International Journal of Modern Trends in Engineering and Research
www.ijmter.com

DETECTION OF SYBIL ATTACK USING POSITION VERIFICATION METHOD IN MANETS

Ch. Niranjan Kumar[1], N.Satyanarayana[2]
[1] *CSE, Sumathi Reddy Institute of Technology for women, Telangana*
[2]*Professor, Dept. of CSE, Nagole Institute of Technology and Science, Hyderabad*

Abstract— Compared to wired networks, Ad hoc networks are more vulnerable to security attacks due to the lack of trusted centralized authority, lack of trust relationships between nodes. This paper focuses on Sybil attack and its detection. A malicious node can generate and control a large number of logical identities on a single device. This gives the illusion to network as these are different legitimate nodes. An algorithm is proposed using position verification to detect the Sybil attack. The algorithm is implemented in Network Simulator and the throughput, and packet delivery ratio with and without Sybil attack.

Keywords- Sybil attack; AOMDV; wireless ad hoc networks; position verification and NS2.

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self managed without any infrastructure. Ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. Ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AOMDV (Ad-hoc On-Demand multipath Distance Vector), AODV, DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

Compared to wired networks, Ad-hoc networks are more vulnerable to security attacks due to the lack of trusted centralized authority, lack of trust relationships between nodes, easy eavesdropping, dynamic network topology, low bandwidth, battery and memory constraints of the devices. The attacks can be of many types where protocol compliant attack called Sybil attack is one of the most difficult attacks to detect.

II. ADHOC NETWORK FEATURES

Ad-hoc networks are best suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective [8]. The initial development of Ad-hoc networks was primarily driven by military applications where rapid network formation and survivability are key requirements. On the other hand, distributed network architecture with all nodes having equal responsibility and using broadcast radio is ideally suited to the military requirements. To overcome the limited radio transmission ranges (i.e. Not all nodes are within the range of every other node) nodes are equipped with the ability to forward information on behalf of others i.e. multi-hop communications. Combined with packet switching technology and suitable medium access control protocols, multi-hop communication provides the basis for resilient, large-scale military ad-hoc networks.

- Independence from central network administration
- *Self-configuring*, nodes are also routers

- *Self-healing* through continuous re-configuration
- *Scalable:* Accommodates the addition of more nodes
- *Flexible*: Similar to being able to access the Internet from many different locations.

III. ATTACKS ON WIRELESS ADHOC NETWORKS

Malicious and selfish nodes are the ones that fabricate attacks against physical, data link, net work, and application-layer functionality as shown in Table 1. Current routing protocols are exposed to active and passive attacks [1].

*Active attacks***:** In an active attack, information is inserted into the network and thus the network operation or some nodes may be harmed. Through which the misbehaving node has to bear some energy costs in order to perform some harmful operation and nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious.

*Passive Attacks***:** A passive attack does not disrupt the normal operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality gets violated. Detection of a passive attack is very difficult for the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted.

Table 1. Types of Attacks

Application layer	Repudiation, malicious code
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Black hole, Gray hole, flooding, Sybil attack
Data link layer	Traffic analysis, monitoring
Physical layer	Jamming, eavesdropping

IV. SYBIL ATTACK

Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes by doing so undermining the redundancy of many routing protocols. This attack is called the Sybil attack.

Since ad-hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have a harder time to destroy the integrity of information. If the same packet is sent over several distinct paths a change in the packets incoming from one of these paths can be detected easily. Thus, isolating a possible intruder in the network becomes possible. Also, if not the same packet but pieces of related information is sent on distinct routes, an eavesdropper might have difficulties putting together the pieces of the information puzzle.

However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded. The attacker may get access to all pieces of the fragmented information or may alter all packets in the same transmission, so that the destination node cannot detect tampering anymore. In a trust-based routing environment, representing multiple identities can be abused to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it in ideal starting point for further attack.

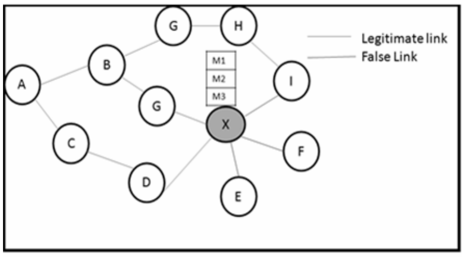


Figure 1. Sybil Attack

Sybil attack is more severe attack, in which attacker disrupts both network topology and multi-path routing protocol functionality. To disturb network topology, adversary often changes the locations with different legitimate node ids. To disturb multi-path routing, the attacker appears with multiple identities in the network, which are taken from the compromised node and appearing in most of the node disjoint paths. Figure 1. Shows the Sybil attack. In this scenario, malicious node X has three identities M1, M2 and M3 and all these identities are spoofed in passive mode. A and F are source and destination nodes need to have multipath between them. Here, malicious node will appear in all multiple paths with different identities such as (A,C,D,M1,F),(A,B,G,M2,F) and (A,B,G,H,I,M3,F).

4.1. Sybil attack on protocols

In Sybil attack, a Sybil node illegitimately claims multiple identities. A Sybil node can generate and control a large number of logical identities on a single physical device. This gives the illusion to the network as if it were different legitimate nodes[3]. It can affect following protocols.

A. Distributed Storage A Sybil attack can disrupt the architecture where data is usually replicated or fragmented on several nodes such as where distributed hash tables are used because in reality data will be stored on Sybil identities generated by the same malicious node.

B. A routing Routing mechanism in which the nodes are supposed to be disjoint is affected by Sybil identities because one node will be present in the various paths and different locations at the same time.

C. Data aggregation In a sensor network due to the lack of resources, data is often aggregated to one node. A Sybil node can change the whole aggregation reading outcome by contributing many times as a different user.

D. Voting Most often in ad hoc and peer-to-peer networks a decision is made using voting where a Sybil node can control the result by rigging the polling process using multiple virtual identities.

E. Misbehavior Detection In misbehavior detection schemes a Sybil node can increase its reputation, credit, or trust, value and can decrease the same value of the other legitimate nodes by exploiting its virtual identities. Eventually, it can diminish the detection accuracy of an intrusion detection system.

F. Traffic Congestion in a Vehicular Ad hoc Network (VANET) A malicious attacker can create the illusion of traffic congestion by spreading false information in a VANET. A malicious attacker can create an arbitrary number of virtual non-existing vehicles and transmit false information in the network to give a fake impression of traffic congestion and eventually divert the traffic unnecessarily.

4.2. EXISTING SYBIL ATTACK DETECTION SCHEMES

A. Group detection method

In Passive Ad-hoc Sybil Identity Detection (**PASID**) method [4]. A single node can detect Sybil attacks by recording the identities namely the MAC or IP addresses of other nodes it hears transmitting. Over time, the node builds a profile of which nodes are heard together, this helps reveal Sybil attackers. This method reduces false positives that can occur when a group of nodes moving together is falsely identified as a single Sybil attacker. By monitoring collisions at the MAC level, we show that we can differentiate these cases. This approach is successful because an attacker operation over a single channel can transmit only serially, whereas independent nodes can transmit in parallel creating detectably higher collision rates.

B. Trusted Certification

It is the most common solution, mainly due to its potential to completely eliminate Sybil attacks [2]. However, trusted certification relies on a centralized authority that must guarantee that each node is assigned exactly one identity, as indicated by possession of a certificate. This offers no method for ensuring such uniqueness and in practice; it has to be performed by a manual configuration. This manual procedure can be costly, and create a performance bottleneck in large-scale systems and in order to be effective, the certifying authority must guarantee the existence of a mechanism to detect and revoke lost or stolen identities. These requirements make trusted certification very difficult to implement in ad-hoc networks which lack by definition, a centralized authority that can provide the certification service.

C. Trusted Devices:

The use of trusted devices can be combined with trusted certification, binding one hardware device to one network entity. While this can effectively, mitigate the Sybil attack. The main issue with this approach is that there is no efficient way to prevent one entity from obtaining multiple hardware devices other than manual intervention [3].

D. Domain Specific

There are some countermeasures that are application-domain specific. For example, in [2], a detection mechanism for ad-hoc networks is proposed based on the location of each node. For an attacker with a single device, all Sybil identities will always appear to move together. However, the defense is not applicable beyond mobile networks and does not protect against malicious nodes with multiple devices.

E. Resource Testing

The main goal of resource testing is to attempt to determine if a number of identities possess fewer aggregated resources than would be expected if they were independent. In resource testing, it is assumed that each physical entity has a bounded amount of a given resource (e.g., limited bandwidth). The verifier then tests whether identities correspond to different physical entities by verifying that each identity has as much resources as an independent physical device should have. These tests include checks for computing power, storage ability and network bandwidth [5].

F. Radio Resource Testing

In this context, radio resource testing is a specific type of resource testing which relies on the assumption that the device radios are incapable of simultaneously sending or receiving on two different frequencies. This idea has been used in to counteract the Sybil attack [6]. However, the authors do not address the details that would allow them to build a protocol capable of operating in real world scenarios. Therefore, they do not present a comprehensive study on the cost and complexity of solutions based on this technique.

G. Registration

One obvious way to prevent the Sybil attack is to perform identity registration. A difference between peer-to-peer networks and wireless sensor networks is that in wireless sensor networks, there may be a trusted central authority managing the network and thus knowing deployed nodes. The central authority may also be able to disseminate that information securely to the network. To detect Sybil attacks, an entity could poll the network and compare the results to the known deployment. To prevent the Sybil attack, any node could check the list of “known-good’’ identities to validate another node as legitimate. The list of known identities must be protected from being maliciously modified. If the attacker is able to add identities to this list, he will be able to add Sybil nodes to the network.

Disadvantages

Each of the defenses against the Sybil attack that we have examined has different tradeoffs. Most defenses are not capable of defending against every type of Sybil attack [7]. Additionally, each defense has different costs and relies on different assumptions. The radio resource verification defense may be breakable with custom radio hardware, and validation may be expensive in terms of energy. Node registration requires human work in order to securely add nodes to the network, and requires a way to securely maintain and query the current known topology information.

V. PROPOSED DETECTION ALGORITHM

The proposed solution uses the position verification for detecting the attack. To mitigate the Sybil attack, we blocked the Sybil node after detecting the Sybil node. We considered AOMDV as the routing protocol used by the network. We assume the network nodes have low mobility and at the time of registration process, they will be static and a number of nodes are already present in the network. The basic assumption of our design is that each new node will come through the registration process as shown in Figure 2. The registration process will register an identity once it is confirmed through position finding process that the said identity is Sybil free, otherwise it will simply be discarded. Each node will then record these registered identities in their Registered Identity List (RIL) (each node maintains the RIL), which will therefore represent a Sybil free identity list. Each node will take or provide services, such as packet forwarding etc, only to/from the nodes that are stored in its RIL, otherwise their packets will be simply dropped.

5.1. Registration process

When a new node comes into the network its one-hop neighbors forward status information of new node with each other. Status information constitutes the signal strength of receiving messages from the new node. We can find the position of new node using signal strength. i.e., one hop neighbors will collaboratively find the position of new node by exchanging the status information with each other. By verifying the new position with register identity list, the new node is confirmed by the neighbors to be Sybil free then they will update their Register Identity list and broadcast to its neighbors to inform the neighbors about new node, otherwise it will simply discard.

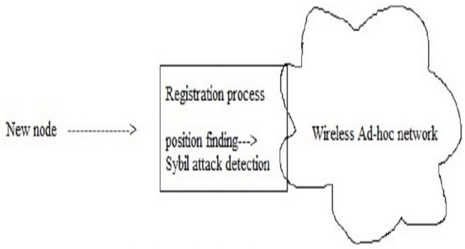


Figure 2. Sybil attack detection Scheme

5.2. Position finding process

According to Z. Sheng, etl [9] “The power received approximately decays with the square of distance.”

$$P_r \, \alpha \;\; P_t / d^2$$

Where ‘P_r’ is the received power at the receiver node, ‘P_t’ is the transmit power at the transmitter node, and‘d’ is the distance between the transmitter and the receiver. If the transmitted power is known, the receiver node can deduce the distance between them and thereby use simple geometric triangulation to locate the transmitter.

Zhong etl, 2004 showed that no node can hide its location in an environment where it is monitored by four or more nodes. Using the ratio of RSSIs from these multiple receivers, no node can hide its location from the authority that controls these monitoring nodes. The author proved as follows.

Suppose a node to be monitored transmits at the power ‘P_t’, node ’a’ will receive this signal at power

$$P_{r(a)} = \;\; P_t \, k / \, d_a^{\alpha}$$

Where ‘$P_{r(a)}$’ is the received power at the node ‘a’, ‘k’ is constant, ‘d_a’ is distance between node ‘a’ and the monitored node, and ‘α’ is the distance power gradient.

The ratio of the received signal at two different nodes, from a to b (a≠b) is

$$P_{r(a)} / P_{r(b)} = (d_a / d_b)^{\alpha}$$

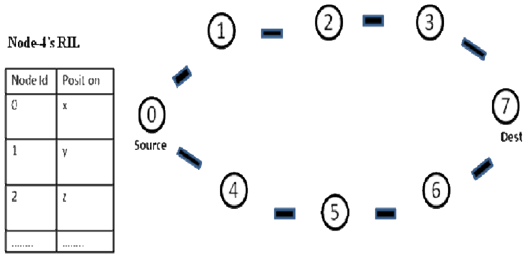
Therefore

$$d_a / d_b = \;\; (P_{r(a)} / P_{r(b)})^{1/\alpha}$$

This equation is independent of the transmit power Pt. Now assume that the position of the monitored node in two-dimensional Cartesian coordinates is (x, y), with nodes a,b,c and d positions as (x_a, y_a), (x_b, y_b) , (x_c, y_c) and (x_d, y_d) respectively. The position (x,y) can be determined by solving the following equation.

$$((x-x_a) +(y-y_a))^2 = \;\; (P_{r(a)}/ P_{r(b)})^{1/\alpha}((x-x_b) +(y-y_b))^2$$
$$= (P_{r(a)}/ P_{r(c)})^{1/\alpha}((x-x_c) +(y-y_c))^2$$
$$= (P_{r(a)}/ P_{r(d)})^{1/\alpha}((x-x_d) +(y-y_d))^2$$

Like this, one hop neighbors find the position of new node.


Node-4's RIL

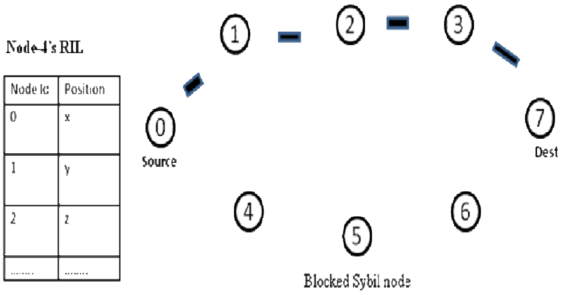
Node Id	Posit on
0	x
1	y
2	z
………	………

Figure 3. Sybil attack detection mechanism in wireless ad-hoc network

As shown in Figure 3 every node in the network maintains the RIL, which consist of node id and Position. Whenever a new node enters into the network, its one hop neighbors find the Position of new node as discussed in the Position finding process.

If new node id's position is matched with RIL's any node position, then that is the Sybil node, otherwise new node is added to RIL.RIL is broadcast to every node in the Network. Each node will take or provide services, such as packet forwarding etc, only to/from the nodes that are stored in its RIL.

After detecting the Sybil node we are blocking the Sybil node. Then source select alternative path for transferring the data to destination as shown in Fig.4. The proposed scheme will cause low communication overhead because RILs are broadcasted only when a new node registers in the network.



Node Id	Position
0	x
1	y
2	z
....	....

Figure 4. Blocking the Sybil node

VI. PERFORMANCE EVOLUTION

The simulation of the Sybil attack in wireless ad-hoc networks using an NS2 network simulator [10]. First, we explain how a node behaves like a Sybil node in wireless ad-hoc network. Figure 5. Shows a simple wireless ad-hoc network. Node-0 wants to communicate with node-7. Here, we are using AOMDV protocol (Ad-hoc on-demand multipath distance vector protocol) for route establishment [11].

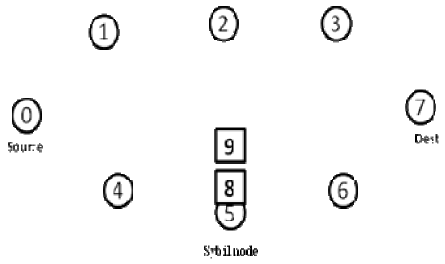


Figure 5. Sybil node in the ad-hoc network

6.1. Simulation Parameters

The parameters used in our simulation are shown in Table 2. A node is selected and given multiple identities which act as Sybil node.

Table 2. Simulation Parameters

PARAMETER	VALUE
Number of nodes	20
Simulation time	50sec
Routing Protocol	AOMDV
Queue Type	Drop Tail
Packet Size	1500 bytes
Transport protocol	TCP
Queue size	50

6.2. RESULTS

We used three simulations to analysis the implementation. In the first scenario we did not use any Sybil node. In the second scenario we added a Sybil node to the simulation. In the third scenario we added the proposed Sybil attack detection solution to attack simulation. Then we compared the performance metrics throughput, packet delivery ratio among without attack simulation, with attack simulation and attack with detection solution simulation.

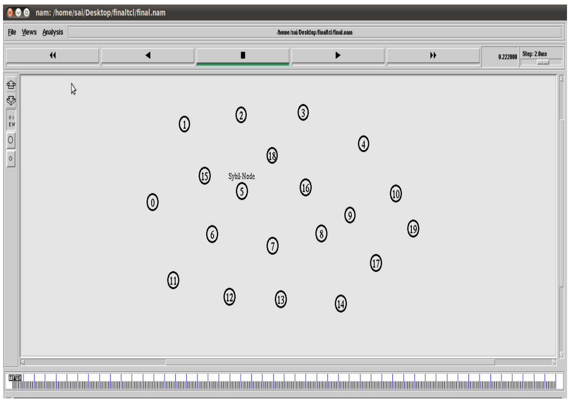


Figure 6. Ad-hoc Network setup for Implementation

6.2.1. Throughput versus Simulation Time

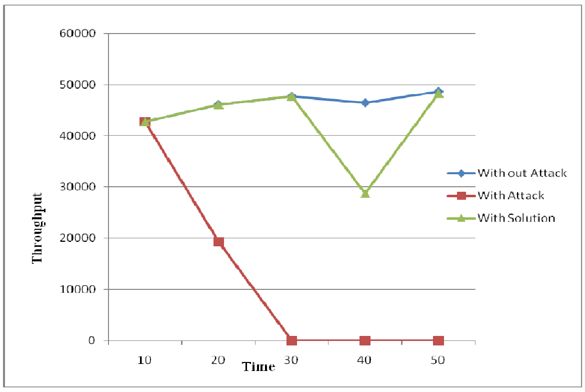


Figure 6. Throughput vs. Simulation Time

6.2.2. Packet delivery ratio versus Simulation Time

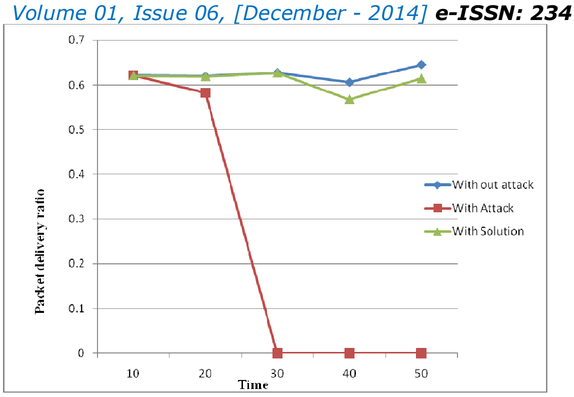


Figure 7. Packet delivery ratio versus Simulation Time

It is observed from the Figure 6,7 that our mechanism gives increased throughput and packet delivery ratio because our method block the Sybil node and choose another route after detection of Sybil attack. Using our detection mechanism with AOMDV gives increased throughput and packet delivery ratio compared to AOMDV.

VII. CONCLUSION AND FUTURE WORK

In this paper we explained the Sybil attack and position verification based mechanism for the detection of Sybil node in Wireless Ad-hoc Networks. To mitigate the attack we block the node after detecting the Sybil node. The detection mechanism is simulated using Network Simulator and found to achieve the required security. The result shows that using our detection mechanism with AOMDV gives increased throughput and packet delivery ratio compared to existing AOMDV. This is done on the wireless ad-hoc networks where the nodes are static. It can be further extended to MANET's in which nodes are not static.

REFERENCES

[1] A. Burg (2003), "Ad hoc Network Specific Attacks", Ad hoc networking: Concepts, Applications and Security Seminar, Technische Universität München, 2003.

[2] J.R Douceur (2002), "The Sybil attack", in Revised Papers from the First International Workshop on Peer-to-Peer Systems, London, UK, pp 251–260, Springer-Verlag.

[3] Levine B.N, Shields C and Margolin N.B (2006), "A Survey of Solutions to the Sybil Attack", Tech report 2006-052, University of Massachusetts Amherst, Amherst, MA, October 2006.

[4] Piro, Chris, Shields, Clay, Levine and Brian Neil (2006), "Detecting the Sybil Attack in Mobile Ad-hoc Networks", IEEE Conference, Securecomm and Workshops 2006, pp 1-11.

[5] Haifeng Yu, Kaminsky M, Gibbons P.B and Flaxman A.D (2006),"SybilGuard: Defending Against Sybil Attacks via Social Networks" , IEEE conference on Networking, IEEE/ACM Transactions, Volume: 16, pp 576–589.

[6] J Newsome, Elaine Shi, Dawn Song, A. Perrig (2004), "The Sybil attack in sensor networks: analysis & defenses" ,IEEE conference, Information Processing in Sensor Networks, IPSN 2004,Third International Symposium 2004, pp 259–268.

[7] J. Wang, G. Yang, Y. Sun and S. Chen (2007), "Sybil Attack Detection Based on RSSI for Wireless Sensor Network", in *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'07)*, 2007, pp 2684-2687.

[8] Ilyas, M. & R. Dorf (Eds.) (2003)," The handbook of ad hoc wireless networks", Boca Raton,FL, USA: CRC Press, Inc.

[9] Z. Sheng, L. Li, L. Yanbin and Y. Richard (2004), "Privacy-Preserving Location based Services for Mobile Users in Wireless Networks", Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297, 2004.

[10] UC Berkeley and USC ISI (1998), "The network simulator ns-2", Part of the VINT project, http://www.isi.edu/nsnam/ns.

[11] Marina, M.K, and Das S. R (2001), "On-demand Multipath Distance Vector Routing for Ad Hoc Networks" *Proc. of 9th IEEE Int. Conf. On Network Protocols*, pp 14-23.