ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Detection & Prevention Techniques of Sybil Attack& its Analysis in Mobile Adhoc Network

Neelam Janak Kumar Patel[1], Dr. Khushboo Tripathi[2]

Ph.D. Research Scholar, Dept. of CSE, ASET, Amity University Haryana, India[1]

Assistant Professor, Dept. of CSE, ASET, Amity University Haryana, India[2]

ABSTRACT: Wireless networking is a technology that allows users to access information electronically, regardless of their geographic position. The use of wireless communication between mobile users has become increasingly popular due to recent performance advancements in computer and wireless technologies. This has led to lower prices and higher data rates, which are the two main reasons why mobile computing is expected to see increasingly widespread use and applications. This paper proposes the algorithm to detect the Sybil node in the mobile ad-hoc networks using AODV protocol. It also shows performance of AODV with no Sybil attack, under attack & after applying our mechanism in the form of simulation result found for certain deviation of nodes in network, by allowing for enactment metrics as throughput, PDR, End to end delay & Packet loss. Simulationsare carried out using widely used simulator NS2.

KEYWORDS:AODV, PDR, Throughput, Sybil, Protocol.

I. INTRODUCTION

A wireless sensor network entails of applications such as environmental monitoring, target tracking, health monitoring, and other various maintenance options. Enactment and topology creation have become important activities in modern research work. The usage of wireless sensor network in a variety of applications is highly important with the prominence on confirming security. Still, Prevention and detection of malicious attacks of all levels may be high or low in wireless sensor network. A diversity of attacks on the network like wormholes, sinkhole, Sybil, sleep, and selective forward attacks in the network are being detected. Many researchers have recognized their own infrastructures which have portable devices, used in various trade services in decentralized and scalable methods. Some of the devices are proficient of management without the use of the internet for multiuser applications. They are used for finding the exact location in the algorithms that enhance the accuracy. The Sybil attacker misinforms other nodes by presenting wrong ID or duplicate ID of the users who are aware of the nodes in the wireless sensor network.

There are two separate approaches for assisting wireless communications between mobile hosts. The first approach is to use a fixed network structure that provides wireless access points. In this network, a mobile host communicates to the network through an access point within its communication radius. When it goes out of range of one access point, it connects with a new access point within its range and starts communicating through it. An example of this type of network is the cellular network infrastructure. A major problem of this methodology is handoff, which tries to handle the condition when a link should be smoothly handed over from one access point to another access point without perceptible delay or packet loss another issue is that networks based on a fixed infrastructure are limited to places where there exists such network infrastructure.

1.1 Mobile Ad-hoc Networks (MANET)

A wireless ad-hoc network is a collection of mobile nodes with no pre-established infrastructure. Each of the nodes has a wireless interface and communicates with others over either radio or infrared channels. Laptop computers and personal digital assistants that communicate directly with each other are some examples of nodes in an ad-hoc network. Nodes in the ad-hoc network are often mobile, but can also consist of stationary nodes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

A mobile ad-hoc network (MANET) [1] is a self-configuring network consisting of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are out of their transmission ranges in the Ad-hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks.

An ad-hoc network [2] uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad-hoc network must be willing to forward packets for other nodes. Thus every node acts both as a host and as a router. The topology of ad-hoc networks varies with time as nodes move, join, or leave the network [3]. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes.

1.2Sybil Attack

Security of mobile ad-hoc networks is one of the major issues; hence research is being done on many routing attacks on mobile ad-hoc networks [4]. The Sybil attack is particularly harmful attack in networks. In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities. In the worst case, an attacker may generate an arbitrary number of additional node identities, using only one physical device. Existing technology uses the route comparison for detecting the Sybil attack from the network. In this attack, a malicious attacker assumes multiple identities while a normal participant is allowed only one identity. This attack is facilitated when obtaining a new identity is inexpensive as is often the case in a Mobile Ad-hoc Network.

II. LITERATURE SURVEY

Security Issues in Mobile Ad Hoc Networks

Security issues and their current solutions in the mobile ad hoc network [4] are discussed. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. The main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Than the security criteria of the mobile ad hoc network and the main attack types that exist in it. The vulnerabilities to the network, issues of security and attacks [5] on the network are described.

Prevention Techniques for Sybil Attack

There are various clusters and main focus is on the path of nodes [6]. The nodes having the path almost similar to the existing cluster, those nodes are put into the corresponding cluster and the node whose path is totally different and does not match with any existing cluster, and then separate cluster is developed for that node. In this, two nodes does not have exactly the same path, if two nodes are having the same path then those nodes are detected as Sybil nodes. Sybil nodes are detected as per the path they follow. All the Sybil identities will have the same path for routing [7]. These nodes are clustered in a separate group and the nodes having similar path are detected and removed from the network.

Parental Control algorithm for Sybil detection in distributed P2P networks

Distributed social peer to peer network are most vulnerable to Sybil attack[8]. It forms a small network within the P2P network and can give unwanted results to other nodes in network, thereby decreasing the interest of non-malicious nodes in the P2P network. An algorithm which is based on reputation scheme is used for detection of Sybil nodes. It uses the false message concept for identifying and verifying the Sybil nodes in the network [9]. In Sybil attack an attacker introduces itself in the network with many P2P identities. If an attacker gets large network identities, it can control large portion of the network. When an attacker wants to join the network, it most likely to get join its other fake nodes. Hence all Sybil nodes, most likely, form a small network inside the P2P network (in case of social network). But if identity assignment scheme, in P2P network, is uniformly distributed, then it is very difficult for an attacker to

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

strategically place such Sybil nodes in network [10]. The limitation of this technique is that it is applicable to the static network only.

Semi-Centralized Multi-Authenticated RSSIBased Solution to Sybil Attack

Sybil attack is a serious threat for today's wireless adhoc networks [11]. In this attack a single node impersonates several other nodes using various malicious means [12].

Detection of Sybil Attack in Mobile Wireless Sensor Networks

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers [13]. The development of wireless sensor networks was motivated by military applications such as battle field surveillance. Today such networks are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. Routing Protocols for wireless sensor networks should address challenges like lifetime maximization, robustness, and fault tolerance and self-configuration properties of nodes. The group of nodes are created. The member node sends their id and power values to the head nodes and then the nodes with low power are chosen as receivers and their neighbouring nods are chosen as senders. The senders send packets to receivers. If there is collision that means both identities are at same location and are Sybil identities.

MANET: Vulnerabilities, Challenges, Attacks, Application

Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks [14]. Due to severe challenges, the special features of MANET bring this technology great opportunistic together.

Lightweight Sybil Attack Detection in MANET

Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed systems that may also be part of a huge complex system, such as a complex system-of-systems used for crisis management operations. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions [15]. Since MANETs [16][17] require a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network [18]. A lightweight scheme detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world tested experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

III. METHODOLOGIES

MANET is a self-governing network, consists of group of nodes that communicates with each other through wireless links. When node enters a network then it requires unique address to communicate with other nodes present in the network. As MANET is a decentralized network, so there is no authority in the network which verifies the identities of the nodes. Sometimes there are attackers who misuse this property of MANET. In this attacker uses identity of another node or some other identity to create misunderstandings between the communications of nodes present in the network or to collect some important information. This type of attacks is called Sybil attack. Sybil word itself explains the Sybil attack which means multiple identities and it is named after the famous multiple disorder patient whose name is "Sybil"(Shirley Ardell Mason). A Sybil attacker can create a lot of damage or destruction to the network in many ways like reduce the trust of the nodes by sending fake information about that node in the whole network and also create misunderstandings among the nodes by not forwarding the data which is requested by another node in the network or by changing the route of the packets. When the voting phenomenon occurs in the network then Sybil attacker can change the result by using its multiple identities behaviour and make the result according to its requirement. So it is necessary to remove the Sybil attack from the network.

According to the algorithm [8] used, there are various clusters and main focus is on the path of nodes. The nodes having the path almost similar to the existing cluster, those nodes are put into the corresponding cluster and the node

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

whose path is totally different and does not match with any existing cluster, and then separate cluster is developed for that node. In this, two nodes does not have exactly the same path, if two nodes are having the same path then those nodes are detected as Sybil nodes. The similarity of the node's path is checked by their overlapping components that how much they are overlapped. The similarity of the path [8] is checked as follows:

$$Sim(L_1, L_2) = \left(\frac{\sum_{i=1}^{k} T_{cmn_i}}{\max(T_{obs1}, T_{obs2})} \right) * \left(\prod_{i=1}^{k} \frac{T_{ovl_i}}{T_{cmn_i}} \right)$$

Here, L1, L2 are nodes
T_{obs} = Period that each node is observed
T_{cmn} = Period in which there are observations of both nodes in the observation table (commonly observed)
T_{ovl} = Period that both nodes are commonly observed and co-occurred in the same region,
k = The number of times in which they are commonly observed.
The first part of equation is used to calculate that till what time both nodes are observed commonly and second part of equation is used to determine the overlap region of the nodes.

IV. The Proposed Algorithm and Architecture

4.1 Flowchart:

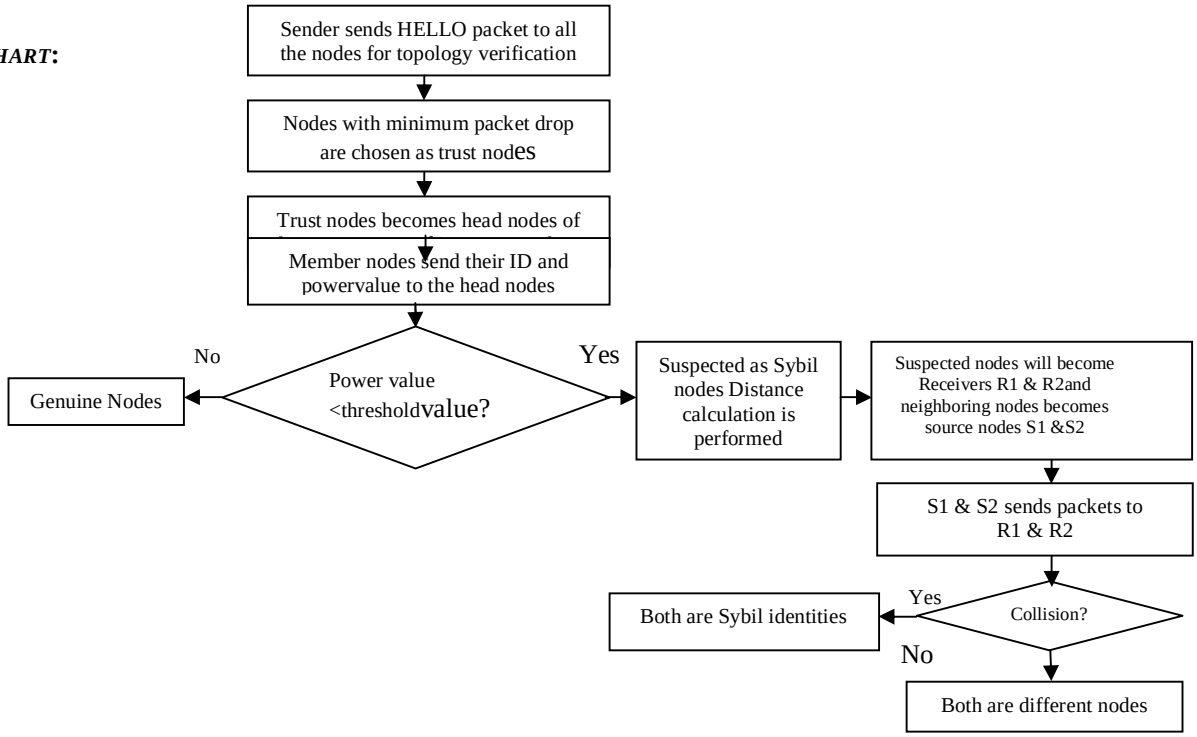


Figure 1: Flowchart of proposed algorithm to check Sybil identities

4.2*Proposed Method*

In this paper we attempt to provide a hybrid solution using a combination of two already proposed methods. According to this newly proposed method the total network will be dynamically divided into several subgroups, as

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

more and more nodes will enter the network. Each subgroup will be under the super vision of a single node, a central authority. Each subgroup will also contain Received Signal Strength Indicator[RSSI] detector nodes**.**

The sender sends HELLO packets to all the other nodes for topology verification. The nodes with minimum packet drop are chosen as the trust nodes. The trust nodes now become the head nodes with a group of its own member nodes. The member nodes send their ID and power value to the head nodes. The head node checks for nodes with power value below the threshold value. If the power value is lesser than the threshold value, those nodes are detected as Sybil nodes & distance calculation is performed according to following steps.

- These abnormal (Sybil) nodes are selected as receiver's r1, r2.
- Two nodes closer to Sybil nodes are selected as senders s1, s2.
- Packets are sent to s1 and s2 to both receivers.
- Since both the identities are present at the same node, there is collision of packets that leads to the packet drops

V. IMPLEMENTATION

Table 1: Parameter Table for 10 nodes

Parameter	Value
Nodes	10
X dimension Topography	500
Y dimension Topography	500
Simulation Time	200

Table 2: Parameter Table for 50 nodes

Parameter	Value
Nodes	50
X dimension Topography	1500
Y dimension Topography	300
Simulation Time	200

10 nodes:

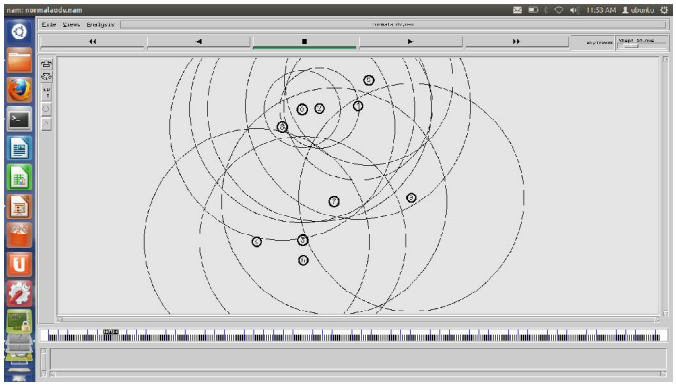


Figure 2(a)Original AODV [18] Routing Protocol-10 nodes

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

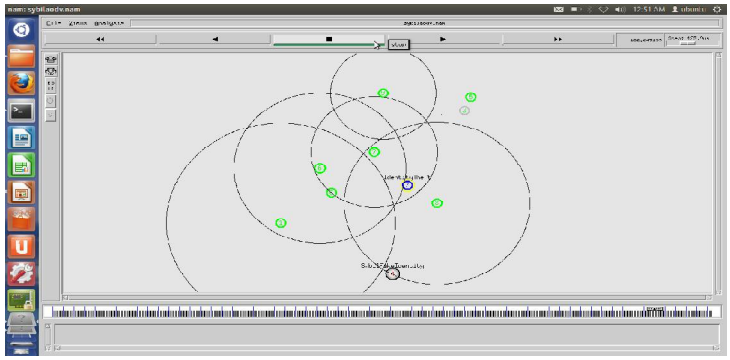


Figure 2(b)AODV Routing Protocol with Sybil Attack-10 nodes

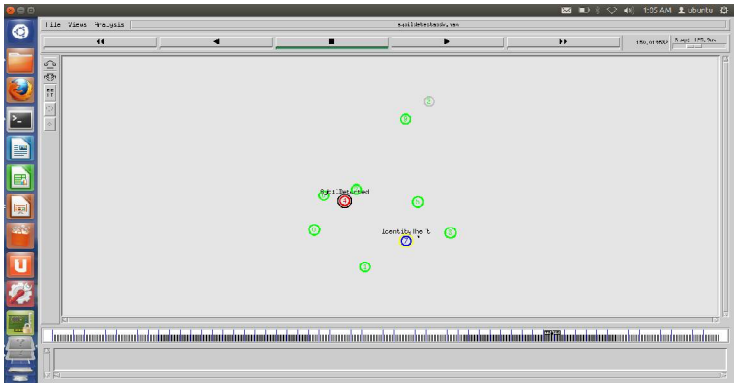


Figure 2 (c) AODV Routing Protocol Sybil Attack Detected-10 nodes

Figure 2: (a) Original AODV Routing Protocol, (b) AODV Routing Protocol with Sybil Attack, (c) AODV Routing Protocol Sybil Attack Detected

50 nodes

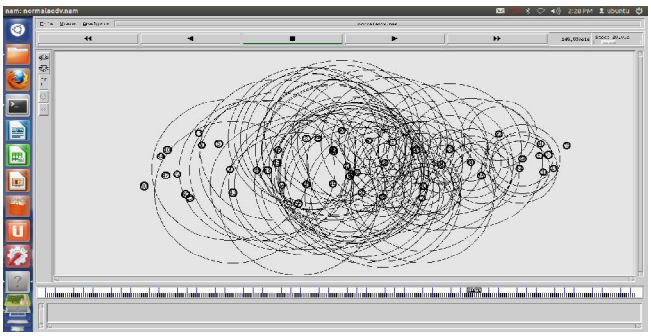


Figure 3(a)Original AODV Routing Protocol-50 nodes

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

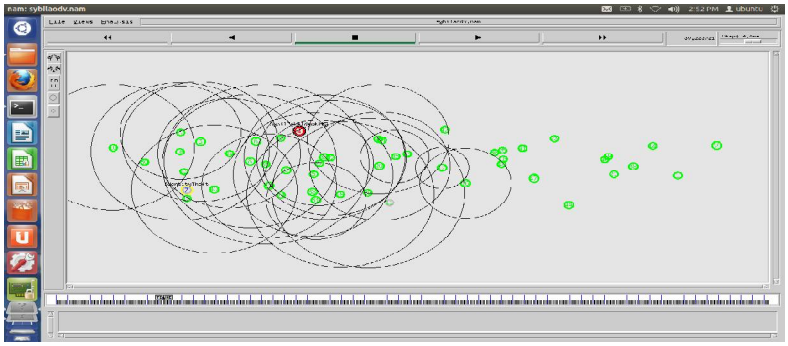


Figure 3(b)AODV Routing Protocol with Sybil Attack-50 nodes

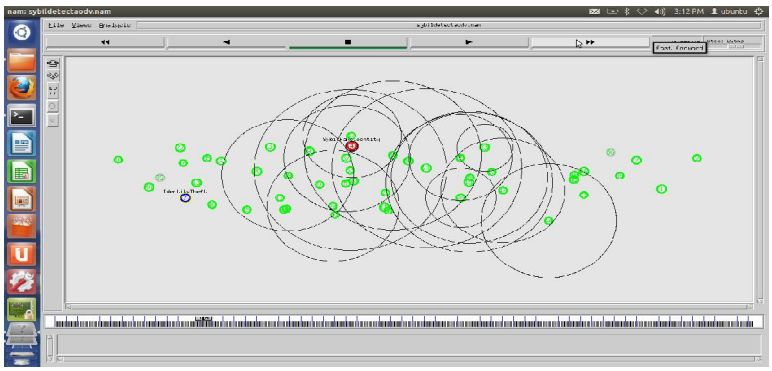


Figure 3(c)AODV Routing Protocol Sybil Attack Detected-50 nodes

Figure 3: (a) Original AODV Routing Protocol, (b) AODV Routing Protocol with Sybil Attack, (c) AODV Routing Protocol Sybil Attack Detected

VI. EXPERIMENTAL RESULTS

The entire system model is simulated using NS2 software with 10 and 50 nodes with a different network topology. We are comparing the different parameters like packets received ratio, packet dropped, delivery rate, Average end to end delay and average throughput for different number of nodes for different situation like when there is no attack in the network, when attacker attacked on the network and when attack is detected and prevented.

There are number of simulation parameters which can be varied, results in change in value of different performance metrics, which can be shown in below table.

Table: 3 (a)Data Messages-10 Nodes

	Without attack	With attack	Attack detected
No. of Sent TRF_MSG	8654	8618	8585
No. of Received TRF_MSG	8620	5322	5298
No. of Dropped TRF_MSG	30	3230	3222
No. of Forwarded TRF_MSG	4365	2679	2669
Delivery Rate (%)	99.61	61.75	61.71
Packet Delivery Fraction (Received/Sent)	0.99	0.6175	0.6171
Avg. End to End Delay (second)	188.57	190.26	197.42
Average Throughput (kbps)	86.74	45.59	53.79

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Table: 3 (b)Data Messages-50 Nodes

	Without attack	With attack	Attack detected
No. of Sent TRF_MSG	556	556	564
No. of Received TRF_MSG	450	284	284
No. of Dropped TRF_MSG	102	96	87
No. of Forwarded TRF_MSG	903	900	990
Delivery Rate (%)	80.94	51.08	50.35
Packet Delivery Fraction (Received/Sent)	0.8094	0.5108	0. 5035
Avg. End to End Delay (second)	147.613	147.701	149.139
Average Throughput (kbps)	20.21	10.22	11.96

Table 3: Comparison Table of Data Messages analysis for Original AODV, with under attack and attack detected (a) 10 nodes (b) 50 nodes

VII. GRAPHICAL COMPARISON OF RESULTS

10 nodes **50 nodes**

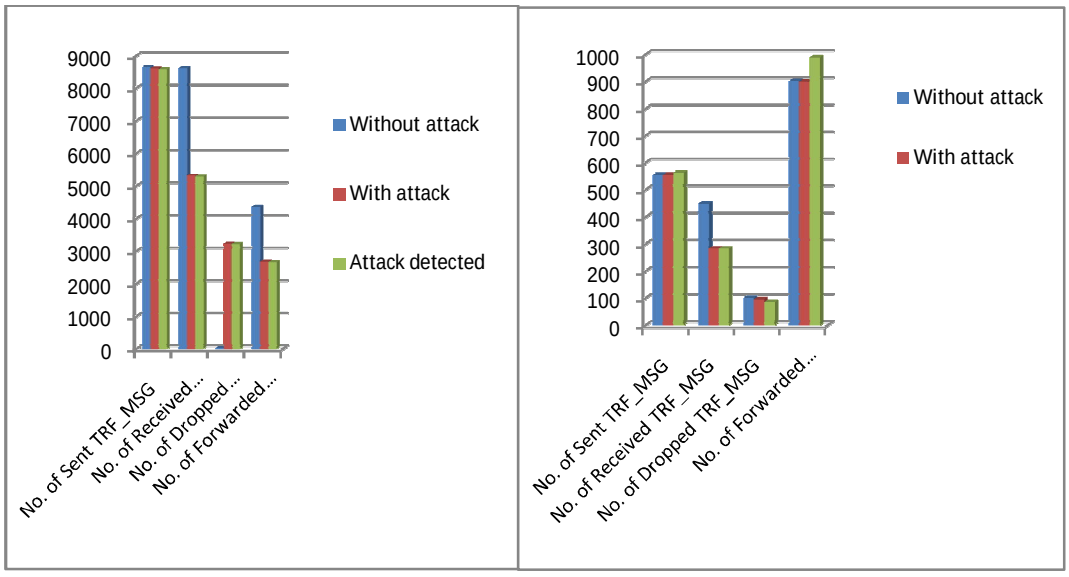


Figure4 (a)ComparisonGraph of Data Messages analysis without attack, with attack and attack detected for 10 nodes and 50 nodes

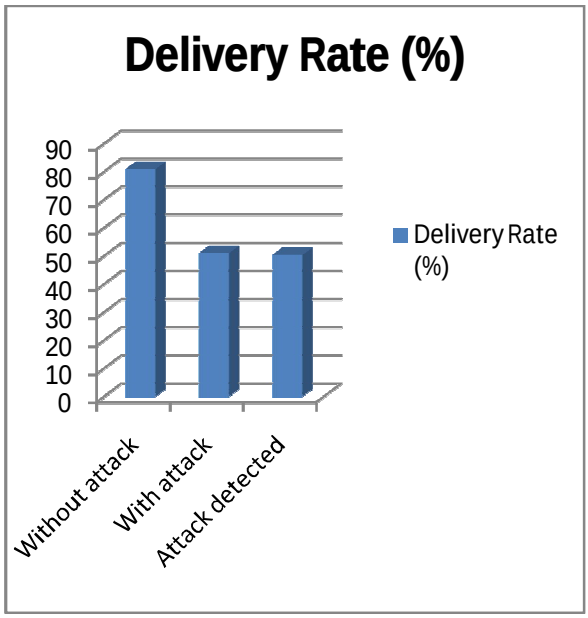
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

10 Nodes



50Nodes

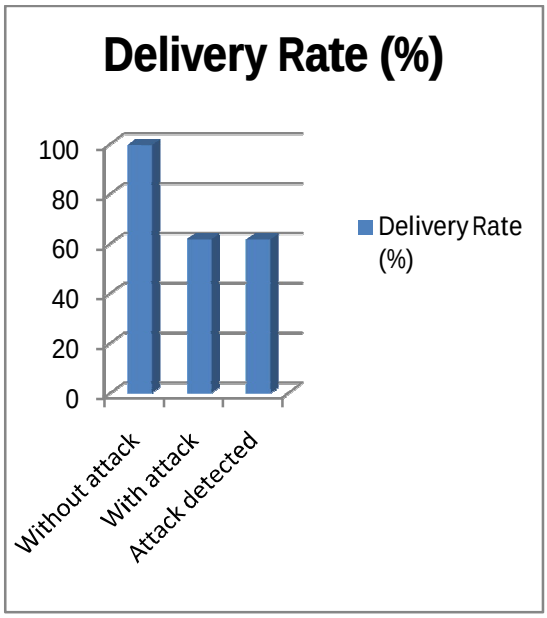


Figure4 (b)Delivery Rate

Analysis

From above graph Figure 6(b) we can say that value of PDR is increasing linearly for original AODV when we vary number of nodes from 10 to 50 as well PDR values for Sybil AODV is low & decreases sharply for same node variation if we compare PDR values for original AODV. At the same time values of PDR for secure AODV is improved compare to Sybil AODV when we vary nodes from 10 to 50. Thus we can say that PDR of AODV is improved for secure AODV which degraded due to Sybil attack.

10 Nodes

50 Nodes

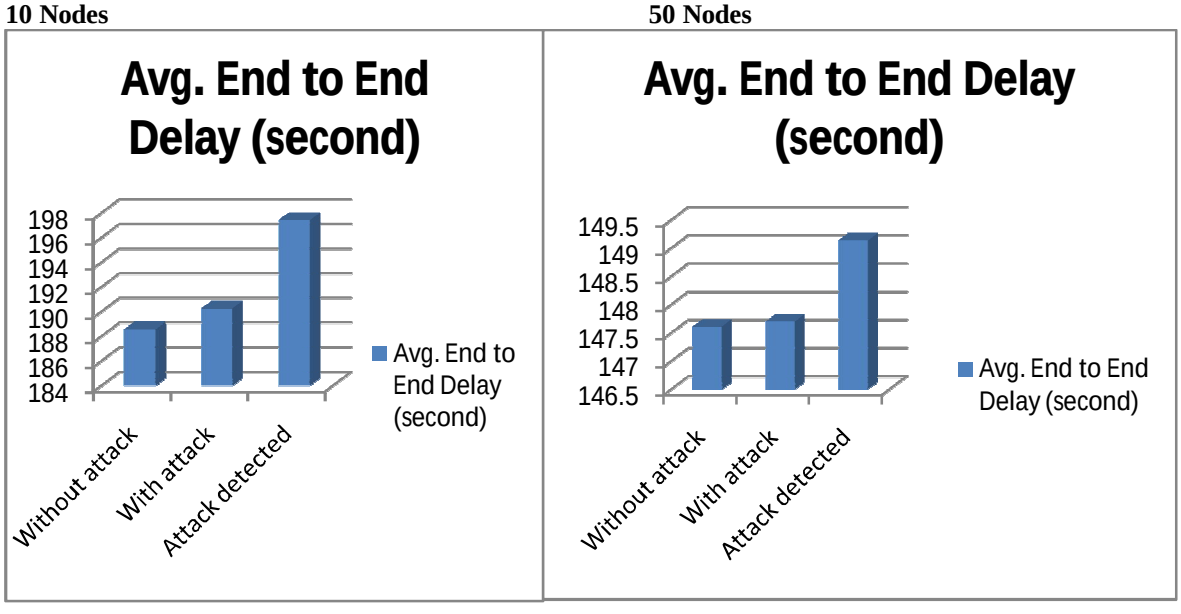


Figure4 (c)Average end to end delays

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Analysis

From above graph Figure 6 (c) we can say that value of end to end delay for original AODV is decreasing but not constantly when we vary number of nodes from 10 to 50, end to end delay for Sybil AODV is high compare to original AODV, but at same time, end to end delay for secure AODV is improved compared to Sybil AODV when we vary number of nodes from 10 to 50. Thus we can say that end to end delay of AODV is improved for secure AODV which degraded due to Sybil attack.

10 Nodes **50 Nodes**

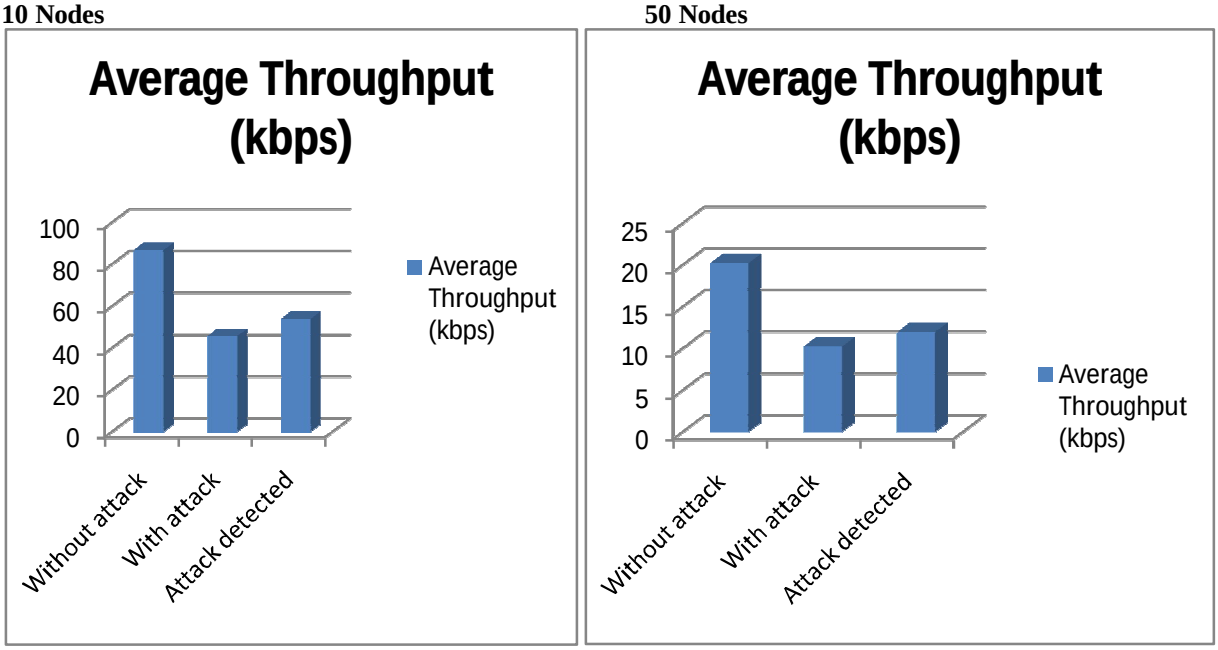


Figure:4 (d)Average throughputs

Analysis

From above graph we can say that, the throughput fororiginal AODV is continuously increasing when we varynumber of nodes from 10 to 50 at same time its value for Sybil AODV is low compare to original AODV for samevariation of nodes but its value for secure AODV isimproved compare to Sybil AODV for node variation of10 to 50.Thus we can say that throughput of AODV isimproved for secure AODV which degraded due to Sybil attack.

VIII. CONCLUSION & FUTURE WORK

There is rapid grow and change in the field of MANETs. While there are still many challenges that need to be met, it is likely that such networks will observe widespread and extensive use within the next few years. One of these challenges is security. Security of mobile ad hoc networks has recently gained momentum in the research community. Security solutions for MANET have to cope with a challenging environment including limited energy and computational resources. With the above proposed work, the attacks which cause the damaged to the network are being easily detected. In this method 50 mobile nodes are used. In which there is one malicious node. For future work we can change the parameters and get the results for our proposed methodology and analyse it for security purpose. Like, Change the MANET area, Change the number of total participating nodes, and Change the number of malicious identities, Change the simulation time.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

REFERENCES

[1] AnamikaPareek, Mayank Sharma, "Architecture for Detection of Sybil Attack in MANET Using Mac Address", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349- 2163 Issue 6, Volume 2 (June 2015).
[2] RoopaliGarg, HimikaSharma, "Lightweight Sybil Attack DetectionTechnique in MANET", International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering, Vol. 3, Issue 5, May 2014.
[3] AmolVasudeva, Manu Sood, "Sybil Attack on Lowest id Clustering Algorithm in the Mobile Ad Hoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.
[4] Pooja,Manisha, et al., "Security Issues and Sybil Attack in Wireless Sensor Networks", International Journal of P2P Network Trends and Technology- Volume3, Issue1- 2013.
[5] Ankit Gupta, Deepak Sukheja et al., "Securing AODV for Defending Sybil Attack in MANET", International Journal of Scientific Engineering and Research (IJSER), Volume 3 Issue 10, October 2015
[6] AnamikaPareek, Mayank Sharma, "Detection and Prevention of Sybil Attack in MANET using MAC Address", International Journal of Computer Applications (0975 – 8887) Volume 122 – No.21, July 2015
[7] John R. Douceur, "The Sybil Attack", Microsoft Research.
[8] RoopaliGarg, HimikaSharma, "Prevention Techniques for Sybil Attack", International Journal of Computers & Technology.
[9] Anil ManoharDogra, Rajvirsingh, "Zone Based Analysis of ZRP under varying mobility and Transmission Range in MANETs", International Journal of Engineering and Computer Science ISSN:2319-7242 Volume 3 Issue 2 February, 2014 Page No. 4007-4016.
[10] AnkushTehale, AmitSadafule et al. "Parental Control Algorithm for Sybil detection in distributed P2P networks", International Journal of Scientific and Research Publications, Volume 2, Issue 5, May 2012.
[11] RoopaliGarg and Himika Sharma "Comparison between Sybil Attack Detection Techniques: Lightweight and Robust", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014.
[12] HimadriNathSaha, Dr.Debika Bhattacharyya, et al., "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack", International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 338 Volume 1, Issue 4, December 2010.
[13] S.Sharmila1, Uma Maheswari, "Detection of Sybil Attack in Mobile Wireless Sensor Networks", International Journal of Engineering Science & Advanced Technology Volume-2, Issue-2, 256 – 262.
[14] Aarti,Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X .
[15] Sohail Abbas, MadjidMerabtiet al.,"Lightweight Sybil Attack Detection in MANETs",IEEE Systems Journal, Vol. 7, NO. 2, JUNE 2013
[16] Buttyan, L.,J. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Network," ACM Mobile Computing and Communications Review, 7(1), 2003 pp. 74 – 94.
[17] Neelam J. Patel, "Detection & Prevention Techniques of Sinkhole Attack in Mobile Adhoc Network: A Survey," International Journal of Latest Research in Engineering and Technology (IJLRET) ISSN: 2454-5031, www.ijlret.com, Volume 2, Issue 4, April 2016, PP 50-54
[18] Neelam Janak kumar Patel, Dr. Khushboo Tripathi, "Sinkhole Attack Detection and Prevention in WSN & Improving the Performance of AODV Protocol," International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE),ISSN(Online): 2320-9801, Vol. 4, Issue 5, and May 2016