interference within the network.

D. **Availability** The whole cost of networks is enlarged due to the modification of conventional encoding algorithms within wireless sensor networks. Because of the existence of several techniques, the modification of code is required so that it can support the code reutilization.

1.2 Attacks on WSN

A number of intrusions may occur at different layers of the network as all these layers perform in dissimilar way and execute dissimilar operations. In these networks, a number of routing protocols are involved which do not comprise any security mechanism. Thus, the malicious can easily break the security of these networks. Different kinds of attacks or intrusions recognized in every layer of the network are given below:

1.2.1 Physical layer attacks

Congestion: As the radio frequencies experience intrusion within the sensor nodes, this result in the generation of a direct attack named as congestion. The denial-of-service circumstances are experienced within the network due to the incidence of this kind of intrusion.

Tampering: This kind of intrusion conciliates the node absolutely. This attack causes extremely hazardous affects. This attack modifies the sensor nodes. The occurrence of this attack can destroy the whole network.

1.2.2 Link layer attacks:

Collision: This intrusion occurs when the channel intercession experiences neighbor-to-neighbor information sharing inside the link layer. The whole packet disrupts when collisions happen in any area of the positioned network. Thus, in this situation packet should be transmitted again due to the occurrence of single bit error.

Exhaustion: The occurrence of interrogation intrusion exhausts the battery power. The power consumption is extremely high in this situation due to the retransmission of packets. This causes absolute exhaustion of the battery of the sensor nodes [5].

1.2.3. Network layer attacks:

Hello flood attack: Higher communication energy is necessary for the transmission of hello packets so that adjacent can be revealed during this kind of intrusion. The malicious creates a delusion inside the network which depicts that a node is neighbor of other nodes. Thus, the incorporated routing protocol will be absolutely interrupted and larger number of intrusions may occur at this time. The attacker node comprises elevated radio communication rage and processing energy because of which different sensor nodes obtain hello packets. These nodes are partitioned in big regions.

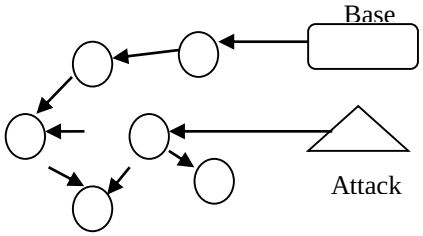


Figure 1.3: Attack broadcast packets

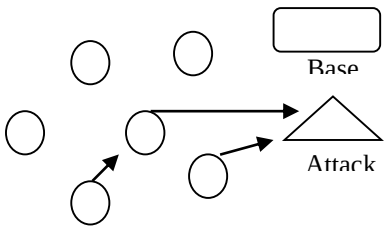


Figure 1.4: Attacker receive packets

Wormhole attack: In the networks, a low-latency connection is established so that the packets can be forwarded from one end to other end quickly using multi-hops. This process launches wormhole attack or intrusion within the network [6]. This intrusion is a big danger for any routing protocol accessible within the network. The detection and prevention of this kind of intrusion is extremely difficult. The wormhole depicts that the node that is though extremely distant, is extremely close to its adjacent, which is an attacker. This may produce perplexed circumstances within the network. The commencement of information sharing at this time will result in the exchange of secret data to the attacker nodes. .

II. RELATED WORK

Ren Xiu –li, et.al (2009) presented a novel approach for the detection of Sybil attack on the basis of range. The range of neighboring nodes was verified through the each node present in the network for identifying the attacker node. The messages were shared amid the nodes for the easy detection of Sybil node. The tested outcomes demonstrated that proposed technique showed better performance in comparison with other existing techniques. This proposed technique was inexpensive and provided correctness. Thus, this approach was utilized mostly for the inexpensive networks and the network having restricted number of resources [7].

BinZeng, et.al (2010) stated that wireless sensor networks were used in large number of applications. Due to the free communication provided by wireless sensor networks, these networks were more vulnerable towards the intrusions. Thus, in these networks, security was considered an indispensable factor for example in peer-to-peer networks. A number of intrusions affected the functionality of these networks and Sybil attack was one of them. In this attack, attack, the distributed system created the false numerous identities and showed that they were several and alienated nodes in the system. When attacker node tried to deceive the truthful node, an edge amid Sybil node and truthful node was existed. In this study, a new protocol was proposed for minimizing the effects of Sybil intrusion. This proposed protocol utilized ant colony optimization (Am) algorithm [8].

James Harbin, et.al (2011) stated that the improvement in wireless sensor network (WSN) was imperative because of its limited battery power and signal congestion intrusions. Thus, in this study, Distributed beam forming clusters were proposed for the advancement of wireless sensor networks. Lesser numbers of sensor nodes participated in the communication procedure and caused connection failure in the network. Due to the free communication provided by wireless sensor networks, these networks were more vulnerable towards the intrusions. During the intrusion, the attacker nodes spoofed the identities of their neighbors. For measuring the effect of these nodes, an investigative scheme was presented in this study [9].

Bin TIAN, et.al (2013) stated that advancement in technology expanded microelectronics technology and wireless communication technology. These technologies proved extremely beneficial in the easy development of low power, low price, multifunction sensor, and wireless sensor networks. Due to the free communication provided by wireless sensor networks, these networks were more vulnerable towards the intrusions. Thus, in these networks, security was the main concern. In these networks, installed Sensors nodes were dispersed arbitrarily because of which this network comprised dynamic network topology. Sensor nodes had inadequate resources and battery energy which resulted in the breakdown of these networks occasionally[10].

P. Raghu Vamsi, et.al (2014) stated that a development was seen in the Wireless Sensor Networks with the expansion of technology. A number of intrusions hampered the performance of this network and Sybil attack was one of them. This attack was considered a big threat. Due to the free communication within this network, this network was prone to different kind of attacks. Extremely inadequate lightweight models were presented in the obtainable schemes. Thus, a lightweight Sybil attack detection framework (LSDF) was proposed for minimizing the affects of Sybil intrusion. The proposed framework used two components identified as evidence collection and evidence validation. Each node monitors the activities of its adjacent nodes within the network for the collection of evidences [11].

Yali Yuan, et.al (2015) stated that a development was seen in the Wireless Sensor Networks (WSNs) with the growth of technology. The wireless sensor networks were extensively used in almost all applications. In wireless sensor networks, the sensor nodes were deployed accurately in hazardous surroundings because of the deployment-aware applications of this network. This network provided free communication atmosphere because of which this network was vulnerable to several types of intrusions. A number of intrusions affected the performance of wireless sensor network. Among these intrusions Sybil attack was considered as one of the main intrusion. In this attack, numerous identities were depicted for the solo node which reduced the localization correctness. This resulted in the destruction of complete network arrangement [12].

Swati Bhagat, et.al (2016) stated that wireless sensor network were used in several applications and in various regions because of their rising technology. These areas included military observation, hospital scrutinizing, forest, and many more. In this study, the wormhole intrusion was reviewed as well. This attack affected the nodes present in the network. These wormhole nodes were identified as false courses as and smaller than the first course in the system. An issue was created in the routing of sensor devices on the basis of distance amid the nodes according to existing situations [13]. In this study, a novel technique was proposed for the powerful transmission of information.

Annie Mathew, et.al (2017) stated that a direct path was created from source to target for information sharing due to the presence of huge amount of sensor nodes. This approach made the sensing procedure simpler. Security was the main threat in these networks because of the free communication atmosphere provided by these networks. A number of intrusions affected the working performance of this network for example sinkhole attack, wormhole attack, gray hole attack and so on. The sinkhole node

established a direct route amid the sink or destination node because of the occurrence of sinkhole intrusion within the network. Up to now, a number of methodologies had been presented using for the effective detection of sinkhole intrusion. In this study, sinkhole intrusion was discussed along with its categorizations and techniques for the detection of this intrusion on the basis of certain aspects [14].

Shams Qazi et.al (2018) A security DV-hop localization algorithm (AWDV-hop) was proposed for the minimization of several issues occurring within the wireless sensor networks [40]. In the first algorithm, the neighbor node relationship list (NNRL) was formed through the utilization of the broadcast flooding. The sensor nodes provided the ID numbers of their neighboring nodes inside the network by using NNRL. The hypothetical and real number of adjacent nodes was compared for the identification of imaginary beacon nodes. The distance to other beacon was estimated within the NNRL for the identification of actual intrusion caused by the beacon nodes. They region was marked with 1 or 2 for the completion of this task. In the end, the other unidentified nodes marked themselves with 1 or 2 on the basis of the marking done by the beacon nodes. No communication was found amid the nodes marked with 1 or 2 because of the extrication among the localization rounds [15].

III PROPOSED APPROACH

Phase of Detection and Isolation of malicious nodes
Following are the various phases of detection of malicious nodes:-

1. Pre-Processing:- The wireless sensor network is configured with fixed amount of sensor nodes. The clustering on the basis of locality is applied in the entire network. The LEACH protocol is used to verify the power and remoteness of each node. The node having utmost power and least distance is selected as the cluster head. The whole nodes occurring in the network will send their information to the cluster head. The cluster head further creates path with the help of other cluster heads and propels this information to the base station. AODV routing protocol is utilized for the establishment of path among source and the destination. AODV protocol is a source node protocol which deluges the route reply packets. The source node selects the most appropriate route towards the destination according to the hop count and highest sequence number. The source node forwards the information to the preferred place. Attacker node launches the misdirectional intrusion with the help of selected route.

2. Detection of malicious nodes: - A number of approaches were proposed in the last few years for the discovery of attacker nodes. The earlier method was monitor mode method. The activity of the neighboring node can be observed with the help of this method. This method does not give good performance in the recognition of attacker node. The second method implemented in the earlier investigation was named as delay tolerance method. This method needs extra hardware and software for the discovery of attacker nodes. This increases the intricacy and cost of the arrangement. The base station applies node localization method for the discovery and segregation of attacker nodes. The node localization technique gathers data on the basis of established route. The base station can collect the whole data of sensor nodes with the help of node localization method. The base station can collect data about the location of sensor node and their delay during the information transmission. The base station scrutinizes the quality of service constraints. When the network throughput is decreased to threshold value, then base station takes action for the discovery of attacker node. The base station checks the network throughput on every hop for the detection of attacker node form the network. The node which decreased the throughput below the threshold value is identified as the attacker node. The gathered data comprises the remoteness of each node from the base station. The distance creates delay in every hop count which exists on the formed route. The base station detects this delay. The delay of every hop is calculated due to which node will enhance the delay within the network and identifies the attacker nodes. The predictable delay is computed with the equation number 1

$$\text{Expected Delay} = \text{Time to live} * \frac{Distance\ between\ each\ node}{Distance\ between\ source\ and\ destination} \quad (1)$$

The distance between each node is calculated with the equation number 2

$$\text{Distance} = (a(i+1)-a(i))^2+(a(y+1)-a(y))^2 \quad (2)$$

The predicted delay is defined with the equation number 3

$$\text{Predicted delay} = \frac{Distance\ between\ each\ node}{Total\ number\ of\ message\ exchange} \quad (3)$$

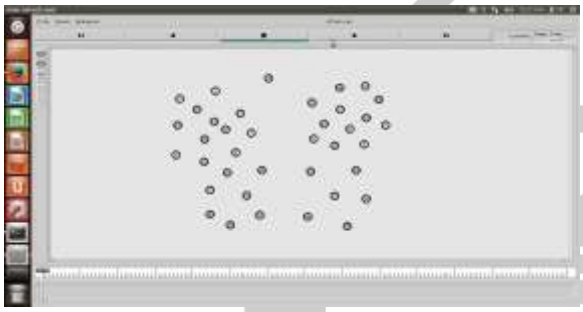
When the predicted delay is above the expected delay then the attacker node is identified from the network. The threshold delay is the forecasted delay. The threshold delay in the network is described as 2 ms if the sensor node enhances the delay above the threshold level which is 2 ms, then that node will be identified as the attacker node. The multipath routing method is implemented for the removal of attacker nodes from the route. The projected method is based on the threshold system for the discovery of attacker nodes and the other applied methods. The proposed approach does not need additional hardware and software, so because of this approach it is preferred for the discovery of attacker nodes.

3. Isolation of Malicious nodes: - In the final stage, the segregation procedure is implemented for the removal of attacker node from the route formed between source and destination. The multipath routing method is used for the elimination of attacker node. The multipath routing technique isolates the attacker node from the network. In this technique, the source floods route request

(RREQ) packets in the network and each node existing close to the destination will reply back with the route reply packets. The source node chooses the finest route from source to destination according to the hop count and sequence number. The source node does not choose the route in which attacker node subsists. The process used for the separation of attacker nodes is described below:
Initialization: Sensor nodes
Output: Assortment of safe route
1. The source transmits route request messages in the network
2. After receiving the route request messages
    Increase the hop count and sequence number
3. if sequence number of novel route > than sequence number of earlier route
    Process the request
    Else
    Discard the request
4. if (attacker node is presented in the path)
    Reject the path
    Else
    Check the hop count and sequence number
5. Choose the safe route from source to destination .

IV EXPERIMENTAL RESULTS

The wireless sensor networks (WSN) are a combination of various extremely small and inexpensive sensing devices or nodes for getting the information in the military areas for monitoring the activities of conflicting sides. Security and power expenditure are the main concerns of WSN because of information sharing property. The attacker nodes which make their entry inside the system launch the security intrusions. LEACH protocol is used to divide the network into clusters and then AODV is used for the establishment of routing path. Below snapshots will show the detection and isolation of malicious node.



II. Figure 5.1: Network Deployment

Fig 5.2: Deployment of Sensor nodes

The network is positioned with fixed amount of sensor nodes(38) as described by the figure 5.1. The network is positioned with fixed amount of sensor nodes as described by the figure 5.2. The entire network is divided into fixed size clusters. The location based clustering is implemented for the clustering of entire network. The different color repreesnet each cluster.

Figure 5.3: Cluster Head Selection

Figure 5.4: Data Aggregati

This figure5.3 is used to represent that The LEACH protocol is implemented for the selection of cluster head in every cluster. The cluster heads are chosen on the basis of remoteness and power. Figure 5.4 is used to represent the initiation of data aggregation phase. The sensor nodes in each cluster start sending data to the Cluster heads .

This figure 5.5 is used to represent the data aggregation in another cluster. All the Cluster heads will create a path and the required information will be transferred to the Base station the help of cluster heads. The direct route will be established from one cluster head to the other cluster head. Figure 5.6 is used to represent the presence of a malicious node in the route. In this route, the attacker node occurs which is responsible for the triggering of the wormhole attack within the network.

Figuer 5.5: Data Aggregration and Transfer to Sink

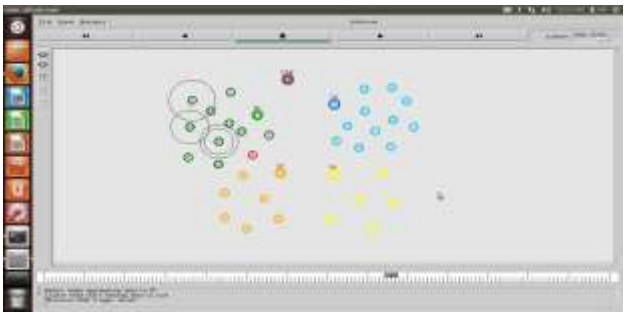


Fig 5.6: Presence of Malicious No

Fig 5.7: Trigger attack

Fig 5.8: Detection and Isolation of Malicious node

The malicious node triggers the attack and start communicating with other nodes in the network. Packet loss occurs due to malicious node in the network. This figure is used to represent the isolation and detection of malicious node in the network. The attacking node 9 is highlighted as 'Malicious'. The multipath routing method is used for the exclusion of attacker node from the route. Source node chooses finest route from the Source to Destination for packets transmission.

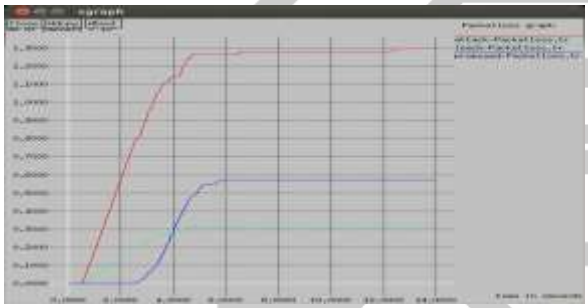


Figure 5.9: Packet loss comparison

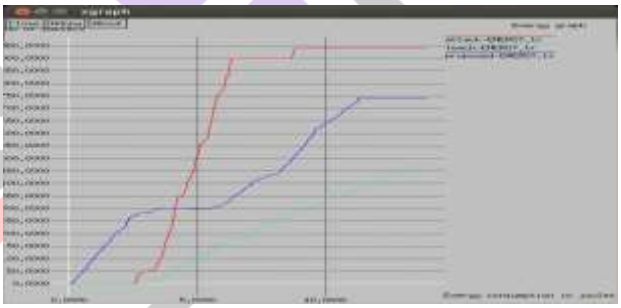


Figure 5.10: Energy Comparison

In figure 5.9 the influence of wormhole intrusion, the leach protocol is compared with the attack scenario and with the proposed methodology on the basis of packet loss as demonstrated. It is analyzed that proposed methodology exhibits decreased packet loss as comparative to attack scenario. In figure 5.10 the leach protocol is compared with the attack scenario and with the proposed methodology for the detection of malicious node in the network. It is analyzed that proposed methodology gives high performance as comparative to attack scenario. It has been identified that the power utilization is decreased after the isolation of wormhole intrusion.

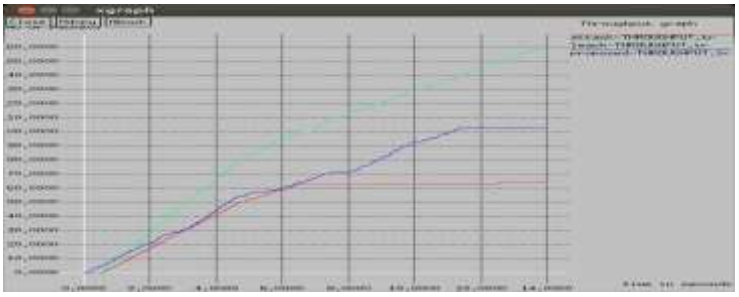


Fig 5.11: Throughput Comparisons

In below figure 5.11 the leach protocol is compared with the attack scenario and with the proposed methodology for the detection of malicious node in the network. It has been evaluated that the network throughput is enhanced at stable rate after the separation of wormhole intrusion.

V CONCLUSION

In this study, it has been analyzed that the LEACH protocol is most efficient approach utilized for the reduction of power utilization within wireless sensor networks. This network can sense the ecological circumstances using sensor nodes occurring inside them. These small sized sensor nodes reduce the life span of these networks. The wormhole attack is identified as an active type of intrusion which decreases the performance of LEACH protocol. In this research study, Distance parameter is introduced for the detection of malicious nodes from the network. The performance of network is scrutinized on the basis of packet loss which is reduced up to 15%, power utilization is reduced by 18% and network throughput is improved by 25%. The approach proposed in this study is used for the detection and isolation of attacker nodes from these networks. The base station evaluates the delay per hop according to the threshold level. The attacker node is identified on the basis of the delay. The node causing maximum delay is recognized as the attacker node. This reduces the power utilization, increases the network throughput and decreases the time delay.

REFERENCES

[1] I.F.Akyildiz et al., "A Survey on Sensor Networks", IEEE Communication Mag., Vol. 40, No. 8, pp.102-114, Aug. 2002.

[2] E.Shi and A.Perrig, "Designing Secure Sensor Networks", Wireless Communication. Magazine, Vol.11, No.-6, pp.38-43, Dec 2004.

[3] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, pp. 30-33, Jun. 2004.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53–57, Jun. 2004.

[5] Kalpana Sharma. M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad- hoc Networks 2010.

[6] David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 2010 IEEE.

[7] Ren Xiu –li, Yang Wei, "Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network", IEEE, 2009.

[8] BinZeng, Benyue Chen, "SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless Sensor Network", International Conference on Computer and Communication Technologies in Agriculture Engineering, 2010.

[9] James Harbin, Dr Paul Mitchell, "Reputation Routing to Avoid Sybil Attacks In Wireless Sensor Networks Using Distributed Beam forming", 8th International Symposium on Wireless Communication Systems, 2011.

[10] Bin TIAN, Yizhan YAO, Lei SHI, Shuai SHAO, Zhaohui LIU, Changxing XU, "A Novel Sybil Attack Detection Scheme For Wireless Sensor Network", IEEE, 2013.

[11] P.Raghu Vamsi and Krishna Kant, "A Lightweight Sybil Attack Detection Framework for Wireless Sensor Networks", IEEE, 2014.

[12] Yali Yuan, Liuwei Huo, Zhixiao Wang and Dieter Hogrefe, "Secure APIT Localization Scheme against Sybil Attacks in Distributed Wireless Sensor Networks", Journal of Latex Class Files, Vol. 14, No. 8, August 2015.

[13] Swati Bhagat, Trishna Panse, "A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network", IEEE, 2016.

[14] Annie Mathew and J.Sebastian Terence, "A Survey on Various Detection Techniques of Sinkhole Attacks in WSN", International Conference on Communication and Signal Processing, April 6-8, 2017.

[15] Shams Qazi, Raad b, Yi Mu, Willy Susilo "Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks", Elsevier, 2018.