IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 4, Ver. II (Jul-Aug. 2014), PP 27-37
www.iosrjournals.org

Identity Based Replicated Node Detection and Localization in Wireless Network

Deepa Hurali[1], Prof. Vidya R. Kulkarni[2]
[1]*Computer Science, KLS Gogte Institute of Technology, Udyambag, Belgaum Karnataka*
[2]*MCA, KLS Gogte Institute of Technology, Udyambag, Belgaum Karnataka*

Abstract: *Wireless networks are more prone towards identity-based attacks, especially the spoofing attacks. These spoofing attacks can further cause many other forms of attacks such as rouge access point attack and denial of service attacks (DOS). Hence the performance of the network is significantly impacted by them. Identity of the node can be verified through cryptographic authentication; however the conventional security approaches are not always possible because it requires infrastructural overhead and key management. In this paper we propose a method for detecting the spoofing attacks. This method utilizes MD5 (Message Digest 5) algorithm, which generates unique identification keys for all the nodes in the network. These unique keys are used as a basis for detecting the attacks and determining the actual number of attackers in the network and to localize these adversaries. Results of the project show that, the proposed method effectively detects the attack and locates the position of the adversaries performing the attack. There by it provides strong evidence to the effectiveness of the proposed method.*

Keywords: *Wireless network security, spoofing attack, Message Digest 5(MD 5), attack detection, localization.*

I. Introduction

Wireless networks are vulnerable to spoofing attacks and the transmission medium of wireless network is openness in nature. Due to this nature, adversaries can monitor any transmission. Further, the attackers can purchase the devices costs very low and use these platforms to launch variety of attacks. Among them identity based spoofing attacks are very easy to launch and can significantly impact the performance of the network. Spoofing attack is a technique in which an attacker forges its identity to masquerades as another device. i.e., the situation in which one entity tries to behave like another entity. The Figure 1 shows an example of spoofing.

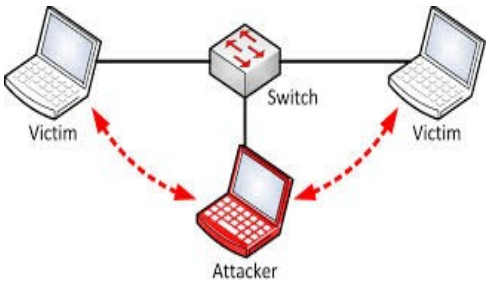

Figure 1: an example of spoofing

Here in the above figure the attacker has spoofed the identity of the victim and is sending the packets to a computer through this spoofed identity only. But, the victim is unaware of spoofing and thinks that the packet is coming from the trusted source only. Spoofing is used to gain unauthorized access to a computer.

1.1 Types of Spoofing

1.1.1 IP Spoofing

IP stands for Internet Protocol and it is used to transfer messages over the Internet [3]; it is a network protocol which operates at layer 3 of the OSI model. IP spoofing involves modification to the packet header with forged source IP address, a checksum and the order value. The diagram below shows the example of IP spoofing.

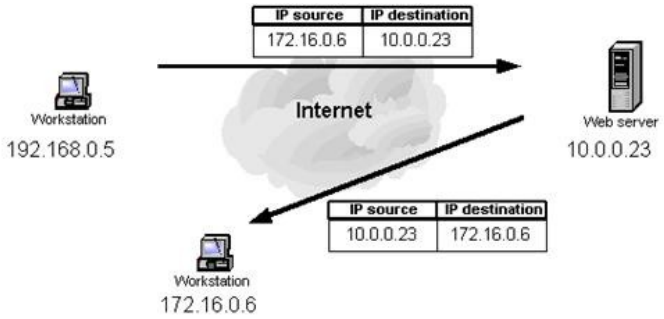

Figure 2: an example of IP spoofing

In the Figure 2 the attacker has spoofed the source IP address and is sending the packets to a computer through this spoofed address only. But, the victim is unaware of spoofing and thinks that the packet is coming from the trusted source only. Spoofing is actually used to gain an unauthorized access to a computer.

1.1.2 ARP Spoofing

ARP stands for Address Resolution Protocol (ARP). ARP Spoofing is a type of attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. As a result the attacker's MAC address will be linked with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address the attacker will begin receiving any data that is intended for that IP address.

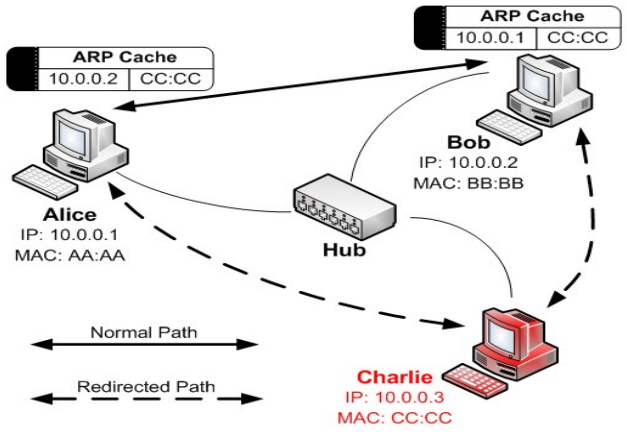

Figure 3: an example of ARP Spoofing

In the Figure 3 the cache table is shown for both the legitimate users. It consists of MAC and IP address. The attacked named Charlie sends falsified ARP messages and hence attackers MAC address is linked to the legitimate IP address. Once the addresses are linked attacker receives data that was intended for legitimate users

1.1.3 Web Spoofing

In Web spoofing false information is provided to the victim by an attacker. Web Spoofing is an attack that allows someone to view and modify all web pages sent to a victim's machine.The figure below shows an example for Web spoofing.

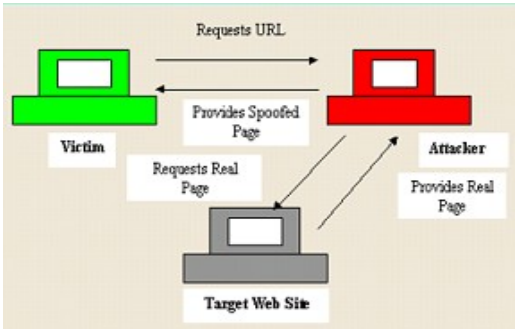

Figure 4: an example of Web spoofing

1.1.4 DNS Spoofing

DNS spoofing is a term used when a DNS server accepts and uses incorrect information from a host that has no authority giving that information. DNS spoofing is in fact malicious cache poisoning where forged data is placed in the cache of the name servers. Spoofing attacks can cause serious security problems for DNS servers vulnerable to such attacks, for example causing users to be directed to wrong Internet sites or e-mail being routed to non-authorized mail. The figure shows an example for DNS spoofing.

Figure 5: an example of DNS spoofing

II. Literature survey

The traditional approaches employ cryptographic based authentication to prevent spoofing attacks in the network [4][5]. B.Wu et al. [4] proposed a secure and efficient key management (SEKM) framework. This framework was for mobile ad hoc networks and it builds a public key infrastructure (PKI) by applying a secret sharing scheme and by using an underlying multi-cast server groups. In SEKM, each server group will create a view of the corticated authority (CA) and then provides corticated update service for all nodes, including the server. A new scheme called ticket scheme is introduced for efficient corticated service. In addition to that an efficient server group updating scheme is also proposed. The performance of the framework is evaluated through simulation.

An authentication framework is proposed in [2] by Bhoge and Trappe. This framework is for hierarchical, ad hoc sensor networks. They proposed a scheme which energy efficient, and distributed. This scheme was introduced to secure the multicast messages from the middle-tier nodes. The scheme does not require any prior knowledge about the hierarchical relation between middle-tier nodes and lowest-tier nodes. Extensive simulations are conducted to evaluate the scheme, and the results show that the scheme is energy efficient. However, the cryptographic authentication may not always be applicable because they require key management and infrastructure overhead.

Recently new approaches were proposed and they utilized physical properties associated with wireless transmission to detect attacks present in the wireless network. A channel based authentication scheme was proposed by L. Xiao et al. [10] to discriminate between transmitters at different locations, and thus to detect the spoofing attacks present in the network. Brik et al. [11] focused on building fingerprints. The fingerprints were built for 802.11b WLAN NICs and were built by extracting radiometric signatures, such as phase errors, frequency magnitude and I/O origin offset to defend against identity attacks. However in wireless network there is an additional overhead associated with radiometric signature association and wireless channel response. Ferreri et al. [3] describe possible denial of service attacks for infrastructure wireless 802.11 networks. Here the authors say that, to carry out such attacks only commodity hardware and software components are required. The

results show that the vulnerabilities exist in various access points and the result also shows that a single malicious station can easily modify any legitimate communication within a basic service set. D. Faria and D.

The works that are closely related to our work are [16], [9]. J. Yang et al. in [16] have developed a DEMOTE system. This system detects the attacks present in the network using RSS traces. DEMOTE system utilizes an unsupervised threshold approach to find an optimal threshold so that the RSS trace of a node identity can be portioned into two classes. However this method can only detect the presence of the attack the localization of the attack is not performed. Y. Chen et al. in [9] proposed a method for both detecting the spoofing attacks, as well as for locating the positions of adversaries who is performing the attacks. They first proposed an attack detector for wireless spoofing that utilized K-means cluster analysis. Next, they described about how they integrated their attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. However this method could only localize single attacker. If multiple adversaries were present in the network then the method failed to locate such multiple adversaries.

Although these methods have varying detection and false alarm rates, none of these approaches provide the ability to localize the positions of the multiple spoofing attackers after detection. Further, Wade Trappe et al. in [17] proposed a method that used spatial information and a physical property as a basis for detecting the spoofing attacks. The method also located the position of the attackers in the network. Our work differs from previous work because the proposed system utilizes MD5 (Message Digest 5) algorithm, which generates unique identification keys for all the nodes in the network. These unique keys are used as a basis for detecting the attacks and determining the actual number of attackers in the network and to localize these adversaries. Results of the project show that, the proposed method effectively detects the attack and locates the position of the adversaries performing the attack. There by it provides strong evidence to the effectiveness of the proposed method.

III. Proposed method

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. Depending on the context, Systems Architecture can in fact refer to:

- The architecture of a system, i.e. a model to describe/analyze a system
- Architecting a system, i.e. a method to build the architecture of a system
- A body of knowledge for "architecting" systems while meeting business needs, i.e. a discipline to master systems design.

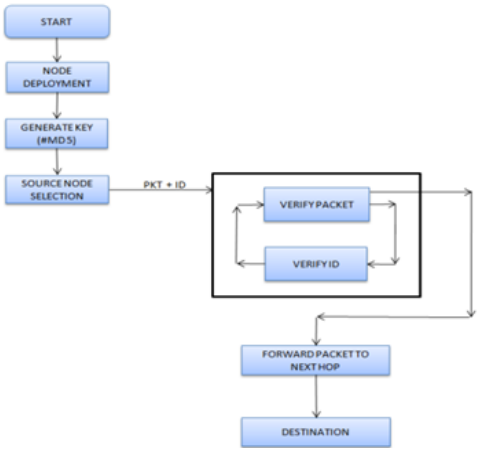

Figure 6: System Architecture

The system architecture is shown in the Figure 6 Steps for the work process of the proposed system is as below:

1. Create the nodes
2. Generate keys for all the nodes and assign the keys to the nodes.
3. Among the nodes created, select one node as the source node.
4. Verify the key ID of the node.
5. If the key is valid send packet to next hop.
6. If the key is not valid then drop the packet.

Initially the nodes are generated randomly then using MD5 the keys are generated. Once keys are generated they are assigned to all the nodes present in the network. Among the nodes present in the network one node is selected as the source node. Then the packet is sent along with the key ID to the cluster head, the cluster head verifies whether the ID valid i.e., it checks whether the Id is unique. If it is unique then the packet is sent to

next hop from there the packet is sent to the destination. If the ID is not unique then the attack is detected and the packet will be dropped.

IV. Implementation

4.1 Creating Mobile Nodes

Creating of nodes begins with setting of simulation-parameter values that will be used during configuration of mobile nodes. The OTcl commands for setup of the mobile node parameters are shown below:

Table 1: Part of the Tcl Script for Setting Mobile Node Parameter

Part of the Tcl script for setting of parameters		Explanations
set val(chan)	Channel/Wireless Channel	;# channel type
set val(prop)	Propagation/TwoRayGround	;# radio-propagation model
set val(netif)	Phy/WirelessPhy	;# network interface type
set val(mac)	Mac/802_11	;# MAC type
set val(ifq)	Queue/DropTail/PriQueue	;# interface queue type
set val(ll)	LL	;# link layer type
set val(ant)	Antenna/OmniAntenna	;# antenna model
set val(ifqlen)	50	;# max packet in ifq
set val(nn)	50	;# number of mobile nodes
set val(rp)	AOMDV	;# routing protocol

4.2 Node deployment

The nodes can be deployed in dense or in sparse manner. It depends mainly on application. There are various different deployment methods or scenarios such as grid, random and square. Here in this project the nodes are deployed randomly. Node deployment can reduce complexity in wireless networks.

4.3 Key Generation

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Keys for each node are generated using md5 hash generator and md5pure algorithm.

4.3.1Algorithm Used for key generation

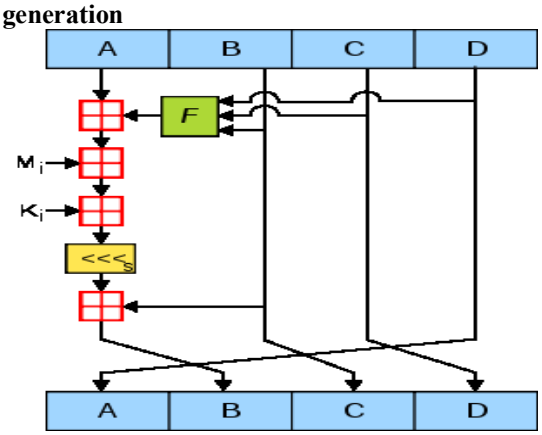

Figure 7: Operation of MD5

The algorithm used here is MD5 (message-digest). It is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. The figure below shows the operation of MD 5 algorithm.

4.4 Mobility

A tool called 'setdest' is developed by CMU (Carnegie Mellon University) for generating random movements of nodes in the wireless network. It defines node movements with specific moving speed toward a random or specified location within a fixed area. When the node arrives to the movement location, it could be set to stop for a period of time. After that, the node keeps on moving towards the next location. The location 'setdest' is at the directory-

'~ns/indep-utils/cmu-scen-gen/setdest/'

4.5 Establish path

The routing protocol is used to establish path between the nodes and the protocol used here is AODV. The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing.

4.5.1 The Basic Protocol

Each AODV router is essentially a state machine that processes incoming requests from the SWANS network entity. When the network entity needs to send a message to another node, it calls upon AODV to determine the next-hop. Whenever an AODV router receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields:

- Destination address
- Next hop address
- Destination sequence number
- Hop count

If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a message queue, and then it initiates a route request to determine a route. The following flow chart illustrates this process:

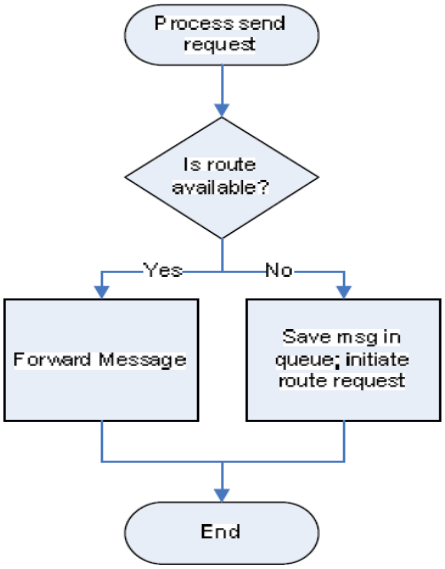

Figure 8: Basic AODV protocol

4.6 Spoofing attack detection

Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets (i.e., spoofing node or victim node). Since under a spoofing attack, the data packets from the victim node and the spoofing attackers are mixed together, this observation suggest to conduct cluster analysis on location id in order to detect the presence of spoofing attackers in wireless network.

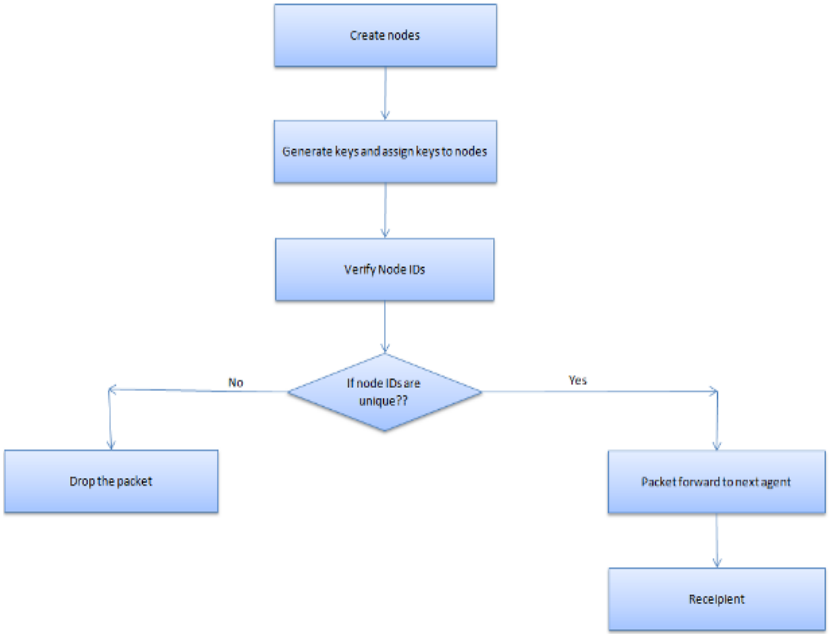

Figure 9: Spoofing attack detection

The Figure 9 shows how the attack is detected. First the nodes are deployed randomly and the path is established, then the cluster head verifies the packet. If the packet is valid i.e.,if the identity of the node is valid then the packet will be sent to next hop and from there it will be sent to destination. If the identity of the node is invalid then the attack is detected and the packet will be dropped. To determine the actual number of attackers found in the network the trace file can be used, that shows the total attackers in the network.

4.7 Localization of attackers

The simulation is performed under Linux environment on NS2. Let us consider the number of nodes deployed in the simulation window for e.g 3000X3000. The nodes are deployed in 2D platform. Each and every position of nodes are defined, thus from the initialized value, the attackers location in the 2D area can be determined accurately.

V. Results

The simulation results from running the script in NS-2 include one or more text based output files and an input to a graphical simulation display tool called Network Animator (NAM). NAM is an animation tool for viewing network simulation traces and real world packet traces. We can either start NAM with the command as follows-

'nam <nam-file>'

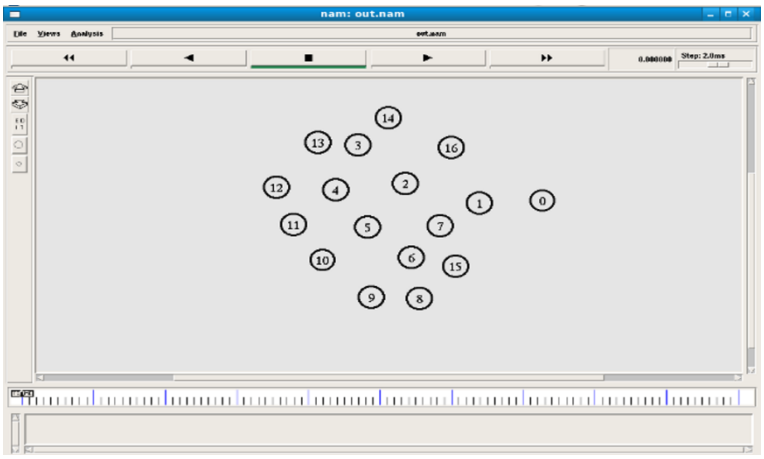

Figure 10: Node Deployment

Here in the above figure 17 nodes are deployed, and they are deployed randomly.

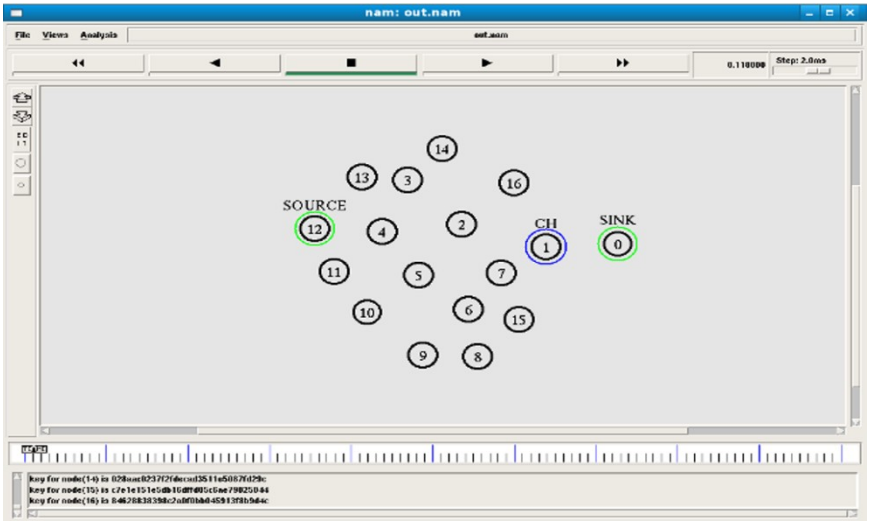

Figure 11: Key Generation

The figure shows node 12 as Source, node 0 as Sink and node 1 as Cluster head. It also displays the keys generated for all nodes at the bottom of the animator

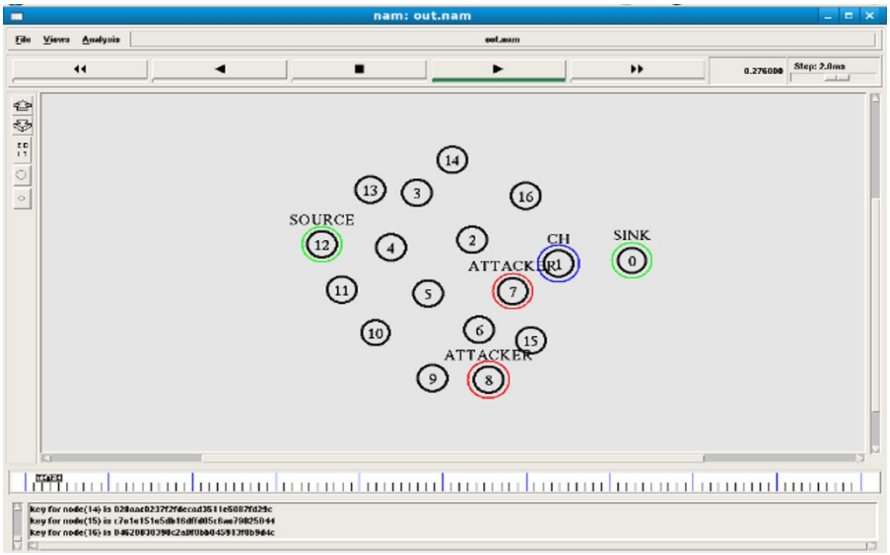

Figure 12: Attack Detection

Here in the above figure Node 8 and Node 7 are the attackers and hence are marked red.

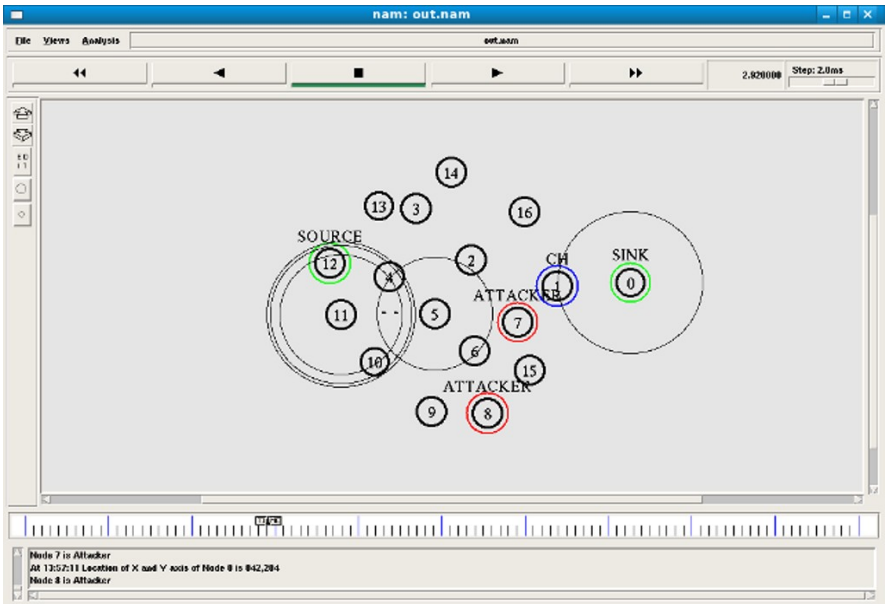

Figure 13: Data Transmission

Here in the above figure the path has been established and the data is been transmitted through that path

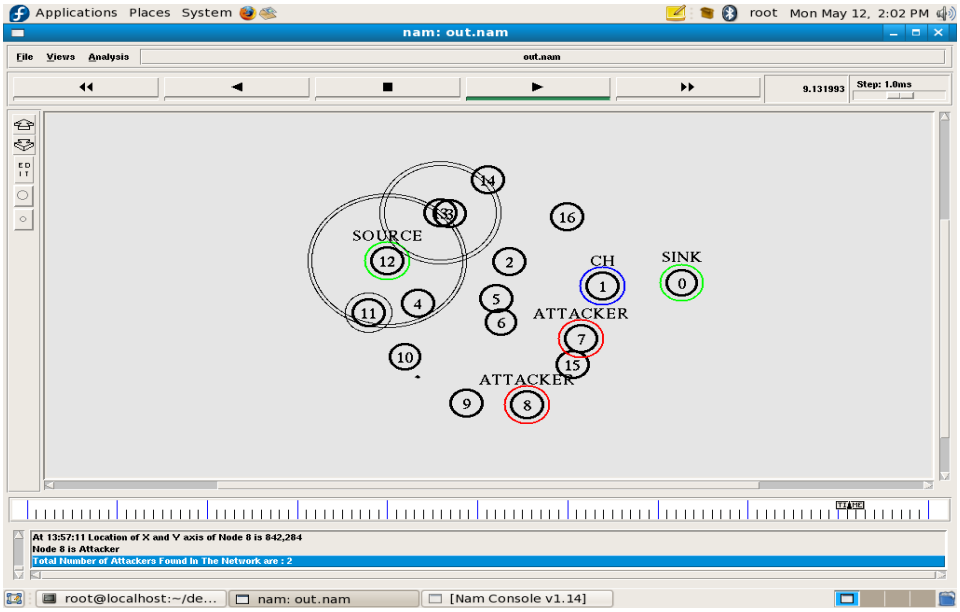

Figure 14: Localization

VI. Performance Analysis

The simulation of the proposed system is done with Network Simulator 2(NS2). The result of the proposed system helps us in analyzing various performance metrics. The performance metrics considered here are throughput and packet delivery ratio.

6.1 Throughput

Throughput is the measure of how fast we can actually send packets through network. The number of packets delivered to the receiver provides the throughput of the network. The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time it takes for receiver to get the last packet.

Table 2: Pause Time Vs Throughput

Pause time	Throughput		
	10% attacks	20% attacks	30% attacks
0	600.356	580.20	551.254
5	786.247	640.54	623.49
10	864.12	796.35	753.65
15	945.36	845.62	803.95
20	1001.621	899.02	921.354
25	921.154	798.36	684.84
30	847.164	710.52	620.87

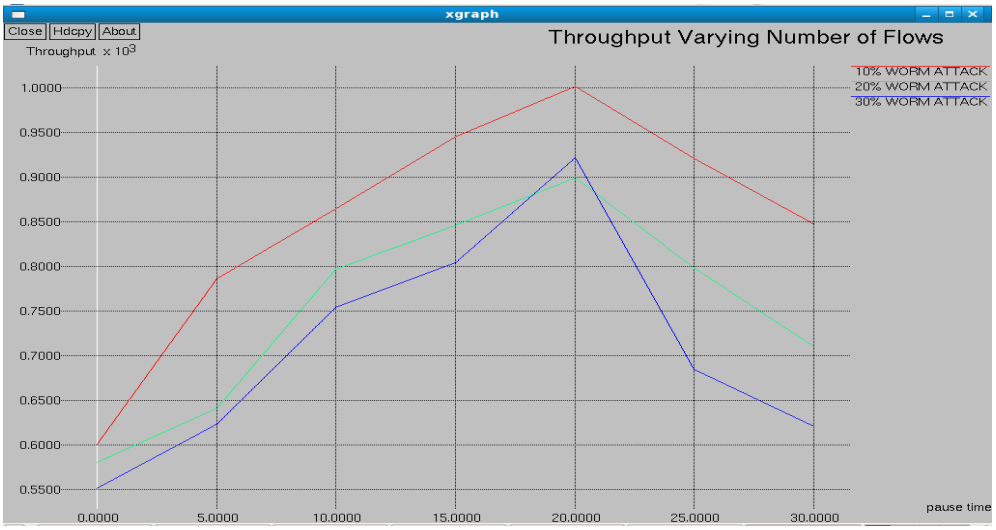

Figure 15: Pause Time Vs Throughput

The above graph defines the throughput for the proposed protocol. The experiment was running 30 seconds. Throughput is the rate at which a network sends and receives data. It is a good channel capacity of net connections and rated in terms bits per second (bit/s).When the attack percentage is low, the throughput is high.

6.2 Packet Delivery Ratio

The ratio of the data packets delivered to the destinations to those generated by the CBR sources. It is the fraction of packets sent by the application that are received by the receivers.

Table 3: Pause Time Vs Packet delivery Ratio

Pause time(no of nodes)	Delay		
	10% attacks	20% attacks	30% attacks
0	0.90	0.86	0.82
1	0.98	0.90	0.80
2	0.98	0.99	0.75
3	1.00	1.00	0.77
4	0.98	0.98	0.84
5	1.00	0.96	0.87
6	0.99	0.98	0.90
7	0.91	0.99	0.96
8	0.99	0.98	1.00

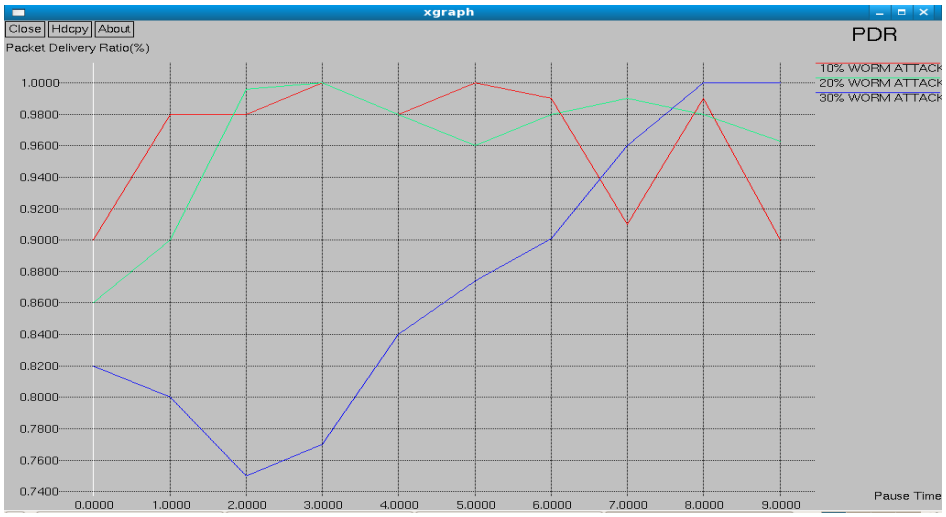

Figure 16: Pause Time Vs Packet delivery Ratio

VII. Conclusion

The proposed approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that it can localize any number of attackers. Determining the number of adversaries is challenging, the proposed identifies them using the trace file. Further, based on the number of attackers determined by the mechanisms, our proposed system can localize any number of adversaries. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

References

[1]. Bellardo.J and Savage.S, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.
[2]. Bohge.M and Trappe.W, "An authentication framework for hierarchical ad hoc sensor networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003, pp. 79–87.
[3]. Bernaschi.M, Ferreri.F, and Valcamonici.L, "Access points vulnerabilities to dos attacks in 802.11 networks," in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.
[4]. Fernandez.E, and Magliveras.S, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.
[5]. Wool. A, "Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677–686, 2005.
[6]. Cheriton.D and Faria.D, "Detecting identity-based attacks in wireless networks using signal prints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.
[7]. Li.Q and Trappe.W, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.
[8]. Chen.Y, Martin.R.P and Trappe.W, "Detecting and localizing wireless spoofing attacks," in Proc. IEEE SECON, May 2007.
[9]. Chen.Y, Trappe.W and Yang.J, "Detecting spoofing attacks in mobile wireless environments," in Proc. IEEE SECON, 2009.