International Journal of Wireless Communications and Mobile Computing
2013; 1(4): 82-90
Published online September 30, 2013 (http://www.sciencepublishinggroup.com/j/wcmc)
doi: 10.11648/j.wcmc.20130104.11

Identifying and locating multiple spoofing attackers using clustering in wireless network

AMALA GRACY[1], CHINNAPPAN JAYAKUMAR[2]

[1]Department of Information Technology, RMK Engineering College, Anna University, Chennai, INDIA
[2]Department of Computer Science and Engineering, RMK Engineering College, Anna University, Chennai, INDIA

Email address:
sag.cse@rmkec.ac.in(A. GRACY), cjk.cse@rmkec.ac.in(C. JAYAKUMAR)

To cite this article:
AMALA GRACY, CHINNAPPAN JAYAKUMAR. Identifying and Locating Multiple Spoofing Attackers Using Clustering in Wireless Network. *International Journal of Wireless Communications and Mobile Computing.* Vol. 1, No. 4, 2013, pp. 82-90.
doi: 10.11648/j.wcmc.20130104.11

Abstract: Wireless networks are vulnerable to identity-based attacks, including spoofing attacks, significantly impact the performance of networks. Conventionally, ensuring the identity of the communicator and detecting an adversarial presence is performed via cryptographic authentication. Unfortunately, full-scale authentication is not always desirable as it requires key management, coupled with additional infrastructural overhead and more extensive computations. The proposed non cryptographic mechanism which are complementary to authenticate and can detect device spoofing with little or no dependency on cryptographic keys. This generalized Spoofing attack-detection model utilizes MD5 (Message Digest 5) algorithm to generate unique identifier for each wireless nodes and a physical property associated with each node, as the basis for (1) detecting spoofing attacks; (2) finding the number of attackers when multiple adversaries masquerading as a same node identity; and localizing multiple adversaries. Cluster-based mechanisms are developed to determine the number of attackers. The proposed model can be explored further to improve the accuracy of determining the number of attackers, by using Support Vector Machines (SVM).

Keywords: Wireless Network, Spoofing Attack, Identity-Based Attack, Message Digest 5, Support Vector Machines, Partitioning Around Medoids (PAM) Cluster Model

1 Introduction

Wireless networks are more prone towards spoofing attacks. In identity-based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks by masquerading as an authorized wireless access point (AP) or an authorized client [1]. An attacker can launch denial-of-service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients. Therefore, identity-based attacks will have a serious impact to the normal operation of wireless and sensor networks. Spoofing attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, rogue AP attacks, and eventually DoS[2].

Spoofing can take on many forms in the computer world, all of which involve some type fraudulent representation of information

1.1. IP Spoofing

Internet Protocol (IP) is the protocol used for transmitting messages over the Internet [3]; it is a network protocol operating at layer 3 of the Open Systems Interconnection (OSI) model. IP spoofing is the act of manipulated the headers in a transmitted message

to mask a hackers true identity so that the message could appear as though it is from a trusted source. IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system.

1.2. ARP Spoofing

Address Resolution Protocol (ARP) is used to map IP addresses to hardware addresses [4]. A table named as ARP cache, is used to maintain a correlation between each Medium Access Control (MAC) address and its corresponding IP address. “ARP Spoofing involves constructing forged ARP request and reply packets. By

sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B". This referred to as ARP poisoning.

1.3. E-Mail Spoofing

In E-Mail spoofing, an email message contains malicious objects, and appears to come from a legitimate source. But in fact, it is from an Attacker. E-mail spoofing can be used for malicious purposes such as spreading viruses / trawling for sensitive business data / other industrial espionage activities.

Normal E-mail message contains the return address at the Top left corner of the mail. This indicates where the mail is generated. But the attackers could over write any name and address in this space, which pretends to be genuine.

1.4. WEB Spoofing

Web or Hyperlink spoofing provides victims with false information. Web Spoofing is an attack that allows someone to view and modify all web pages sent to a victim's machine. They can observe any information that is entered into forms by the victim. This can be of particular danger due to the nature of information entered into forms, such as addresses, credit card numbers, bank account numbers, and the passwords that access these accounts.

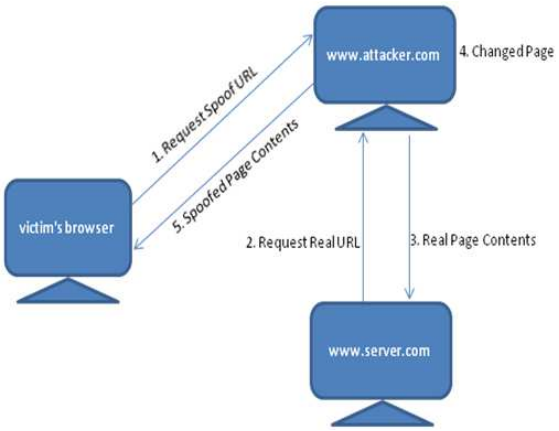

Fig.1. *Working of WEB Spoofing*

1.5. DNS Spoofing

A DNS spoofing attack can be defined as the successful insertion of incorrect resolution information by a host that has no authority to provide that information. It may be conducted using a number of techniques ranging from social engineering through to exploitation of vulnerabilities within the DNS server software itself. Using these techniques, an attacker may insert IP address information that will redirect a customer from a legitimate website or mail server to one under the attacker's control – thereby capturing customer information through common man-in-the-middle mechanisms.

The attacker targets the DNS service used by the customer and adds/alters the entry for www.mybank.com – changing the stored IP address from 150.10.1.21 to the attacker's fake site IP address (200.1.1.10).

The customer queries the DNS server.

The DNS responds to the customer query with "The IP address of www.bank.com is 200.1.1.10" – not the real IP address.

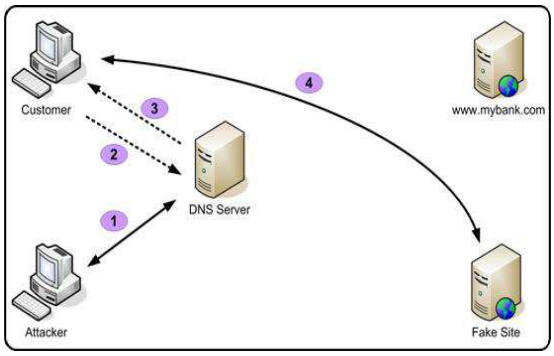

Fig.2. *Working of DNS Spoofing*

However, authentication requires additional infrastructural overhead and computational power associated with distributing and maintaining cryptographic keys.

A different approach is proposed, where in the physical property associated with each wireless node is used to assess the presence of adversaries in the wireless network. This method is hard to falsify, and not reliant on cryptography as the basis for detecting spoofing attacks. This approach enables to detect and localize multiple adversaries in the network, with high detection rate and minimal infrastructure. In a large-scale wireless network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks. Therefore, the problem can be divided into 2 folds such as

- Detect the presence of spoofing attacks,
- Determine the number of attackers, and localize multiple adversaries.

The identification and localization can be done in the following ways:

Generalized Attack Detection Model

This can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods.

Localization of Attackers

Identify the positions of multiple adversaries even when the adversaries vary their transmission power levels.

The main contribution of the paper is organized are as follows:

- To effectively detect the presence of spoofing attack
- To count the number of attackers
- To identify the location of multiple adversaries in the network
- To provide solution to identify adversaries in the

network where in there is no additional cost or modification to the wireless devices themselves
- To avoid authentication key management
- To avoid overhead
- To develop a mechanism where in there is low false positive rate

This paper is organized as follows: section 2 deals with literature of related works in various spoofing attacks prevailing in Wireless network. Section 3 explains about proposed system architecture and how the adversaries are identified in the proposed mechanism. Section 4 presents the simulation and performance evaluation. Section 5 concludes the proposed system.

2. Related Works

Intrusion detection mechanisms are readily available to prevent the wireless network from exploiting vulnerabilities at IP layer or above than IP layer. Whereas, attacks that are exploiting vulnerabilities at link layer demands different set of intrusion detection mechanisms. Following works are relevant to this paper, and their summary is as follows:

Each node in a wireless network can be identified by its location information, which is hard to falsify and not reliant on cryptography. Cluster base mechanism uses this location information, to detect spoofing attacks in wireless networks. This method is capable of both detect and provide the number of adversaries in the wireless network, and spoofing the same node identity. There were experiments conducted on 2 test beds through 802.11 networks (Wi-Fi) and an 802.15.4 (ZigBee) network in two real office building environments. This method having a detection rate of above 98% and determining the number of adversaries with the hit rate of over 90%.

Sequence number-based MAC Address Spoof detection algorithm is employed to detect adversaries in the Wireless network[5]. Presence of MAC Address spoofing can be detected in real-time WLAN environments. This algorithm best work, when the casual attackers do not take advantage of false negative of the algorithm. If they exploit, then the algorithm can detect the presence of MAC spoofing, whereas, it does not detect the spoofed frames. By means of K-means cluster analysis, both detection of spoofing attacks and locating positions of adversaries in the network either Area based (and) point based localization algorithms [6]. This method can detect the presence of adversaries with high detection rate as well as low false positive rate. DEMOTE system uses Received Signal Strength (RSS) traces collected over time. Then it achieves an optimal threshold to partition the RSS traces into classes for attack detection. Temporal constraints used in this Algorithm Alignment Prediction method, to predict the best RSS alignment of partitioned RSS classes for RSS trace for reconstruction over time [7].

Supporting Quality of Service (QoS) in ad hoc is a challenging task. A lot of researches have been done on supporting QoS in the ad hoc but most of them are not suitable .Clustering technique provides a solution to support QoS in ad hoc networks [8]. The clusters must be long-lived and stable based on the effective functioning of cluster based routing algorithms. Difficult to furnish QoS without knowing any state information. The proposed method includes the spatial and temporal stability of the nodes. The first select a node as cluster head. The node elected as the cluster head is such that it has maximum associativity as well as satisfies a minimum connectivity requirement. The cluster head collects and aggregates information in its own cluster and passes information. By rotating the cluster-head randomly, energy consumption is expected to be uniformly distributed. Effective work has been done for Cluster Reorganization. Cluster Head Re-election is periodically done so that the cluster head is centered in a cluster. many clustering proposals for increasing network lifetime are reported suggesting different strategies of cluster head selection and its role rotation in the ad hoc networks, using different parameters .Cluster management will be effective, since the cluster heads are elected based on various parameters like processing capabilities, speed of the node, number of neighbour nodes and associativity with the neighbour nodes. Though overhead is incurred initially due to cluster setup, cluster maintenance will be easier in the long run. Ultimately routing efficiency will increase due to long-lived clusters and reduced control packets.

Mobile ad hoc network (MANETs) becomes a popular research topic due to their self-configuration and self-maintenance capabilities. Security is a major concern for providing trusted communications in a potentially hostile environment. Multimodal biometric technology provides potential solutions for continuous authentication in high security mobile ad hoc networks [9]. Continuous user authentication is an important prevention-based approach to protect high security mobile ad hoc networks (MANETs).Intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities. A MANET is an infra structure less network for mobile devices connected by wireless link. The mobile network is often vulnerable to security attacks even though there are many traditional approaches, due to its features of open medium and dynamic changing topology.Multi-modal biometrics is deployed to work with intrusion detection systems (IDSs) to overcome the shortcomings of uni-modal biometric systems. Multimodal biometrics can be used to alleviate some drawbacks of one mode of biometrics by providing multiple verifications of the same identity.The cluster head is elected in which Dempster-Shafer theory is evaluated in order to increase the observation accuracy to maintain high security and trusted MANET. The Dumpster–Shafer evidence theory was originated by Dempster and later revised by Shafer. It's essential idea is that an observer can obtain degrees of trust about a proposition from related proposition's subjective probabilities. Since each device in the network has measurement and estimated limitations, more than one

device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster–Shafer theory for data fusion.

Due to shared nature of medium in wireless networks, it is simple for an adversary to launch a Wireless Denial of Service (WDoS) attack [10]. These attacks can be easily launched by using off-the-shelf equipment. For illustration, a malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers. Jamming techniques vary from simple ones based on the continual transmission of interference signals, to more sophisticated attacks that aim at exploiting vulnerabilities of the particular protocol used. Various techniques were proposed to detect the presence of jammers. Finally, numerous mechanisms which attempt to protect the network from jamming attacks were discussed.

TCP SYN flooding and IP address spoofing attacks were launched on Multi-hop wireless networks. TCP SYN flooding occurs when establishing a TCP connection for data transmission. But, even after a TCP connection is established, TCP protocol is flooded by a novel connection flooding attack which aims at consuming the entire bandwidth allocated to a network. Even though numerous techniques are available to counter this attack, there is no single technique, which effectively protects the network from TCP SYN Flooding attack. It proposes a defense mechanism which involves in defending such flooding attack and also prevents IP spoofing, which is the gateway for such flooding attacks. The performance analysis is carried out and it proves the effectiveness of the proposed defense mechanism in terms of time delay and false positive rates. Exponential back-off restoration algorithm was used to counter Denial-Of-Service attack, which is considered to be one of main threats to wireless multi-hop networks [11]. This algorithm overcomes weakness of traffic burst based detection methods. The proposed method can detect anomaly and restore the network scheme to defeat low-rate DoS launched by rogue nodes. Exponential backoff restoration (EBR) algorithm is proposed to reduce performance degradation.

Trust issue in wireless sensor networks is predominant, in security schemes [12]. It is necessary to analyze how to resist attacks with a trust scheme. It categorizes various types of attacks and countermeasures related to trust schemes in WSNs. Furthermore, it provides the development of trust mechanisms, give a short summarization of classical trust methodologies and emphasize the challenges of trust scheme in WSNs. An extensive literature survey is presented by summarizing state-of-the-art trust mechanisms in two categories: secure routing and secure data. Based on the analysis of attacks and the existing research, an open field and future direction with trust mechanisms in WSNs is provided

Wireless Sensor Networks (WSNs) pose host of security issues in the area of development and secure routing protocols [13]. Improving network hardware and software may address many of the issues, but others will require new supporting technologies. With the proliferation of usage of Wireless Sensor Networks, the security mechanisms play an important role. Recently proposed solutions address but a small subset of current sensor network attacks. Also because of the special battery requirements for such networks, normal cryptographic network solutions are irrelevant. New mechanisms need to be developed to address this type of network.

Due to vulnerability of Wireless networks, towards spoofing attacks, host of other forms of attacks can be launched on the networks [14]. A spoofing attack is the most common online attack in which an adversary or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. It demands for more sophisticated defense mechanisms. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it requires key management and additional infrastructural overhead. Various defense mechanisms were discussed.

This work differs from the previous study mentioned earlier, by using MD5 and physical property associated with each node, to identify the presence of adversaries in the wireless network, and using SVM to identify number of such adversaries in this Network. Finally, by using NS2, to simulate and verified the results.

3. Proposed System Architecture

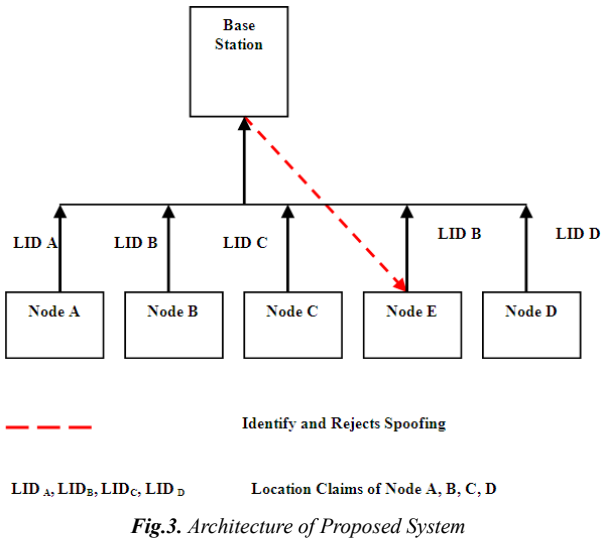

Fig.3. *Architecture of Proposed System*

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate access into Wireless network. Fig.3 considers a wireless network with N nodes. Let N denote the set of all nodes in the network. Nodes are deployed in 2D platform. Each node is associated with unique location identifier using MD5. If any one of the node needs to communicate with the base

station, it will check the location ID of respective node. If the base station finds that any two nodes has the same location ID (ie. Node B), then it meant that spoofing has taken place. A base station is a radio receiver / transmitter that serves as the hub of the local wireless network, and may also be the gateway between a wired network and the wireless network. It typically consists of a low-power transmitter and wireless router.

3.1. Message Digest 5

Fig.4 MD5(Message Digest 5) algorithm uses message of arbitrary length, as input and produces an output of 128-bit "fingerprint" or "message digest" of that input. This algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner. MD5, with its 128bit encryption algorithm has 1,280,000,000,000,000,000 possible combinations. It mainly used for Verifies data integrity and particularly in Internet-standard message authentication.

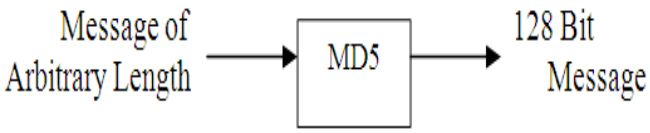

Figure.4. *Working of Message Digest 5*

3.2. Node Deployment

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

3.3. System Module

Detection and Localization of Spoofing attackers are identified from the following modules.

- Detection of Spoofing Attack
- Find the Number of Attackers
- Localization of Attackers

3.3.1. Detection of Spoofing Attacks

Spoofing attack detection is performed using Cluster Analysis. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. Fig.5 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 suggests to conduct cluster analysis on location id in order to detect the presence of spoofing attackers in wireless network.

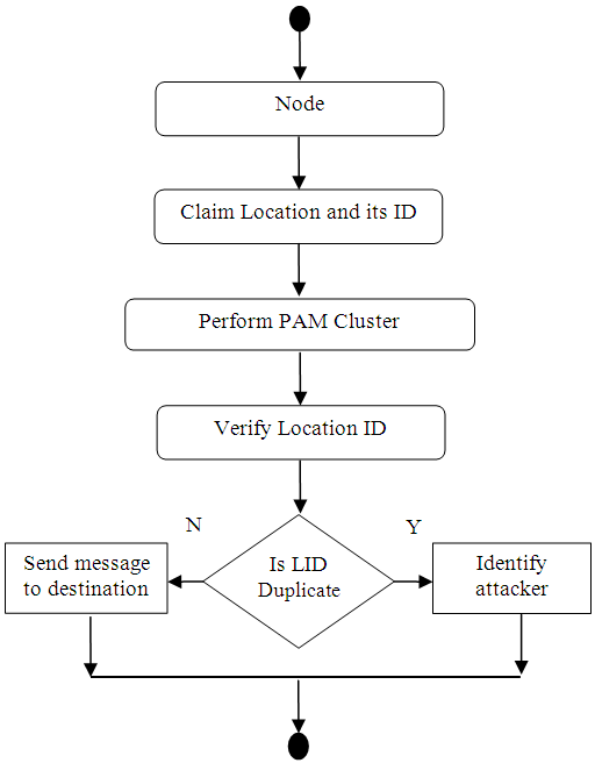

Fig.5. *Activity diagram of proposed system*

3.3.1.1. GADE

A Generalized Attack Detection modEl that can both detect spoofing attacks as well as determine the number of adversaries using Cluster analysis. In GADE, the Partitioning Around Medoids (PAM) cluster analysis method is used to perform attack detection and then applied cluster-based methods to determine the number of attacker.

3.3.1.2. PAM

The PAM Method is a popular iterative descent clustering algorithm. Compared to the popular K-means method, the PAM method is more robust in the presence of noise and outliers. Spoofing attack detection is performed using Cluster Analysis. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. consider the wireless nodes are composed of several clusters of Ordinary Nodes.

The PAM algorithm partitioned a dataset of ‘n’ objects into a number of clusters (‘k’), where both the dataset and the number k is an input of the algorithm. This algorithm works with a matrix of dissimilarity, where its goal is to minimize the overall dissimilarity between the represents of each cluster and its members.

The PAM algorithm can work over two kind of input, the first is the matrix representing every entity and the values of its variables, and the second is to work with the dissimilarity matrix directly. This algorithm has following two phase.

Build Phase

- Choose k entities to become the Medoids, or in case

these entities were provided use them as the Medoids
- Calculate the dissimilarity matrix if it was not informed, and
- Assign every entity to its closest Medoids.

Swap Phase
- For each cluster search if any of the entities in the cluster having value lower than the average dissimilarity coefficient, if it does select the entity that lower the most this coefficient as the medoids for this cluster;
- If at least the medoids from one cluster has changed go to (3), else end the algorithm.

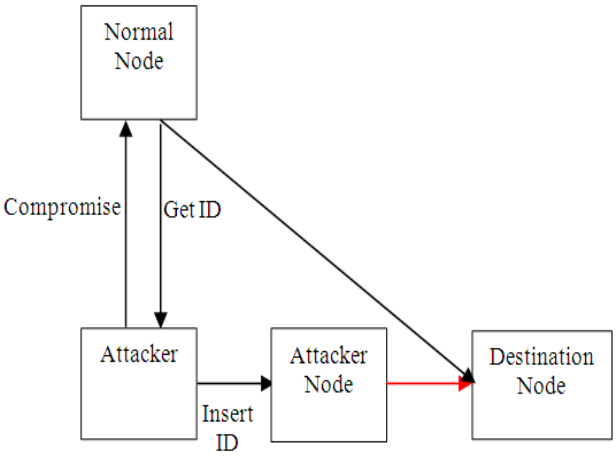

Fig.6. *Spoofing Attack Detection*

Fig.6 shows, how Spoofing attacks are detected by same location id. Attacker gets the ID of normal node and makes use of the same to send packets to Destination node.

3.3.2. Determine the Number of Attackers

SVM used to improve the accuracy of determining the number of spoofing attackers in the network. SVM is widely used in object detection & recognition. It has two types that are Linear SVM and Nonlinear SVM. SVM is used to classify the number of the spoofing attackers.

The advantage of using SVM is that it can combine the intermediate results (i.e. features) from different statistic methods to build a model based on training data acquired from cluster, to accurately predict the number of attackers. On detecting a attacker in the wireless network, SVM increment the target Value by '1', else '0'. SVM can be applied to solve classification and regression problems. Some of SVM applications are Handwriting Recognition, 3D Object Recognition, Speaker Identification, Face Detection, Text Categorization, Bio-Informatics, and Image Classification.

Fig.7 shows on detecting multiple adversaries present in a Wireless network. In Multi Spoofing attack, ID of a compromised Node is used by multiple adversaries present in the network, to send packet to Destination Node.

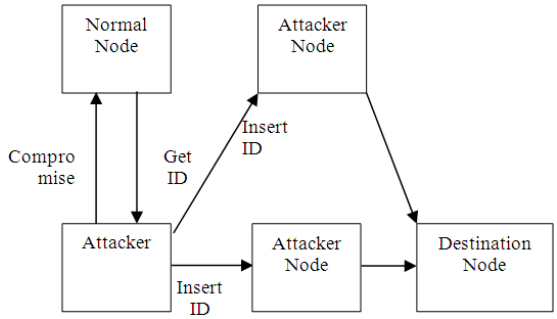

Fig.7. *Detection of Multi Spoofing Attack*

3.3.3. 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. The proposed method can be extended to networks like 802.11(WiFi), 802.15.4(ZigBee) to localize the attackers, in real life environment.

4. Performance Evaluations

The simulation of the proposed system is done with Network Simulator 2(NS2). The results of the proposed system helps in analyzing various performance metrics such as False positive rate, detection rate, delay metric, energy level and hit rate. This graph provides an analysis for finding the overall performance of the system.

4.1. Setting Environment

The proposed system has executed under the NS2 environment, where in Tcl language is used to simulate. This environment is having parameters as follows:

Application	: VMware
Operating System	: Linux - Red Hat
X Axis	: 1400
Y Axis	: 1400
Channel Type	: Wireless Channel
MAC Type	: 802_11
Routing Protocol	: AODV

4.2. Simulation Evaluation

Fig.8 compares existing and proposed method of detecting the attackers in the wireless environment.

On analyzing the relationship between false positive rate with detection rate, it is found that Detection Rate becomes Constant after a certain False positive rate. The Threshold detection rate decreases when the distance between two centroids in signal space increase. Threshold detection rate is inversely proportional to dB. If the Distance becomes more, then False Positive Rate will increase.

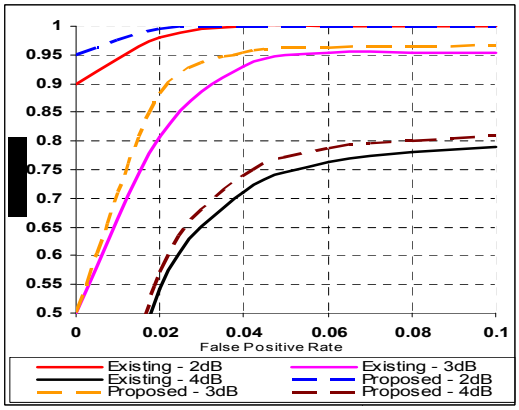

Fig.8. *False Positive Rate Vs Detection Rate*

4.2.1. Detection Rate Vs Time

Fig.9 shows about how detection rate is changing with respect to time. It is inferred that, high detection rate can be achieved after a considerable time.

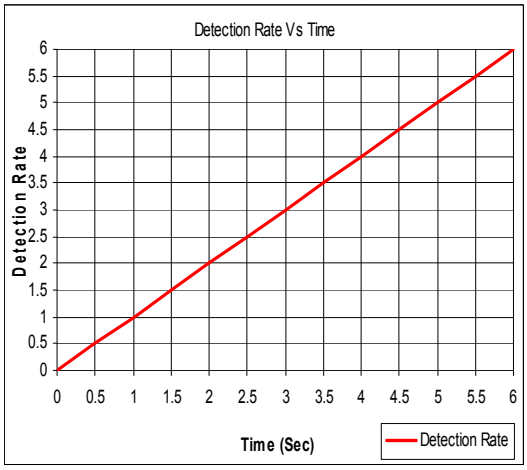

Fig.9. *Detection Rate Vs Time*

4.3. Performance Evaluation

4.3.1. Delay Vs Time

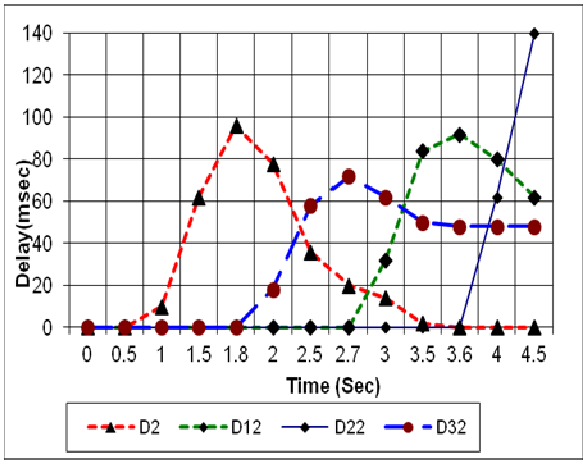

Fig.10. *Delay Vs Time*

Fig.10 shows the graphical representation of the delay metric, where x axis represents time and y axis represents delay. In this study, 4 nodes where chosen randomly, and measured the delay against time in seconds. The graph shows decrease in delay due to the network bandwidth and connectivity of the nodes. This mainly helps to prolong the connectivity of network and increase the performance.

4.3.2. Energy Vs Number of Attackers

Various Energy levels are measured against the number of attackers in the wireless environment, and the same represented as below. In this figure, Number of attackers are considered in X axis and energy levels in Joule is considered in Y axis.

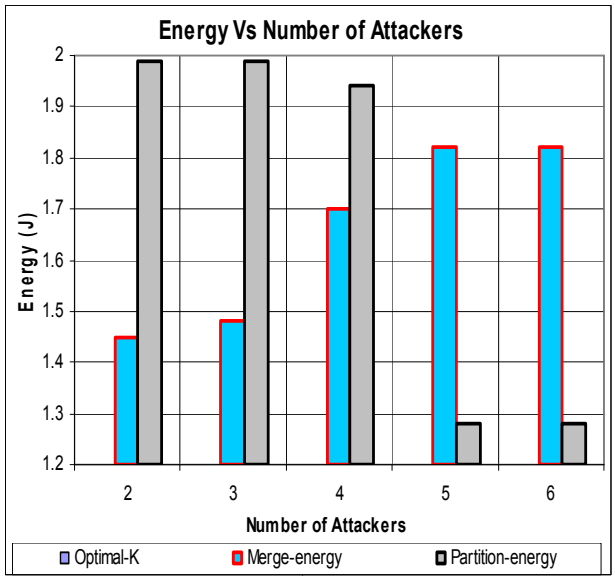

Fig.11. *Number of Attackers and Energy level*

From the fig.11, it is inferred that, Merge Energy level will increase as the number of attackers, increases. On the contrary, Partition energy level is decreased as the number of attackers increase. As a result, it is evident that, Merge energy and partition energy levels are inversely proportional to each other. Once the number of attackers in the environment is crossing 4, partition energy level drops drastically, and similarly there is a significant increase in the Merge energy level.

4.3.3. Hit Rate Vs Number of Attackers

A comparative study is conducted between the Existing and proposed method on the basis of hit rate. In X axis Number of attackers are considered and in Y axis hit rate is considered to plot this graph.

From the study, it is found that proposed method is having higher hit rate than existing method. But in both of methods, hit rate is decreased as the number of attackers increases. Proposed method is more efficient in identifying the attackers than that of existing method.

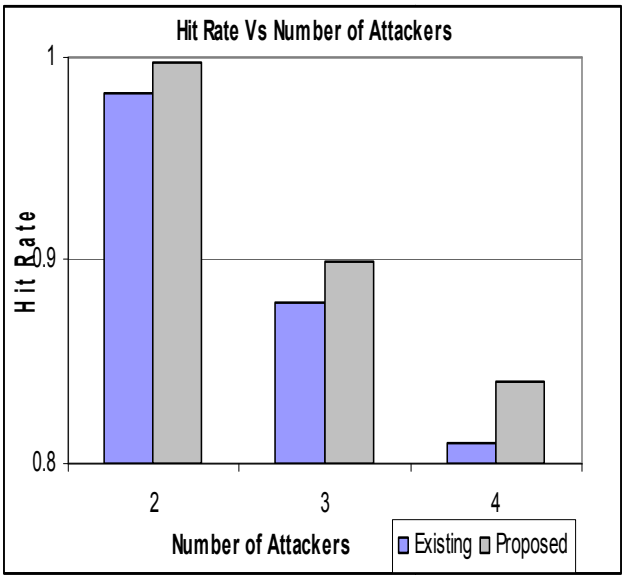

Fig.12. *Hit Rate Vs Number of Attackers*

4.3.4. Time Vs Number of Attackers

SVM method adopts supervised machine learning algorithm, wherein it training data plays a vital role. We have used the training data to explain the relation between Time and Number of attackers present in the system.

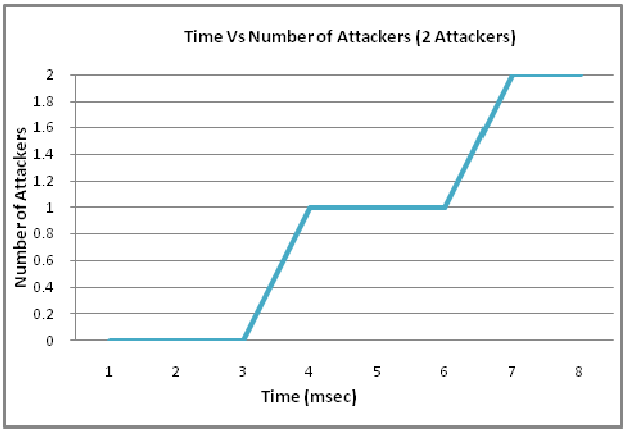

Fig.13. *Time Vs Number of Attackers (2 Attackers)*

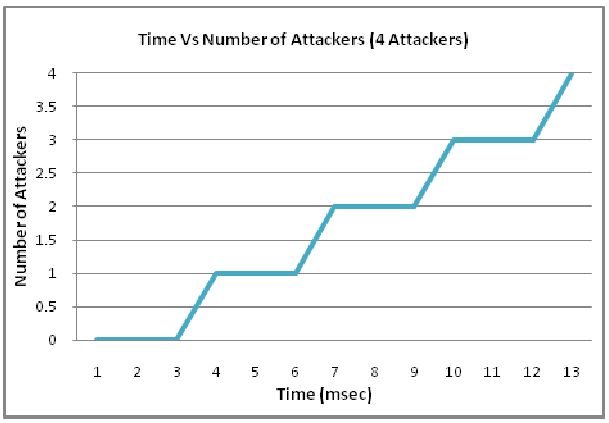

Fig.14. *Time Vs Number of Attackers (4 Attackers)*

5. Conclusion

Wireless networks are used in numerous applications. Due to its proliferation of usage, there exist threats in terms of spoofing attacks. In the proposed approach detection of the presence of attacks as well as determine the number of adversaries as same node identity. It can localize any number of attackers and eliminate them. Determine the number of adversaries in particular, is a challenging task. This mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution, that use cluster analysis alone.

Further, based on the number of attackers determined by the mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. 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. The proposed methods can achieve over 99 percent Hit Rate and Precision when determining the number of attackers

In future, based on the outcome of this model, explore further to find ways to eliminate those identified multiple adversaries, from the wireless network. Thus way, wireless networks will be more robust and less prone to attack.

References

[1] Jie Yang, Yingying Chen, Wade Trappe and Jerry Cheng, "Determining the Number of Attackers and Localizing Multiple Adversaries in Wireless Spoofing Attacks", *Proceedings of 28th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2009, pp. 666–674.

[2] Wei Che, "Defending against TCP SYN Flooding Attacks under Different Types of IP Spoofing", *Proceedings of International Conference on Mobile Communication*, 2006, pp.38.

[3] Diana Jeba Jingle, Elijah Blessing Rajsingh, "Defending IP Spoofing Attack and TCP SYN Flooding Attack in Next Generation Multi-hop Wireless Networks", *International Journal of Information & Network Security,* Volume 2, No.2, 2013, pp.160-166.

[4] P.Ramesh Babu, S.D.Lalitha Bhaskari, CH. Satyanarayana, "A comprehensive Analysis of spoofing", *International Journal of Advanced Computer Science and Application* Volume 1, No.6, 2010.

[5] Fanglu Guo and Tzi-cker Chiueh, "Sequence Number-Based MAC Address Spoof Detection", *Proceedings of 8th International Symposium on Recent Advances in Intrusion Detection*, 2005, pp.309-329.

[6] Yingying Chen, Wade Trappe and Richard P. Martin, "Detecting and Localizing Wireless Spoofing Attacks",

Proceedings of 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007, pp.193-202.

[7] Jie Yang, Yingying Chen, Wade Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments", *Proceedings of 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2009, pp.107-189.

[8] Jayakumar C and Chellappan C, "Quality of Service in Associativity based Mobility-Adaptive K-Clustering in Mobile Ad-hoc Networks", *International Journal of The Computer, the Internet and Management,* Vol.14, No.1, 2006, pp.61-80.

[9] P. Infant Kingsly, C. Jayakumar, Mahendran Sadhasivam, S. Deepan Chakravarthy, "Smart Way for Secured Communication in Mobile Ad-hoc Networks", *International Journal Computational Intelligence and Informatics*, Vol.2 No. 1, 2012, pp.1-9.

[10] Pelechrinis, K., Krishnamurthy, S.V., "Denial of Service Attacks in Wireless Networks: The Case of Jammers", *IEEE Journal of Communications Surveys & Tutorials,* Volume 13, Issue: 2, 2011, pp.245-257.

[11] Qiang Liu, "Enhanced detection and restoration of low-rate denial-of-service in wireless multi-hop networks", *Proceedings of International Conference on Computing, Networking and Communications (ICNC)*, 2013, pp. 195-199.

[12] Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", *Journal of Network and Computer Applications*, Volume 35, Issue: 3, 2012, pp.867–880.

[13] Koffka Khan, Wayne Goodridge & Diana Ragbir, "Security in Wireless Sensor Networks", *Global Journal of Computer Science and Technology Network, Web & Security*, Volume 12, Issue: 16, Version 1.0, 2012.

[14] Divya Pal Singh, Pankaj Sharma and Ashish Kumar, "Detection of Spoofing attacks in Wireless network and their Remedies", *International Journal of Research Review in Engineering Science and Technology*, Volume 1, 2012, pp.1-5.

[15] Jayakumar C and Chellappan C, "A QoS aware energy efficient routing protocol for wireless ad-hoc networks", *Asian Journal of Information Technology*, Vol.4, No.6, 2005, pp.578-582.

[16] Karmel A and C. Jayakumar, "Analysis of MANET Routing Protocols Based on Traffic Type", *IJREAT International Journal of Research in Engineering & Advanced Technology*, Vol.1, Issue 1, 2013, pp.1-4.

[17] K. Tan, Guanling Chen, D. Kotz, A Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength", *Proceedings of 27th Conference on Computer Communications*, 2008, pp.1768-1776.

[18] Iyad Aldasouqi and Walid Salameh, "Detecting and Localizing Wireless Network Attacks Techniques", *International Journal of Computer Science and Security*, Volume 4, No.1, 2010, pp.82-97.

[19] Daniel B. Faria and David R. Cheriton, "Detecting identity-based attacks in wireless networks using Signal prints", *Proceedings of 5th ACM Workshop on Wireless Security*, 2006, pp.43-52.

[20] Jie Yang, Yingying Chen, Wade Trappe and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", *IEEE Transaction on Parallel and Distributed System*, Volume 24, No.6, 2012, pp.44-58.

[21] A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless LANS with key refresh and host revocation", *Journal of ACM/Springer Wireless Networks*, Volume 11, 2005, pp.677–686.

[22] Jayakumar C and Chellappan C, "Optimized on demand routing protocol of mobile adhoc network", *Informatica*, Vol.17, No. 4, 2006, pp.481-502.

[23] M. Vijay Anand and C. Jayakumar, "Secure Routing in Manet Using Artificial Immune System Based on Danger Theory", *International Journal of Emerging Research in Management &Technology*, Vol.2, No.4, 2013, pp.73-77.