International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 5,May 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Detecting Sybil attack using AODV in MANET

Nirmal Patel[1], Pratik Modi[2]

[1]*Department of Computer Engineering, LDRP-ITR, 09.nirmal@gmail.com*
[2]*Department of Computer Engineering, LDRP-ITR, pratik1031@gmail.com*

[1,2]*KSV University*

Abstract- In mobile ad-hoc networks (MANET) security is a challenging issue because of its open nature, framework less property and portability of hubs. In designing new security techniques for mobile ad-hoc networks, one must think about the attacks and in addition the characteristics of that attacks that could be started against the mobile ad-hoc networks and existing detection systems. Mobile ad-hoc network is vulnerable to different kind of attacks. To provide safe data transmission the security must be provided against these attacks.

Keywords -Mobile ad hoc networks; Vulnerabilities of MANET; Sybil attack; AODV

I. INTRODUCTION

A Mobile Adhoc Network (MANET) is a collection of independent mobile nodes connected by wireless links. The nodes communicate to each other via radio waves. The mobile nodes that are in range of each other can communicate directly. The nodes that are not in the range needs the intermediate nodes to route the packet in order to communicate. These networks are distributed and do not need any kind of help. The MANET is infrastructure less.

The nodes can communicate without a fixed infrastructure. The nodes create a topology that is dynamic. In MANET the nodes are mobile. Any node can join or leave the network at any time, so it doesn't have any fixed topology. Figure 1 shows a simple ad hoc network with four nodes. Node A and node C are not within the range of each other. But the node B acts as a router and packets can be forwarded between A and C. Similarly nodes C and D are not within the range of each other. Here also B is an intermediate node, so it will forward the packet between C and D. This is an example of ad hoc network. MANET supports dynamic topology. That is, nodes are free to move randomly with different speed. Thus, the topology may change at unpredictable time. This is a unpredictable time.

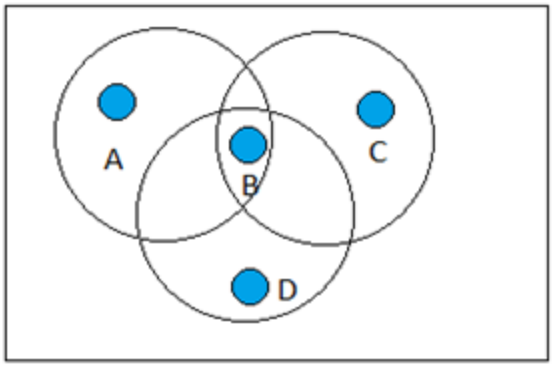

Figure 1: Example of MANET

II. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

A. Lack of Secure Boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defence in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network[8].

B. Limited resources

Resource constraints are a further vulnerability. There can be a variety of devices on MANETs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of new attacks. For example, mobile nodes generally run on battery power. This has led to emergence of innovative attacks targeting this aspect. Furthermore, introduction of more security features into the network increases the computation, communication, and management load. This is a challenge for networks that are already resource constrained.[8]

C. Cooperativeness

Routing algorithms for MANETs usually assume that nodes are cooperative and non malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. For example, a node can pose as a neighbour to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly.[8]

D. Dynamic topology

MANET nodes can leave and join the network, and move independently. As a result, the network topology can change frequently. It is difficult to differentiate normal behaviour of the network from anomaly/malicious behaviour in this dynamic environment. For example, a node sending disruptive routing information can be a malicious node, or else simply be using outdated information in good faith. Moreover, mobility of nodes means that we cannot assume nodes, especially critical ones (servers, etc.), are secured in locked cabinets as in wired networks. Nodes with inadequate physical protection may often be at risk of being captured and compromised.[8]

E. Wireless links

First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks. Furthermore, wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.[8]

III. SYBIL ATTACK

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.[1]

IV. EXISTING WORK

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 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 is checked[3].

V. PROPOSED ALGORITHM

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 receivers 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.

The above algorithm detects the Sybil node from the network using the neighboring nodes for the data transfer and then by observing the data collision. There would be collision of data packets on the Sybil node as Sybil node represents multiple identities on a single node. If both the identities are at the same node then there would be collision.

VI. RESULTS

Packet Delivery Ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. The Fig.2 shows that PDR is heavily affected.

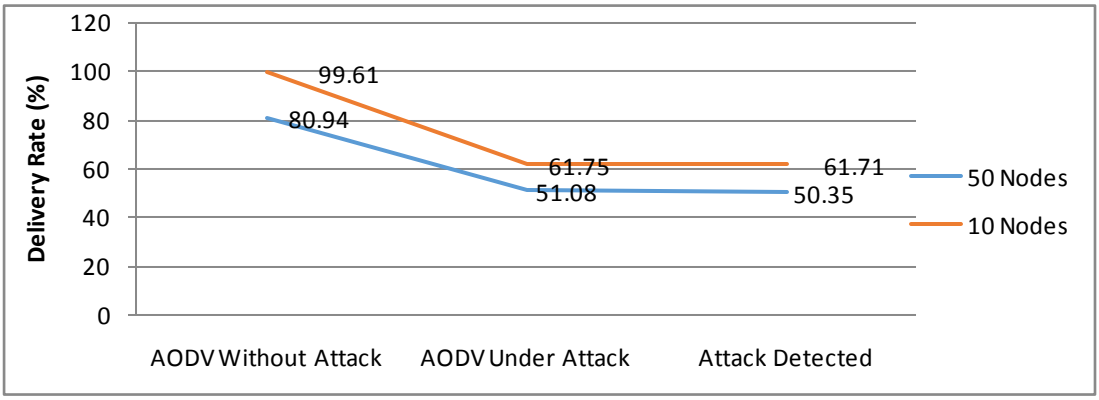

Figure 2: Packet Delivery Ratio (PDR)

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition,

buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.

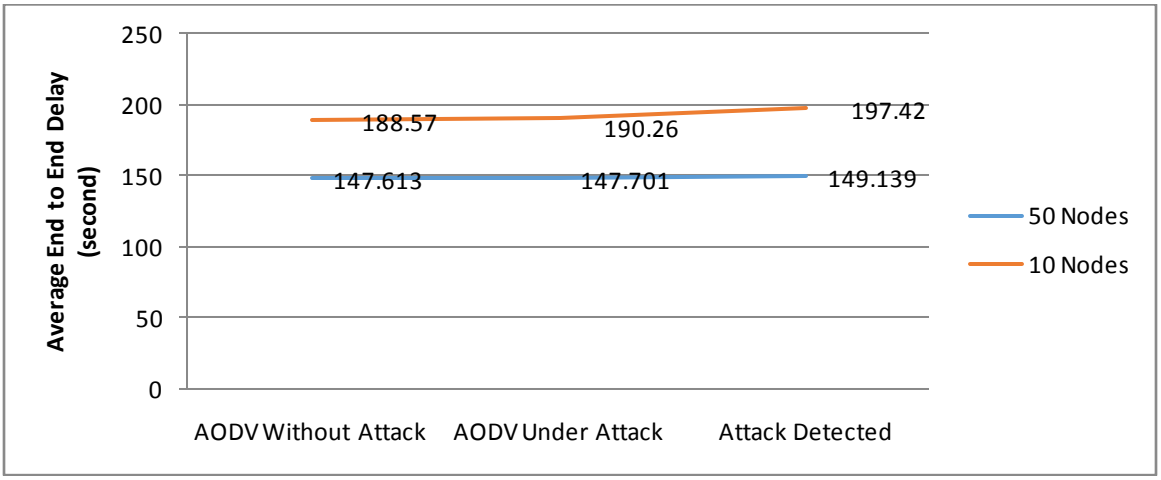

Figure 3: End-to-end Delay

VII. 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 below parameters and get the results for our proposed methodology and analyze it for security purpose. Like, Change the MANET area, Change the number of total participating nodes, Change the number of malicious identities, Change the simulation time.

REFERENCES

[1] www.wickipedia.com
[2] John R. Douceur, The Sybil Attack, Microsoft Research
[3] Roopali Garg and Himika Sharma, Prevention Techniques for Sybil Attack,
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
[4] Anil Manohar Dogra, Rajvir singh, ZONE BASED ANALYSIS OF ZRP UNDER VARYING MOBILITY AND RANSMISSION RANGE IN MANETs, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 February, 2014 Page No. 4007-4016
[5] Ankush Tehale, Amit Sadafule, Swapnil Shirsat, Rahul Jadhav, Satish Umbarje, Sandip Shingade, Parental Control algorithm for Sybil detection in distributed P2P networks,
International Journal of Scientific and Research Publications, Volume 2, Issue 5, May 2012
[6] Chris Piro Clay Shields Brian Neil Levine, Detecting the Sybil Attack in Mobile Ad hoc Networks
[7] Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering, Security Issues in Mobile Ad Hoc Networks- A Survey, University of Maryland, Baltimore County
[8] MANET: Vulnerabilities, Challenges, Attacks, Application [Priyanka Goyal, Research Scholar, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India Vinti Parmar, Dept. of CSE, Technological Institute of Textile and Science, Bhiwani, Haryana, India Rahul Rishi, Dept. of CSE, Technological Institute of Textile and Science,

Bhiwani, Haryana, India]
[9] Alice Cheng, Center for Applied Mathematics Cornell University, Ithaca, NY 14853 and School of Operations Research and Industrial Engineering, Cornell University, Ithaca, NY 14853 , Sybilproof Reputation Mechanisms.
[10] Chuang Lin, Yuanzhuo Wang, Yang Wang, Haiyi Zhu, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, P.R. China, Stochastic Game Nets and applications in Network Security
[11] Lesniewski-Lass, C. (Apr. 2008) "A Sybil-proof one-hop DHT," in *Proc.ACM SocialNets*, Glasgow, Scotland.
[12] Sieka, B. (2006) "Using Radio Device Fingerprinting for the Detection of Impersonation and Sybil Attacks in Wireless Networks," in *Proceedings of ESAS*.
[13] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, Carnegie Mellon University, The Sybil Attack in Sensor Networks: Analysis & Defenses
[14] 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
[15] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester" An Overview of Mobile Ad Hoc Networks: Applications and Challenges"
[16] Himadri Nath Saha, Dr. Debika Bhattacharyya, Dr. P. K.Banerjee, "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack", *International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004)* 338 v*olume 1, Issue 4, December 2010*
[17] S.Sharmila1, Research Scholar, Anna university, Tamil Nadu, India, G Umamaheswari, Assistant Professor, Department of ECE, PSG College of Technology, Tamil Nadu, India, Detection of Sybil Attack in Mobile Wireless Sensor Networks, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-2, 256 – 262
[18] Murat Demirbas, Department of Computer Science and Engineering Department State University of New York at Buffalo, Youngwhan Song, Department of Computer Science and Engineering Department State University of New York at Buffalo, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks
[19] Aarti Department of Computer Science & Engineering , MRIU Faridabad, India. Dr. S. S. Tyagi, Department of computer science & Engineering, MRIU, Faridabad, India, "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
[20] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, Lightweight Sybil Attack Detection in MANETs, IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013
[21] Buttyan, L. and J. Hubaux (2003) "Report on a Working Session on Security in Wireless Ad Hoc Network," *ACM Mobile Computing and Communications Review*, 7(1), pp. 74 – 94.

