ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 4, April 2015**

# Defense Against the Sybil Attack with the Grid Based Transitory Master Key in Wireless Sensor Networks

Blessey.P.M[1], Princy.P.M[2]

PG Scholar, Dept. of Computer Science, S.A. Engineering College, Chennai, Tamil Nadu, India[1]

UG Scholar, Dept. of Computer Science, Bhajarang Engineering College, Chennai, Tamil Nadu, India[2]

**ABSTRACT:** The Wireless sensor network (WSN) is one of the most emerging and developing technologies that promises a variety of security features. Providing security to the sensor network is the prominent characteristic to avoid network based attacks. The Sybil attack is the most frequently occurring attacks against the sensor networks, where one malicious node can gain access using different identities illegitimately. Here, we illustrate the threats presented by the Sybil attack and the defenses against such attacks to enhance the security for many network applications. This attack can be exactly determined with the help of certain functions such as position verification, routing, transitory master key. Various types of sybil attack have been organized and explained to have better knowledge about the differences between each type and the procedure to counteract against such threats. Thus, the approach has been presented to avoid such attacks to provide the effective sensor network [3].

**KEYWORDS**: sensor networks, sybil attack, security, sybil attack taxonomy, transitory master key.

## I. INTRODUCTION

The major applications of wireless sensor networks such as military environment, environmental sensing, industrial monitoring, home intelligence, health monitoring may face mission-critical tasks. Security is one of the main challenging issues in the hostile environment, since it is necessary to withstand such threats and to rapidly overcome all the risks as an effect of the attacks. Most of the sensor nodes probably monitors the environment to gather information according to the application, it is used for. During such data monitoring and gathering process, the confidential information is disclosed resulting in illegitimate activities. Therefore, such security breaches in the network by certain attacks such as sybil attack, helps in gaining control over sensor nodes with forged identity. Safe operations in the sensor network are demanded and it is provided, which is more complicated than in MANETs. The most complicated feature that is necessary for every wireless communication is the security, since sensor nodes are vulnerable to the threats. Adversary is capable to eavesdrop, modify, messages in the network. Frequent changes done in the network topology may lead to the passive eavesdropping and active interference. In this, there has always been a trade-off between the security level and resource consumption. Hence, the best suited cryptography for WSN is the symmetric cryptography.

The necessary requirements for the security are the confidentiality, integrity and availability. The wireless sensor networks are susceptible to various threats during the transmission of information. Moreover, there is a high chance of additional vulnerability since the nodes in the network are most probably placed in the unprotected of the hostile environment. It is practically not possible to protect each and every individual sensor of a large-scale network from security attacks. The opponent tries out various types of attacks in order to degrade the network.

The secrecy of keys used in the network assures the security of the cryptographic system. Keys used in the cryptographic operations are pre-distributed to each communicating nodes prior to the exchange of information in a secure manner. One of the main defensive techniques to avoid the sybil attack is the key management scheme. The key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

management scheme is the mechanism that provides secure communication between the nodes by distributing different kinds of cryptographic keys in the network, such as individual keys, cluster keys, pairwise keys, and group keys.

There are many routing protocols in the sensor network, which is quite simple. This indeed makes the network vulnerable to attacks. Table (1) lists the active attacks that occur in the network such as Sybil attacks, sinkhole attacks, wormhole attacks, selective forwarding, spoofed routing information, black hole attacks, Hello attacks, Byzantine attacks and Information Disclosure and its defensive measures [6].

A. *Sybil Attack*

Presence of a single node at different parts of the sensor network with the forged identity. The network employs a location aware routing that requires nodes to exchange the information to route the packets with its neighbors. Each node exchanges set of coordinates with its neighbors, but by using this an attacker can perform a sybil attack by forging the identity of other nodes.

B. *Sinkhole Attack*

A compromised node may lure at most all traffic from a particular area is directed towards the sink. Forcing nodes in the part of the region to route the data towards it. The compromised nodes are advertised to look attractive to the surrounding neighbors nodes.

C. *Wormhole Attack*

Wormholes may be able to completely destroy the routing if the base station is placed nearby the adversary. Tunnel messages received in one part of the network and replays them in a different part. It consists of more than one malicious node and tunnel between them. The wormhole nodes used to fake the shorter distance path than the original path within the network by confusing the routing mechanism [4] which contains the knowledge about the distance between the nodes. It is the easiest threat that can be launched by the attacker without compromising nodes or gaining knowledge of the network.

D. *Selective Forwarding*

Malicious nodes refuse to forward particular messages or drops them and makes sure that they will not be promoted further. It is capable of modifying packets and forwards the altered messages. It combines with other attacks, like sinkhole, etc. In the data flow, the malicious node itself is included in the path. It can block the essential information from reaching the base station. To detect selective forwarding, two algorithms such as binary search and forward search algorithm.

E. *Spoofed Routing Information*

The attack has taken place in order to gain the routing information broadcasted between the nodes. It is the most direct attack against the routing protocol to disrupt the network. The opponent can be able to create loops, attack or repel network traffic, generate the modified error message or packets, shorten or extend the source routes, end-to-end latency improvement and the separation of the network.

F. *Blackhole and Grayhole Attack*

A blackhole is an attack of advertising falsely about the path that it is shorter and stable path during the shortest path discovery process. Prevention of transmitting data packets to the destination node and difficult in shortest path finding is the main purpose of such illegitimate nodes. Grayhole attack is done with a mischievous node by dropping the packets which makes the detection of lost packets is even more difficult.

G. *Byzantine Attack*

Byzantine attack is an undetectable or rarely detectable attack since the misbehavior is not revealed in the network. It is a one of the network layer attack that presents a single node or a set of compromised nodes that works together to attack the network by dropping messages, creating routing loops and forwarding packets in the non-optimal routes. Hence, this attack disrupts the routing services.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

H. *Information Disclosure*
The name itself implies the behavior of this attack, which discloses the important information of the network. An unauthorized user can obtain the confidential information revealed or exposed by a compromised node.

I. *Resource Consumption Attack*
The resources in the network are power supply, computational power and bandwidth. In this attack, an unauthorized node consumes the resources of other nodes by transmitting a request for route discovery and by forwarding unnecessary packets. Hence this attack is called as the sleep deprivation attack.

J. *Routing*
The routing protocols [4] susceptible to the different types of attacks such as routing table overflow,routing table poisoning, packet replication, route cache poisoning and rushing attack.

K. *Hello Flood*
The best quality route to reach the base station has been advertised by an adversary to every node in the sensor networks. Such advertisement brings out a huge number of nodes to choose the path gaining the trust of each node in the network that the sender is within the neighborhood. A malicious node can transmit power by sending, recording or replaying the hello message. It creates an illusion that the sender of the message is the neighbor of the every node in the network. Furthermore, the network routing is confused. Hence, the nodes transmit packets to the attacker assuming it to the neighbor.

L. *State Pollution Attack*
Faulty as well as existing address provided by the mischievous allocator to the newly created nodes in the sensor network may cause such kind of attack

M. *Fabrication Attack*
Injecting fabricated packets in the network, which cause confusions and complexity in the network. Message fabricated attack is launched by mischievous nodes such as in route salvaging attacks.

N. *Modification*
Modifying the routing packets may cause the integrity of the network to be jeopardized. The malicious node is included as the nodes in the sensor network are free to move and have relationship among nodes.

One of the challenging threat to the routing mechanism in sensor node is the sybil attack,a malicious node pretends to have unrealistic nodes working together. An attacker can make use of various types of sybil attack to trouble or to compromise the network protocol. This attack targets network services and affects the auto configuration schemes and secure allocation schemes based on trust model. Here, we examine the harmful network layer attack called the sybil attack since it is more complicated than other types of attacks. Sybil attack can easily attack or compromise nodes and get confidential data with false identities. Sybil Attack has been prevented by the following defenses such as the radio resource testing, key validation for random key predistribution[1]. Prevention can be done using a transitory master key, position verification and registration. Hence, we propose to detect such attack using transitory master key, which is the effective way to defeat the sybil attack.

## II. RELATED WORK

A. *Grid Based Key Predistribution*
Grid based key predistribution is one of the polynomial pools based key predistribution[1] type which creates a grid of m*m with a set of 2m polynomials.Fig.1 describes that each row and each column in the grid is assigned with polynomial share such as $f_j^r(x,y)$ and $f_i^c(x,y)$. The setup server provide the grid intersection to each node, and assigns polynomial shares of that particular row and column to the node which indeed generates pairwise key for path establishment.To establishes pairwise key between a node with its neighbor nodes, nodes in the network check either for a common row or a column.If it has common row or coloumn ci= cj or ri= rj then the node gets polynomial share

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

from $f_i^c(x,y)$ or $f_j^r(x,y)$ to generate the pairwise keys between the nodes. If there is no common rows or columns is present between two nodes, then an intermediate node is found through which pairwise key generation is made possible[5],[7].

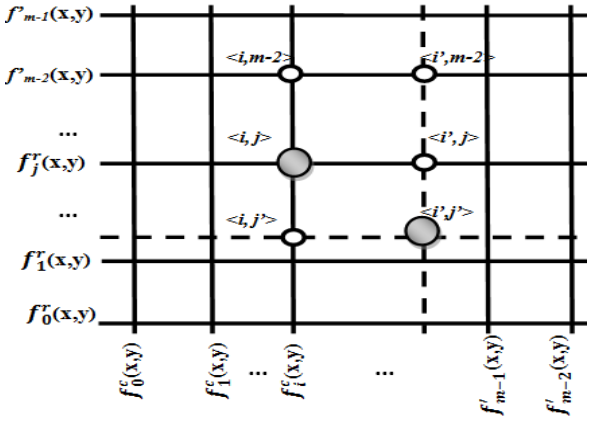


Fig.1. Grid Structure of polynomials

B. *Transitory Master Key*

In the transitory master key[2] , the master key is pre-configured in each sensor node as mentioned in Fig.2. In order to generate the pairwise keys, network nodes share the master key with the neighbor nodes. When the time period is longer, there is higher possibility of compromising the master key Therefore, The master key is erased from its memory after a time period. The master key is retrieved by the adversary only if the master key is stored in flash memory or even in volatile RAM. The compromising of the node cannot take less than a lower bound of time. Therefore, MK should be erased before this time.

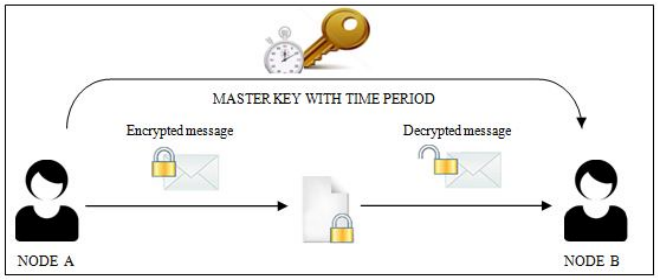


Fig.2. Structure of Transitory Master Key

## III. SYBIL ATTACK TAXONOMY

Sybil attack is an active attack in the network layer, where the malicious node tends to have a large number of nodes by claiming multiple fake identities to control the system. Forge the identities of the legitimate nodes in order to impersonate other nodes in the network. Sybil Attack may obscure, overwhelm and take advantage of the sensor network[3]. Three dimensional taxonomy of sybil attack has been discussed to understand the types and the effect of these attacks. The attacker threatens the reputed system of the network with large number of the fake identities. Since the identities generated are easier and cheaper, the network is exposed to sybil attacks. The intention is to have redundancy, reliability and resource sharing by using multiple identities in the network. Such an attack can gain the control to network substantially. Multiple identities in the network belong to the same malicious device may eavesdrop communication or misbehaves. The different forms of sybil attack are categorized as

A. *Communication*

A communication is achieved with the sybil nodes are direct and indirect communication to overhear and to misbehave to ruin the reputed network system. Fig.3 differentiates the concepts of direct and indirect communication.

(1) Direct communication:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Direct communication is a type of threat, where mischievous nodes make direct communication with the authorized nodes in the network. This mischievous device overhears the messages send by the legitimate node to the sybil node. Similarly, messages sent in return from nodes are from the mischievous device. Testing the node directly whether it is a valid or not using direct validation.

(2) Indirect Communication

Indirect Communication is a version where there is no direct communication between the sybil nodes and legitimate nodes.Malicious node is presented as an intermediate in the node path that routes the message to the sybil node. Nodes which have been already verified are allowed to validate other nodes.

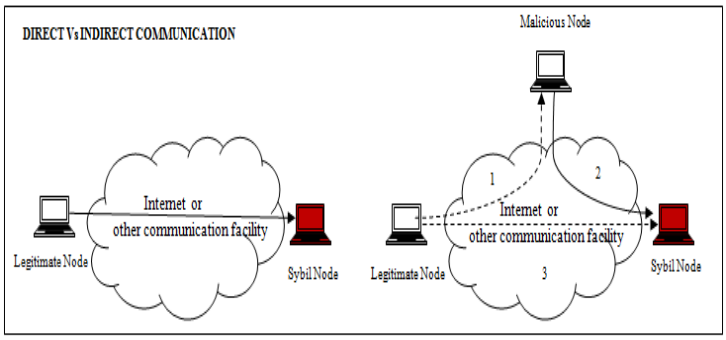


Fig.3. Structure of Communication Taxonomy

B. *Identity*

Forging and stealing the identity of the authorized nodes is the two techniques to have additional illegal identities. Fig.4 illustrates the structure of the identity taxonomy by comparing the fabricated and stolen identities in the network.

(1) Fabricated Identity

Creation of fake identities by a single adversary is to obtain more resources from the network. When there are no restrictions about the identity or any kind of verification technique, then the mischievous node will choose a node randomly and gets connected with the network. For a sensor node, it does have an identity like IP address which can be faked to do illegal activities.

(2) Stolen Identities

Assigning the identities of the authorized nodes to the sybil nodes. If the network avoids threats by limiting the services only to the authorized nodes, in such cases the identity is stolen to have the services for an illegitimate purpose. If the opponent destroys the masquerade nodes, then the stolen identity is undetected. Disabling the stolen identity of the authentic node will put an end to identity theft.

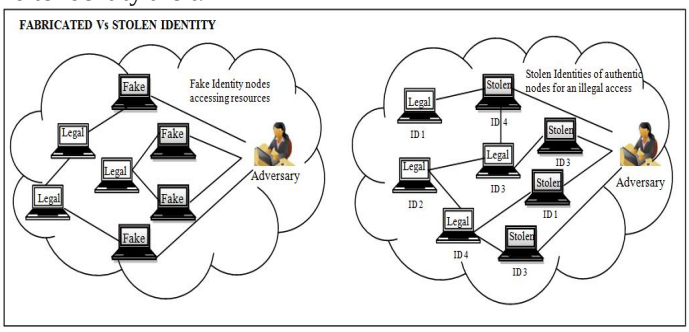


Fig.4. Structure of Identity Taxonomy

C. Simultaneity

Fig.5 describes the simultaneity taxonomy of sybil attack by which an adversary gains access in the network.

(1) Simultaneous

All fake identities of an adversary have been simultaneously taken part in the network as a cycle. A hardware entity can use a single identity at a time, these identities are employed in a cyclic process pretending as if they are present

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

simultaneously. This is type of attack, where an attacker craves to join the service by involving all the identities at once.

(2) Non-simultaneous

Adversary expresses the huge number of identities over a period of time. In non-simultaneous attack, the attacker keeps track and has knowledge that which identity has gained access to the network. An identity departed from the network has been replaced with the other identity that is recently connected to the network. The attacker should use the identity only once,since identity can depart and join multiple times in the network.

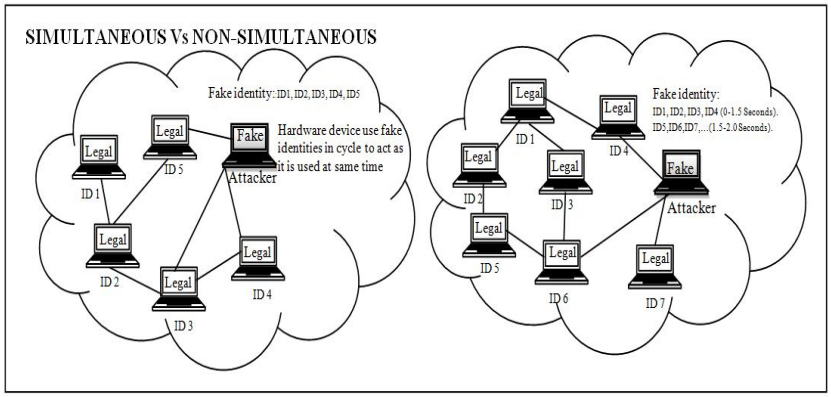


Fig.5. Structure of Simultaneity Taxonomy

## IV. ATTACKS

Several types of protocols in network layer have been attacked by the use of sybil attack. Here, the distributed storage, routing, data aggregation, fair resource allocation and misbehavior detection algorithms, that face the effects of civil attack is discussed [6].

A. *Known Attacks*

(1) Distributed Storage

Sybil Attack is capable of easily defeating the duplication or the fragmentation of a peer-to-peer storage systems as well as provide the duplication or the fragmentation of data stored in the sybil identities created by a single mischievous node.

(2) Routing

Sybil attacks mainly focus on misbehaving in the routing algorithm within the sensor network. Multipath or dispersed routing is one of the susceptible routing protocols, which disjoint the paths that pass through a malicious node illegitimately containing several sybil identities. Sybil attack could be present in multiple area all over the network rather than being located in a single set of coordinates, which is another susceptible routing protocol called the geographic routing.

B. *New Attacks*

(1) Data Aggregation

Sensors usually gather the sensed information from the environment and aggregates them in order to transmit the data to the base station. Aggregation of data will conserve energy by transmitting once rather than transmitting for each sensor reading. Including the faulty sensor reading by any malicious node doesn't make a difference, but with the sufficient amount of sybil nodes,the aggregated reading can be altered completely.

(2) Voting

Sensor network can make use of voting technique for any tasks. Sybil attack has the ability to make voting in favor of the civil nodes based on the number of identities owned by the adversary. It could even pretend that the legitimate node is misbehaving called the blackmail attack. The Sybil attack can vote that the faulty identities of the misbehaving node are legitimate by using the symbol nodes to vote for each identities.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

(3) Fair Resource Allocation

Network resources are assigned between the nodes in the network for an equal time period, but with the help of sybil attack, a malicious node can gain an inequitable amount of resource shared between the sensors. This results in minimizing the resource for the legitimate needs and indeed provide the attacker more resources to have complete access.

(4) Misbehavior Detection

The Wireless Sensor Network has the possibility to detect certain types of misbehaving nodes. Such misbehavior detector gets to know few misbehaviors, but it takes corrective actions, when a same node is found to have repeated misbehaviors or offenses. An adversary with large number of sybil identities can misbehave as much as possible by not misbehaving enough to take actions against the attacker. Corrective actions are made to cancel the misbehaving nodes in the network, but the attacker still misbehaves with new Sybil identities, never been cancelled.

Table(1): Major Attacks and its defenses in the Network Layer

| ATTACKS | DEFENSES |
|---|---|
| Sybil Attack | Authentication, Monitoring, Redundancy, Identity certificate. |
| Sinkhole Attack | Redundancy checking and Detection of the mint route. |
| Wormhole Attack | Authentication, Probing and Proactive routing protocol routing node detection by the signal strength. |
| Selective Forwarding | Egress filtering, Authentication, Monitoring. |
| Spoofed Routing Information | Egress filtering, Authentication, Monitoring. |
| Black hole and Gray hole Attack | Local Monitoring can detect packer forge, packet modification, intentional packet delay and packet drop. |
| Hello Ford | Authentication, packet leashes by using geographic and temporal information, Suspicious node detection by signal strength. |

## V. DEFENSE USING TRANSITORY MASTER KEY

To avoid the Sybil attack in wireless sensor network, there are certain defenses that have been developed earlier such as Radio Resource Testing, Random Key Predistribution, Position Verification, Registration, Code Attestation. The advanced defense technique to detect and avoid a Sybil attack is done using a transitory master key[2].

By creating fake routes in ad hoc networks, disrupting multipath routing protocol, cheating peer to peer computing systems may ruin the integrity of the reputation system. An adversary may compromise node and deploys multiple replicated node in the network. Such fake nodes attempts to establish pairwise keys [5] with the authenticated nodes in the network other than its neighbor nodes. Hence, Sybil attack may work in key pre-distribution scheme as the base station is not aware of the network topology. In Grid Based Transitory Master Key (GBTMK) scheme, the base station is not engaged in key establishment and each node maintains a list of its authenticated neighbors that helps to prevent Sybil attack and replication attacks. The network also contains an intrusion detection system (IDS) keeps that track on the mobile node by monitoring its behavior and the changing position of the node. IDS checks whether the behavior of the node remains same as the original or have been deviated that match the attacker. For the secure communication purpose, messages are securely linked to the identities of the node rather than the node itself. Nodes identity is generally unique and the identities are based on the co-ordinates in the grid. Each node is pre-configured with the set of polynomials and transitory master key to generate a pairwise key. When the polynomial is shared with its neighbor

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

nodes, a pairwise keys are generated which is indeed combined with the transitory master key as an input to the key generation function. As a result of the key generation function, pairwise keys are generated between the nodes in the network as expressed in Fig.6. The key distribution center helps to distribute the pairwise keys among the nodes in the network. The master key is retained only for a short period of time. Each Sybil node takes more time to find out the identity of the other authorized node to gain the resources, but by the time Sybil node finds the identity, the master key is erased and compromising of key has been difficult. Thus, the Sybil node loses the ability to gain the resource by compromising nodes with its shared secret key. Therefore, GBTMK- a hybrid approach provides the best feature to perform the cryptographic operation and sybil attack avoidance.

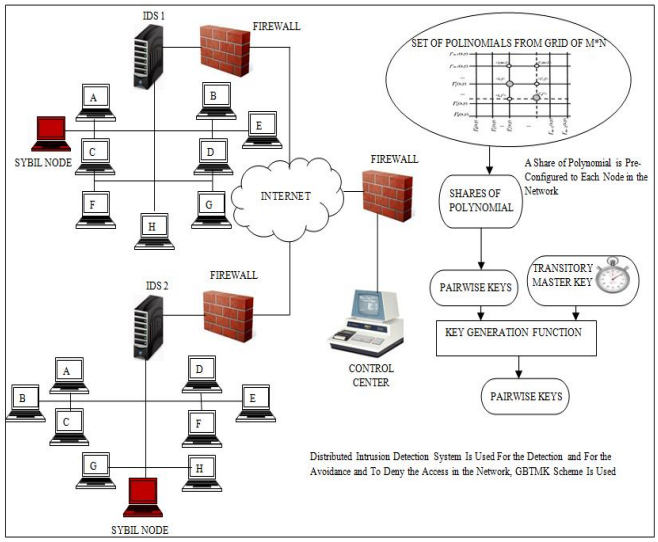


Fig 6. Pairwise Key Generation Using The Hybrid Technique

## VI. CONCLUSION AND FUTURE WORK

Here, we discuss about detail study of Sybil attack, differing attack types of taxonomy and the defenses against the civil attack. An enhanced technique, Grid Based Transitory Master Key (GBTMK) scheme has been employed among the nodes in the network through which node verifies its neighbor nodes, whether it is a sybil identity or not and prevent the sybil attack. Therefore, the proposed scheme is used to secure communication during data sharing and provides robustness to compromised nodes.

## REFERENCES

1. Leenu Rebecca Mathew, Jyothish K John, "A Survey of Key Pre Distribution Schemes in Wireless Sensor Networks", International Journal for Scientific Research & Development, Vol. 1, Issue 2, pp. 949-952, 2013.
2. J. Deng, C. Hartung, R. Han, and S.Mishra, "A practical study of transitory master key establishment for wireless sensor networks," in Proc.1st Int. Conf. Security and Privacy for Emerging Areas in Commun.Netw., Washington, DC, USA, pp. 289–302, 2005.
3. K. Sohraby, D. Minoli and T. Znati, "Wireless Sensor Networks: Technology, Protocols, and Applications," John Wiley and Sons Inc., Hoboken, New Jersey, 2007.
4. P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in adhoc wireless Networks", Wireless networks, Vol. 7, Issue 6, pp. 609–616, 2001.
5. W. Du, J. Deng, Y. S. Han, and P. K. Varshney,"A pairwise key pre-distribution scheme for wireless sensor networks", In ACM CCS, Washington, DC, USA, pp. 42–51,Oct. 2003.
6. C. Karlof and D. Wagner,"Secure routing in wireless sensor networks: Attacks and countermeasures", In First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127, May 2003.
7. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks", In ACM CCS, Washington, DC, USA, Vol. 20, pp. 52-61,Oct. 2003.
8. Haowen Chan, Adrian Perrig, and Dawn Song.,"Random key pre-distribution schemes for sensor networks", In SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy ,Washington, DC, USA, pp. 197, 2003.