Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DETECTION AND PREVENTION OF SYBIL ATTACK IN WIRELESS SENSOR NETWORK EMPLOYING RANDOM PASSWORD COMPARISON METHOD

[1]R. AMUTHAVALLI, [2]DR. R. S. BHUVANESWARAN
[1]Assistant Professor, SSN College of Engineering, Chennai, India
[2]AssociateProfessor,Anna University, Chennai, India
E-mail: [1]amuthavalli@ssn.edu.in , [2]bhuvan@annauniv.edu

ABSTRACT

Security is imperative for some Sensor Network Applications. An especially unsafe assault against sensor and impromptu systems is known as the Sybil attack, where a node illegitimately asserts numerous characters. In this type of attack a legal node is converted into a Sybil node which is a replica node with a different personality but using a similar ID. This leads to data leakage which causes data integrity violations. In existing research, nodes can detect the suspect nodes by checking the nodes in its neighborhood i.e within a given range. The neighbor nodes exchange information about each other and detect the Sybil node as it provides misleading information. The Sybil nodes are not detected directly by checking the ID or other node related information. In this paper, a Random Password Comparison [RPC] method is proposed that facilitates deployment and control of the position of node thereby preventing the Sybil attack. The RPC method is dynamic and accurate in detecting the Sybil attack. This method improves data transmission in the network and will also increase the throughput.

Keywords: *Wireless Sensor Networks; Sybil Node, Data Integrity Violation, Random Password Comparison.*

1. INTRODUCTION

Wireless sensor network is a highly distributed group of spatially distributed autonomous nodes that employ millions of tiny, inexpensive sensors for monitoring our physical surroundings. They are termed as adhoc networks as they require no infrastructure and can accommodate themselves to any existing infrastructure. Due to these reasons, WSN is used in many areas such as Military surveillances, environmental conservation, domestic applications, and so on.

As WSN finds application in many diverse areas from military to commercial applications, it becomes important that it is made secure against malicious attacks. The conventional network security mechanisms are inadequate for wireless sensor networks. Hence researches are trying to build a sensor trust model that would solve the problems that go beyond the capability of traditional techniques and also it would address the challenges of maximizing the processing capabilities of wireless sensor nodes. Sybil attack is the process by which a solitary node acquires the multiple characteristics of the other nodes in the network. The Sybil attack is one of the primary attacks that would facilitate the onset of many different attacks in the network. This type of attack can reduce the effectiveness of fault-tolerant schemes and pose a threat to geographic routing protocols. This attack can pose many problems by targeting many residences simultaneously. Fundamentally, a compromised node baits all the transportation within the network by making itself look attractive with respect to routing algorithm. The network attackers are divided into two major types, inside attacker and outside attacker. This in turn is divided into passive attackers and active attackers. A Sybil attack is an inside, passive attacker.

This paper concentrates on the problem of securing the wireless sensor networks. The table1.1describes in detail, the attack types, their definitions and their pictorial representation.

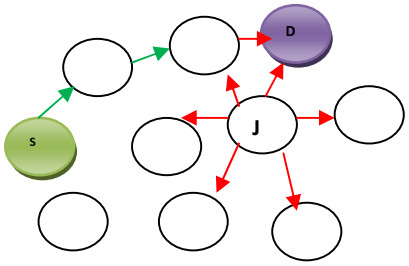
Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This is followed by the existing research work the method for the detection of the Sybil attack based on range particularly suitable for systems of low-cost and lacking resources of wireless sensor network [1]. The rest of the paper is organized as follows; In Section 2, we have discussed related works (Existing work). Section 3 proposed system model and algorithms are discussed. In Section 4 simulation results are shown Section 5 and 6 is conclusion and reference papers are included.

1.1. Various Attacks on Wireless Sensor Network

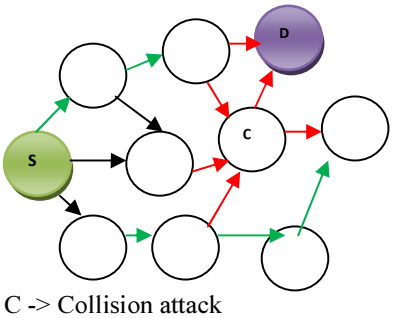
Table - 1.1: Jamming Attack



Good Traffic → Bad Traffic

A node in the network interrupts the whole network by simply sending messages to other nodes, and changing the behavior of node into out of service.

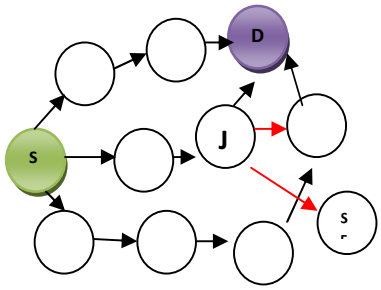
Table - 1.2: Collision Attack



C -> Collision attack

At a given time multiple nodes communicate and send data packet to each other; the nodes in between cause collisions which spoil the communication among nodes.

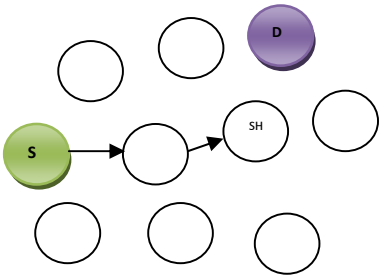
Table - 1.3: Selective forwarding attack



SF -> selecting Forward attack

When data is transmitted in multipath, the attacker node will take the data and send it through some other path and drop the packet, which spoils the path selection and the data won't reach the destination correctly.

Table - 1.4: Sinkhole attack



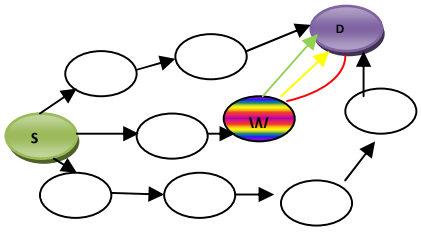
SH-> Sinkhole Attack

A node in the network receives all the information in the path and does not pass it to the next hop. The intermediate node acts as the sink node. It can be any node on the route where the data is transmitted from Source to Destination.

Table - 1.5: Wormhole attack

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



W -> Wormhole attack

It is also named as replay attack, and can occur in any portion of the network. It behaves similar to sink-hole node or Sybil node. The wormhole attack also happens on the route where the data is transmitted from source to destination.

In this paper the work focused in two ways one is route discovery and data routing. While route discovery each node is verified with its assigned random password, time taken to transmit a data packet and the distance among the nodes. All these information [ID, time, PWD] is stored in a routing table for further verification. After successful route discovered, the data packet is transmitted once again by cross verifying the nodes information from routing table. The complete paper contribution is listed as:

- RPC based password assignment
- Route-Discovery and Routing Table Maintenance
- Data transmission by verifying the Routing Table Information using Check-route

In this paper RPC algorithms detect and prevent the Sybil attack with successful routing.

2. RELATED WORKS

The applications of WSN are Area monitoring, Environmental / Earth monitoring, Industrial monitoring, Agriculture monitoring, Structural monitoring, Passive localization and tracking. Various simulations are applied to investigate the energetic nature of WSN [2] because WSN are used in conservational investigation tasks. The sensor nodes have limitations in storage, power, latency, constraint bandwidth and reduced corporal size [3]. Since WSN nodes have limitations, safekeeping is most important role needed to detect and prevent malicious activities in the network [4]. The security can be applied in terms of confidentiality, Authenticity and availability. There are various types of attacks that occur in WSN, [5] broadly classified into two types that is inside the route and outside the route. In [6], the sinkhole, wormhole, and Sybil attacks are occur directly during transmission when data is passed from the data passed from source to destination. It is also said that in [7], the simulation can be done for detecting a single node or several trustable nodes join to improve the accuracy of the detection. One of the authors [8] reviewed that an IMAODV, AODV, MAODV, are compared and the better performance canbe obtained in the IMAODV.

In a Sybil spasm, the entire malevolent nodes which destroy the WSN by using a huge amount of fake appearances in order to disturb the network's rule [9]. Paper [10] surveys the present state-of-the-art protected multipath direction-finding protocols in WSNs and categorize the protocols and their security related function description. Paper [11] provides an all-inclusive impression of safekeeping issues. Paper [12], proposes a security mechanism based on LEACH routing protocol against Sybil attacks. A neoteric discovery mechanism, called CRSD is introduced and explained about RSS [Received Signal Strength in [13] among two individual nodes. Routing discovery including security among reliable nodes [14] is also proposed earlier. In [15] the attacks faced by WSNs were analyzed. Security should deploy in natural applications and global business [16]. The "Security Aware Ad-hoc Routing (SAR)" was introduced in [17]. A set of experiments carried out in sensor networks are miscellaneous and so the attention is directed attention on attacks on Wireless Sensor Network [18]. It is proposed in [19] some of the security area for Wireless Sensor Network. Additional, security being energetic to the approval and use of sensor networks for numerous applications; we have completed an in depth danger analysis of Wireless Sensor Network. In [20] paper have discovered overall security intimidations in wireless sensor network and made an wide study to classify available data collecting protocols and examine conceivable security threats on them.

The Existing system [1] model has two levels. In the first level Sybil node is suspected

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and in the second level it is confirmed to be a Sybil node. The steps of finding out the Sybil nodes are as below:

Step 1: Every node in the route should provide their neighbor node information within the range and within a distance to the source node in order to discover the route. The nodes which share an equal distance have to be found and then the suspect nodes which share the same distance have to be detected and grouped according to shared distances. These nodes are saved as the suslist1. The structure of suslist1 is:

Distance1: suid1, suid2….

Distance2: suid1, suid2…

Step 2: The suslist is proposed in the same way and from line, the suid1 is checked with suid2, compare and check the suid1 with suid3 and so on till the end. If any suid matches with the any other suid in the same line, take that suid as a Sybil id and make a new list for Sybil nodes.

Step 3: as is shown in step one,the first line compared with each line below till the end of the suslist2 and the Sybil node numbers are found and added to the Sybil node list.

Step 4: every line of the Sybil list is checked and if there are two or more susids in one line, it means the susids in this line are all Sybil nodes output with the same malicious nodes. The numbers of Sybil nodes are detected after many processes in the existing system. So it takes more time to detect the node as a malicious node, and it affects the overall network quality and performance.

The main disadvantage of the existing approach is that it consumes a lot of time as the work load is doubled during transmission. This increases the time and cost component. The major portion of the time is spent in verifying the nodes in the route, outside the route and in the complete network. As Sybil comes with duplicate ID, verification based on the ID only, makes this approach less accurate.

3. PROBLEM STATEMENT

Due to the nature of WSN data transmission among two nodes need multi-hop communication. The intermediate nodes in the route is elected dynamically also nodes are moving nodes in the network. Hence any node can move very closely to the other nodes and can capture the nodes information. Since a node can act as another node and interrupt the network functionality. To avoid node duplication [Sybil] a RPC algorithm is proposed to prevent the Sybil attack by verifying the nodes ID and location.

4. RANDOM PASSWORD COMPARISON ALGORITHM TO PREVENT SYBIL ATTACK

In this paper an algorithm is proposed to address the different traffic levels and security considerations during the data transmission in a Wireless Sensor Network. The Network G has a base station BS, and comprises of N number of nodes deployed randomly. The algorithm generates a routing table (rtable-RPC) to store the information of each node's id, the time and a password. The intermediate nodes in the route are identified between source and destination. The intermediate node's information is then compared with the RPC database. If the information matches, the node is considered to be a normal node otherwise node is considered to be a Sybil node. A Sybil node will not able to submit the dynamic password which is assigned to all the nodes in the network. The proposed system model is shown in Fig 4.1.

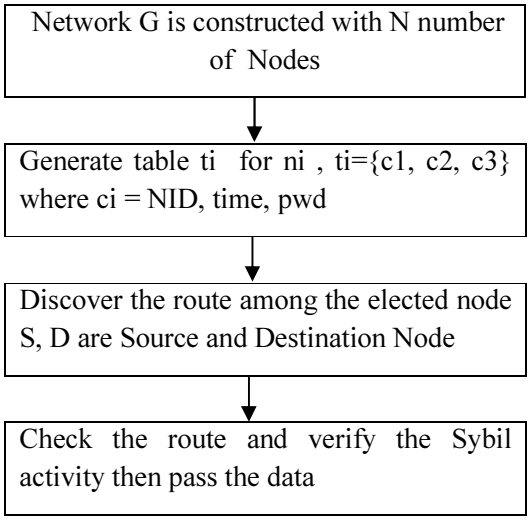


Figure- 4.1: System Model

A Random password generator generates a new password, every few seconds for each node and sends it to all the nodes in the network. When a destination node communicates with the source node, the destination node's id, time delay and the random password corresponding to the time delay will be compared with the RPC database. If the id, corresponding to the time delay with

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Nid	Time	Pwd
K	1:00	Rty
K	1:05	Yui
K	:	Iuy
K	t_i	Oiu
K	:	Poi
K	:	Lpo
k	t_n	Qwe

Nid	Time	pwd
i	1:00	Asd
I	1:05	Frt
i	:	Fgt
i	t_i	hyu
i	:	Uio
i	:	Bgr
I	t_n	kio

Figure 4.2(a): Sybil Node detection

the password is matched, the source node will send the data otherwise the node is considered as a Sybil node Figure- 4.2 (b). The nearest neighbor is found by calculating the minimum distance from the source node as given in (1)

$d_{ij} = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \forall$ i j denotes node index … (1)

$node(i) \leftarrow gen(nid, time, pwd) i \ni \int_{i=0}^{i=n} record(rtable) \ldots$ (2)

$pwd(currentNodei) \forall \int_{i=0}^{i=n} pwd(n_i) \ldots$ (3)

$CurrentNode(time, pwd) \forall rtable(nodeid, time, pwd)$ … (4)

After a given time interval, the RPC will generate the node id, time and pwd to be compared with the data stored in the rtable as specified in (2). This rtable is then utilized during route discovery between source node and destination node. Based on the match (id, time and password) as in (3) and (4) the source node will proceed with data transmission or else designate the node as a Sybil node. If the destination node D is identified as a good node, the source node S will send the data to D. Since all nodes in the network are sensor nodes, a node L which is in the nearest sensing region of node D, will recognize the data from S, and will mimic as node D and try to acquire the data. This node L would be a Sybil node Fig (4.2-a).

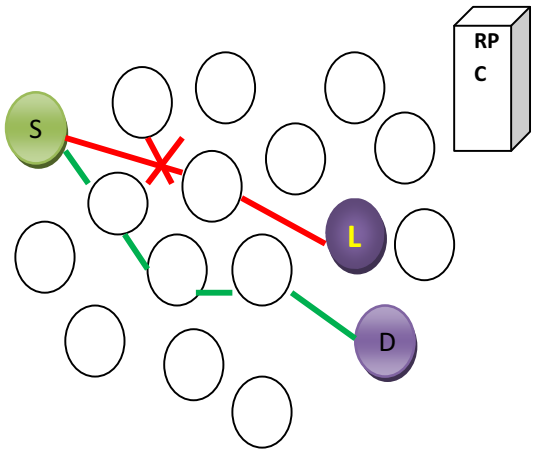


Figure 4.2(B): Shows The Random Password For Ith Node.

The simulation results show that a network in which each node has a unique ID and location, this scheme would detect 99.5% of the Sybil nodes with no more than a 5% false detection rate. The Random Password Comparison method algorithm is shown in Fig 4.3.

1. $Network\ G, which\ has\ n\ number\ of\ nodes, G = \{n1, n2, n3 \ldots . ni, .. nn\}$
2. $Table\ T = \{t1, t2, t3 \ldots . ti, \ldots . tn\}$ $where\ ti\ is\ table\ for\ ith\ node$
3. $Table\ T\ is\ commonly\ available$
4. $in\ BS\ where\ it\ can\ be\ authenticate\ all\ nodes\ in\ G.$
5. $c1, c2, c3\ are\ the\ three\ columns\ in\ the\ table\ ti\ where\ c1\ is\ the$
6. $node\ id, c2\ is\ the\ time, c3\ is\ the\ password\ generated\ for\ node.$
7. $Elect\ any\ two\ nodes\ S, D\ as\ Source\ and\ Destination\ Node\ in\ G.$
8. $Node\ D\ sends\ a\ data\ request\ message\ to\ node\ S.$
9. $A\ route\ discovered\ between\ S\ and\ D\ using\ the\ sub-procedure\ DISROUT(S, D)\ is\ obtained.$
10. $Now\ S\ sends\ data\ in\ the\ same$

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$route\ verifying\ for$

11. $Sybil\ Activity\ by\ CHKROUT(S, D)$

$in\ all\ the\ nodes\ found\ in\ the\ route.$

$Then\ node\ S\ sends\ a\ data\ to\ D.$

Figure 4.3 Random Password Comparison Algorithm

The RPC algorithm gives three values c1, c2, c3 for every node and they are stored in the rtable. When a route is discovered from source node to destination node, every nearest node should submit their id, time, password (pwd) which is then compared with the rtable values. If the node is genuine then it is chosen as the nearest neighbor and added to the route [eq(5)].

$$If\ \{\forall\ next_{node(id,time,pwd)} \in rtable(rec_i)\}$$

$$route \leftarrow route + next\_node$$

$$else\ \{choosenext\_node\} \quad (5).$$

If the node id, time, pwd of a next neighbor does not match with the rtable, it means that the current node is discarded and another node is chosen for the same process. This process continues until the destination node is reached.

If the node id, time, pwd of a next neighbor does not match with the rtable, it means that the current node is discarded and another node is chosen for the same process. This process continues until the destination node is reached

DISROUT (node n, node m)

1. $node\ n\ looks\ towards\ D\ for\ the\ next\ neighbor$
2. $get\ the\ node\ information\ from\ the\ neighbor$

$node\ \ ni\ and\ compare\ it\ with\ table\ ti\ information$

3. $check\ if\ (\ ti(c1, c2, c3)\ ==\ ni\ (c1, c2, c3)\ )$
4. $updaterouteTablert\ = \{S, ni, \ldots\}$
5. $else$
6. $reject\ the\ node\ ni, and\ look\ for\ ni + 1$
7. $repeat\ step\ 2$
8. $end\ if$
9. $return\ \ rt$

Figure 4.4 DISROUT Algorithm

The *DISROUT* algorithm (Fig 3.4) compares the node id, password and time of generation of password with the routing table. If it matches it implies that the node is a good node and can continue with further processing, if not, it is detected as Sybil node.

CHKROUT (node n, node m)

1. $Receive\ route\ information\ from\ rt$
2. $Get\ the\ node\ information\ from$
3. $\quad rt\ table\ ni\ and\ compare\ with$
4. $\quad table\ ti\ information$
5. $Check\ if\ (\ ti(c1, c2, c3)\ ==\ rt\ (c1, c2, c3)\ )$
6. $Update\ \boldsymbol{routeTablert}\ = \{\boldsymbol{S, ni}, \ldots\}$
7. $else$
8. $reject\ the\ node\ ni, and$
9. $\quad look\ for\ ni + 1$
10. $repeat\ step\ 2$
11. $until\ D$
12. $end\ if\ ;\quad return\ rt$

Figure 4.5 CHKROUT Algorithm

The sub procedures DISROUT and CHKROUT detect the route from source to destination before transmitting the data. These comparisons require the RPC method to assign random values to all the nodes to check if the nodes are normal nodes or not. In this paper, as the Sybil node is detected during the initial phase of data transmission, there is no data loss, resulting in time and energy savings for the nodes. This also results in improvement of network efficiency.

5. SIMULATION RESULTS

The proposed schemes have been experimented in the simulation environment in ns2. The simulation parameters are shown in Table 4.1

Table-5.1: Simulation Parameters

Parameter	Level
Area	1000m x 1000m
Speed	1 to 15 m/s
Radio Propagation Model	Two-ray ground reflection
Radio Range	250 m

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Method	Round1		Round 2		Round 3		Round 4		Round 5		Round 6			Round 7
Normal vs Existing	NN	SN	NN	SN	NN	SN	NN	SN	NN	SN	NN	SN	NN	SN
	20	1	40	3	60	3	80	4	100	9	500	14	1000	29
RPC	20	1	40	2	60	2	80	3	100	3	500	9	1000	13

Number of Nodes	20 to 1000
MAC	802.11
Application	CBR, 100 to 500
Packet size	50
Simulation Time	100 s
Placement	Random
Malicious Population	Upto 5%
Sybil Ids per malicious node	2
Pause Time	2ms

The network deployed with 20 nodes and how they communicate with each other. During the communication, RPC functionality is defined and the Sybil node is also detected. The Figure-4.1 shows that node number 11 collects information from node 3 and moves to another place and changes its id as 9. Periodically based on the id, time and dynamic password of the node, the Sybil node is detected.

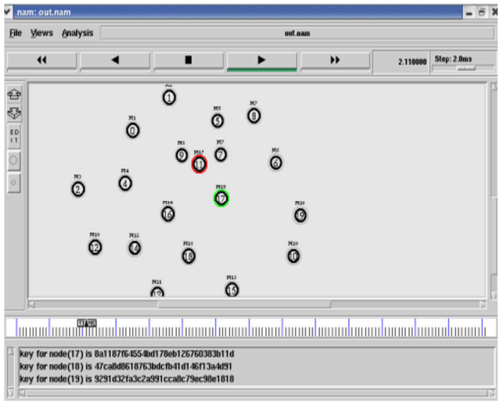


Figure-5.1 Node 11 Is Detected As Sybil Node

Applying RPC method the number of node acting as Sybil is reduced as much as possible. Initially Sybil is detected but due to the comparisons that have to be made, the RPC provides more prevention than detection.

The Table 5.2 shows that the number of normal node deployed in the network and the each iteration number of Sybil nodes are detected by the existing and the proposed approach. The number of Sybil nodes detected in the proposed approach is comparatively less than the existing approach

Table-5.2 EXISTING method vs. RPC [Sybil Node Detected]

The performance comparison is shown in Figure 5.2. The number of iterations with number of Sybil nodes detected using existing and proposed approach. Each iteration the detection of Sybil node is reduced when compared to existing approach. In 7th iteration the Sybil node detected is 13 out of 1000 nodes whereas in existing approach it is 29.

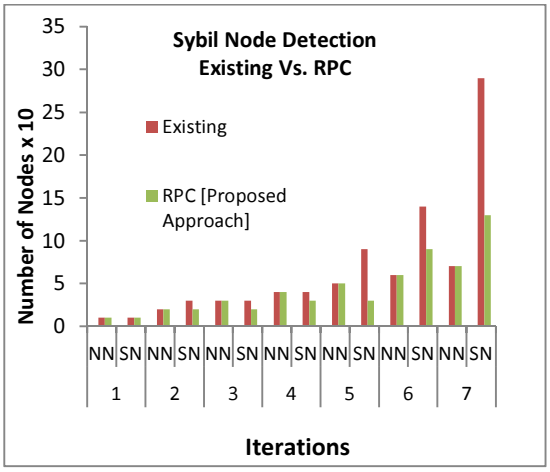


Figure-5.2: Existing Vs. Proposed [Sybil Node Detected]

Table- 5.3 shows the Sybil nodes detection time is stages from time at which it first occurs and time at which it is detected in the network based on the proposed approach.

Table-5.3 Sybil Node Detection Time In Stages

	Sybil Occurring Time			Sybil Detection time		
Method	100	500	1000	100	500	1000
Existing	3.1	3.9	4.5	9	14	21
RPC	0.5	0.7	0.9	3	6	7

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Compared with the existing methods, the proposed method detects the Sybil nodes in the initial stage itself [while route discovery]. But in other methodologies, Sybil nodes are detected during the data transmission.

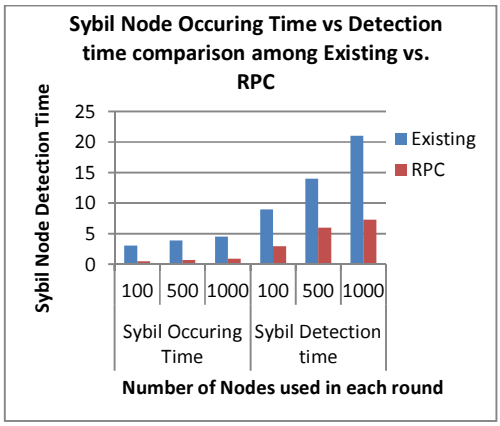


Figure-5.3 Number Of Sybil Node Detected Vs. Time

The Number of Sybil nodes detected out of 500, 1000, 1500 normal nodes in the network and the time Sybil node detected are detected is graphically given in the Figure- 5.3. Data leakage is more in the existing approach. But in the proposed approach the data leakage is not available but time consumption is a considerable factor in the proposed approach while assigning and comparing the dynamic values of every node in the route.

The Table 5.4 shows that the network QoS parameters results are shown better performance after applying RPC. The simulation is repeatedly applied with different number of nodes as 500, 1000, etc., and efficaciousness of RPC is compared. Even when the network size increase, the results of the RPC method shows better performance than the existing approach.

Table-5.4 Qos Parameter - Existing Vs Proposed Approach

Parameter	Existing approach	Proposed approach
Delay Time	5.7845%	4.8975%
Throughput	287689	435678
Energy	67.45%	74.56%

The throughput obtained by the proposed approach with existing is observed in many rounds where the number of nodes is increased in each round.

Table-5.5 Throughput Comparison Existing Approach Vs Proposed Approach

Time	Existing	RPC
0	0	0.2
50	0.23	0.4
100	0.12	0.62
150	0.18	0.65
200	0.47	1
250	1.12	1.45
300	1.4	1.8
350	1.6	1.92

The throughput comparison with Time is also shown in the Figure-5.4. Throughput is increased as the time increases in proposed approach.

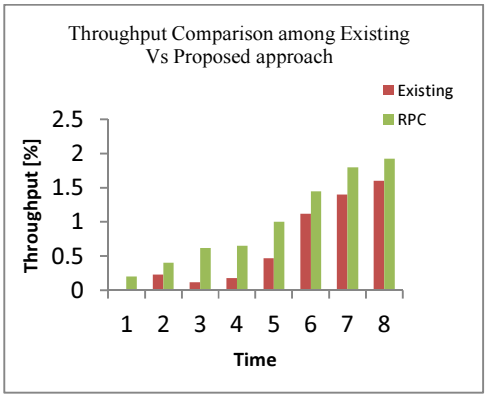


Figure-5.6 Throughput Comparison

The Energy consumed by the RPC and in the existing approach is observed in many rounds where the number of nodes is increased in each round, is given in the Table- 5.6. The energy has been calculated using the following formula (6).

Journal of Theoretical and Applied Information Technology
10th September 2014. Vol. 67 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$currentEnergy = E_{intialEnergy} - [E_{recEnergy} + E_{tranEnergy} + E_{IdleEnergy}] \quad (6)$$

Table-5.7 Energy Comparison Existing Approach Vs Proposed Approach

Time	Existing	RPC
0	0.6	0.9
1	0.4	0.89
2	0.5	0.89
3	0.6	0.9
4	0.5	1.1
5	0.4	1.1
6	0.6	1.1
7	0.61	1.1
8	0.62	1.3
9	0.6	1.4
10	0.65	1.5

The comparative result of the proposed system [red] versus the existing system [green] can be presented graphically and is depicted in Figure-5.5. The figure clearly shows that the proposed approach obtains better throughput, and better energy.

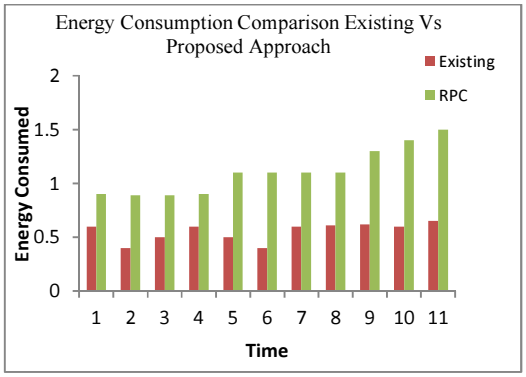


Figure-5.8 Energy Comparison

The comparative result of the proposed system versus the existing system can be presented graphically and is shown in Figure-5.6. The delay time is achieved in the network; it is clear from the graph that the proposed approach performs better than the existing system

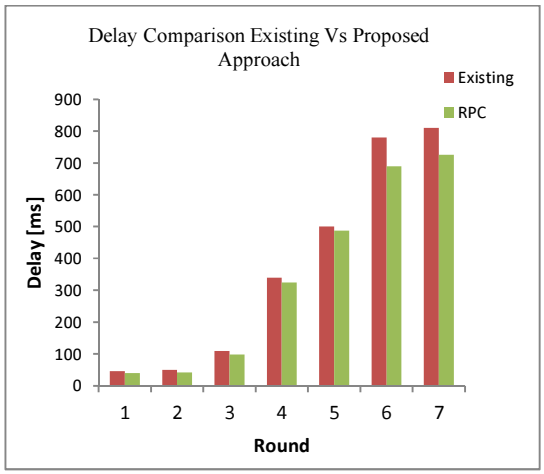


Figure-5.9 Delay Time Comparison

We use two main metrics to determine the detection accuracy of the proposed scheme in different environments, i.e., True Positive Rate (TPR) and False Positive Rate (FPR) [7]. True positive means a malicious node has been correctly detected and false positive means a good or legitimate node has been incorrectly detected as a malicious one and the rate is calculated as follows:

$$\text{True Positive Rate} = \frac{CorrectlyDetectedSybilNodes}{TotalNumberofNodes}$$

$$\text{False Positive Rate} = \frac{Wrongdetectionof SybilNodes}{TotalNodesdetectedasSybil}$$

In the proposed approach the Sybil nodes are detected by ids, time and (pwd) at assumed values only. Of the 3 parameters used, 2 parameters are real and the third one is assumed, the original Sybil detection is also correct up to 70%. The proposed approach also calculates the TPR and FPR and

TPR = 13 / 1000, FPR = 3/13.

The TPR and FPR values are calculated and shown in Table-5.7 are derived using NS2. Also the TPR, FPR are computed in each round of the simulation by changing the number of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes deployed in the network and it is clearly shown.

*Table-**5.7** TPR-FPR comparison among Existing Vs. Proposed Approach*

Nodesize	No. of. Attack		Existing System		Proposed System	
20	1	1	5%	0	5%	0
40	3	2	7.5%	0	5%	0
60	3	2	7.5%	0	5%	0
80	4	3	5%	0	3.75%	0
100	9	3	9%	0	3%	0

6. LIMITATIONS

In this paper, it is necessary to include the route repair mechanism, in case of route failure. The TPR can be increased for more number of nodes deployed in the network.

7. CONCLUSION

In this paper the RPC algorithm discovers a valid route by checking each node is a trustable node or a Sybil node and transmits the data very safely. The RPC algorithm is too dynamic, and generates password more effectively to avoid ID-duplication. The efficiency of RPC algorithm is proved from the above graph and tables. The Sybil nodes are detected and data leakage is avoided completely using RPC. As the Sybil nodes are detected in the initial route discovery stage, this enables the network to continue with their further transmission without any fear of attack.

REFERENCES

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

[2]. Tamilarasan Santhamurthy, "A Comparative Study of Multi-Hop Wireless Ad-Hoc Network Routing Protocols in MANET", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011 ISSN (Online): 1694-0814.

[3]. Abirami, K.Shanthi, "Sybil attack in Wireless Sensor Network", IJET, ISSN: 0975-4024 Vol 5 No 2 Apr-May 2013.

[4].S.Sharmila, G.Umamaheswari, "Detection of Sybil attack in Mobile Wireless Sensor networks", (IJESAT) International Journal of Engineering Science &Advanced Technology, Volume 2, Issue 2, 256-262

[5]. MahamoodulHasan MD, Syed Shaheen, "BSMR: Byzantine-resilient secure multicast routing in multihop wireless networks", International Journal of Computer Trends and Technology- volume3 Issue- 2, 2012.

[6]. Sohail Abbas, MadjidMerabti, David Llewellyn-Jones, and KashifKifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.

[7]. A.V.Pramod, Md. Abdul Azeem,M, OM. Prakash,"Detecting the Sybil Attack in Wireless Sensor Network", International Journal of Computers & Technology(IJCT), volume 3, No. 1, AUG, 2012

[8].Gaurav Sharma, VaishaliSahu, Prashant Kumar Maurya, MahendraSrivastava, Ashish Allen Robert, " Improved Multicast AODV: A Review", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May Jun 2012, pp 1082-1087

[9]. Kuo-FengSsu, Wei-Tong Wang, Wen-Chung Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information", Computer Networks 53 (2009) 3042–3056, 2009 Elsevier B.V.

[10]. ElianaStavrou, Andreas Pitsillides, "A survey on secure multipath routing protocols in WSNs", Computer Networks 54 (2010) 2215–2238.

[11].Xiangqian Chen, Kia Makki, Kang Yen, and NikiPissinou, "Sensor Network Security: A Survey" IEEE Communications Surveys & Tutorials, VOL. 11, NO. 2, SECOND QUARTER 2009.

[12]. Shanshan Chen, Geng Yang, Shengshou Chen, "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks", 2010 IEEEDOI 10.1109/CMC.2010.265.

[13].ShaoheLv, Xiaodong Wang, Xin Zhao and Xingming Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", 2008 IEEE DOI 10.1109/CIS.2008.69.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14]. Weichang Li, Hongning Li, Min Xie,Shupo Bu, "An Identity-based Secure Routing Protocol in WSNs", 2011 IEEE, DOI 10.1109/CIS.2011.160

[15]."21 ideas for the 21st century" Business Week, Aug. 30, 1999:78-167.

[16] BONNIE DORR, "Ten emerging technologies that will change the world", University of Maryland (College Park, MD) Computerized translation of Web documents , Technology Review February 2004.

[17] SasikanthAvancha, Jeffrey Undercoffer, Anupam Joshi, JohnPinkstonSecure, Sensor networks for perimeter protection,Computer Networks 43, 2003, pp. 421-435.

[18]. Dr. Yudhvir Singh, DheerDhwaj Barak, VikasSiwach, Prabha Rani, "Attacks on Wireless Sensor Network: A Survey", IJCSMS, Vol. 12, Issue 03, Sept 2012, ISSN (Online): 2231-5268.

[19]. Hemanta Kumar Kalita1, and AvijitKar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[20].Prabhudutta Mohanty, Sangram panigrahii, Nityananda Sarmaand Siddhartha Sankar Satapathy,"Security Issues in Wireless Sensor Network Data Gathering Protocols: A SURVEY", Journal of Theoretical and Applied Information Technology © 2005 – 2010, JATIT.