International Journal of Security and Its Applications
Vol. 11, No. 5 (2017), pp.39-48
http://dx.doi.org/10.14257/ijsia.2017.11.5.04

A Survey on Impersonation Attack in Wireless Networks

R. Regan[1] and J. Martin Leo Manickam[2]

[1]*Department of CSE, University College of Engineering, Villupuram, Anna University, India*
[2]*Department of ECE, St. Joseph's College of Engineering, Chennai, India*
[1]*reganr1985@gmail.com*, [2]*josephmartin_74@yahoo.co.in*

Abstract

Commucation being a mode of sending and receiving understanding is gaining extra popularity in today's world. Today wireless systems are increasingly getting used for primary conversation and undertaking to hold electronic knowledge transmissions comfortable. Almost always, it's problematic to implement mighty security in small-footprint devices having low processing power, low memory capacity and utilising unreliable, low bandwidth. Impersonation attack may be very common in these days in wireless network, but the principal hindrance is the security. There is lots of solution provided by different researcher but still faces research challenge. Impersonation attacks are also known as spoofing attacks. The attacker assumes the identification of one more node in the network, as a result receiving messages directed to the node it fakes. As a rule this would be some of the first steps to intervene a network with the intention of accomplishing further assaults to disrupt operation. In this paper we describe the causes of Wireless impersonation attack, their vulnerable effects and various defense mechanisms for defending this attack.

Keywords*: Wireless network, impersonation attack, Defenses mechanisms*

1. Introduction

Wireless technologies have advanced with extraordinary speed in the previous couple of years. Not just have the capacity and performance of wireless communications systems enhanced exponentially, however so has the range of information and services that can now be accessed using mobile devices. Mobile phones and other handheld devices for example palm pilots permit incredibly increasing amounts of information to be retrieved, stored and transmitted in real time. This incorporates text, audio and video data, as delineated by the simplicity with which mobile phone users are today able to converse by voice, email, SMS, take and transmit digital photographs, stream audio and video files, and upload or download a range of material specifically by means of the internet [10]. The primary advantage of Wireless system is communicating with rest of the world while being mobile. The weakness of this is their limited bandwidth, processing capabilities, memory, open medium and less secure compared to wired devices. As wireless systems are progressively being utilized for communication it is becoming a challenge to keep electronic data transmissions secure[6].

On top of everything, security needs for wireless devices are greater than those of regular wired-network devices. This is due to the very nature of their use; they are mobile, they are on the edge of the network, their connections are unreliable, and they tend to get destroyed accidentally or maliciously. Security processing can easily overwhelm the processors in wireless devices. This challenge, which is unique to wireless devices, is sometimes referred to as the security-processing gap. Wireless networks lack appropriate security infrastructure, and give potential attackers easy transport medium access. Malicious attackers can be divided into two types. First is known as Focused attackers

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2017 SERSC

where these attackers are full time, dedicated professionals who have nothing better to do than target a specific enterprise an second is called as Opportunistic attackers who will attack a wireless network. Although several attacks have been addressed including active, passive eavesdropping, man-in-the-middle, replay, session hijacking, using traffic analysis, and masquerading, existing authentication schemes cannot fully protect hosts from well-known impersonation attacks. Impersonation attacks have the distinctive power to not solely determine the presence of those attacks however conjointly localize adversaries. Therefore, it's vital to detect the presence of spoofing attacks, determine the amount of attackers, and find the location of the attackers and eliminate them [1].

2. Main Issues for Providing Security in Wireless ad hoc Network

- **Identification issue** Nodes having access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication link the node should be capable enough to identify another node. As a result node needs to provide his/her identity as well as associated credentials to another node. The delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node.

- **Privacy Issue** The identification issue simultaneously leads to privacy issue for MANET. Mobile node uses various types of identities and that varies from link level to user/application level. Also in mobile environment very frequent mobile node is not ready to reveal his/her identity or credentials to another mobile node from privacy point of view. Any compromised identity leads attacker to create privacy threat to user device. Unfortunately the current mobile standards do not provide any location privacy and in many cases revealing identity is inevitable to generate communication link. Hence a seamless privacy protection is required to harness the usage of ad hoc networking [29].

3. Multi-layer Attacks

Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multilayer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks [30].

3.1. Denial of Service

Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks [32].

3.2. Man-in-the-middle Attacks

An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender [32].

 Copyright ⓒ 2017 SERSC

3.3. Impersonation Attacks

Impersonation attacks are particularly easy to launch and can cause significant damage to network performance. For example, in an 802.11 network, it is easy for an attacker to collect useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an If config command to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames an attacker can still spoof management or control frames to cause significant impact on networks[28].

Impersonation attacks are launched by using other node's identity, such as MAC or IP address [15]. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks. In reality wireless networks lack appropriate security infrastructure, and give potential attackers easy transport medium access. Rogue wireless access points deserve particular attention since they are not authorized for operation. They are usually installed either by employees or by hackers. Attention has been paid to finding rogues by using: Wireless sniffing tools (e.g., Air Magnet or Net Stumber), walking through facilities and looking for access points that have authorized Medium Access Control (MAC) addresses, vendor name, or security configuration,

- A central console attached to the wired side of the network for monitoring (e.g., Air Wave),
- A free Transmission Control Protocol (TCP) port scanner (e.g., Super Scan 3.0), that identifies enabled TCP ports.

At the point when source send any message to distinctive centers inside the framework then that threatening center also recover that rub and mishandled all the information Impersonation strike is key driver of plotting attack in which traded off hub infused noxious hub into the system also make number of imitated duplicate of pernicious hub for doing future assaults in general system [31].

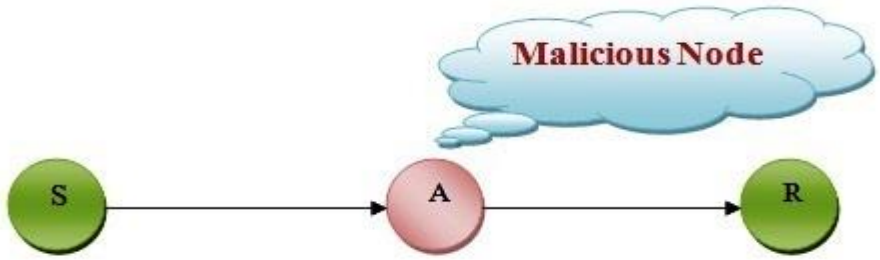

Figure 1. Impersonation Attack

In above Figure 1 S is the source and R is destination and A is intermediate node. Another node that is malicious node replaced its identity with intermediate node and hides its actual identity with other nodes. So when source send any message to other nodes within the network then that malicious node also get that massage and misused all the information Impersonation attack is main cause of colluding attack in which compromised node injected malicious node in to the network and make number of replicated copy of malicious node for doing future attacks in overall network [14]. Colluding attack consist of mainly two phases:-

1) Node injection attack 2) Node Replication attack

Impersonation attack take place in wireless sensor Network in following ways as in Figure 2. Wireless sensor networks (WSN) consist of a large number of small low cost devices called sensor nodes or motes. A sensor node is a self-contained entity typically consisting of a battery, transceiver, micro-controller and sensors. Attempted by the adversary to sensor nodes by impersonating a legitimate sensor node or a outside user. The vital goal of this attack is to send fake messages on behalf of a legitimate sensor node and obtaining sensor nodes data on behalf of a authenticated user [16].

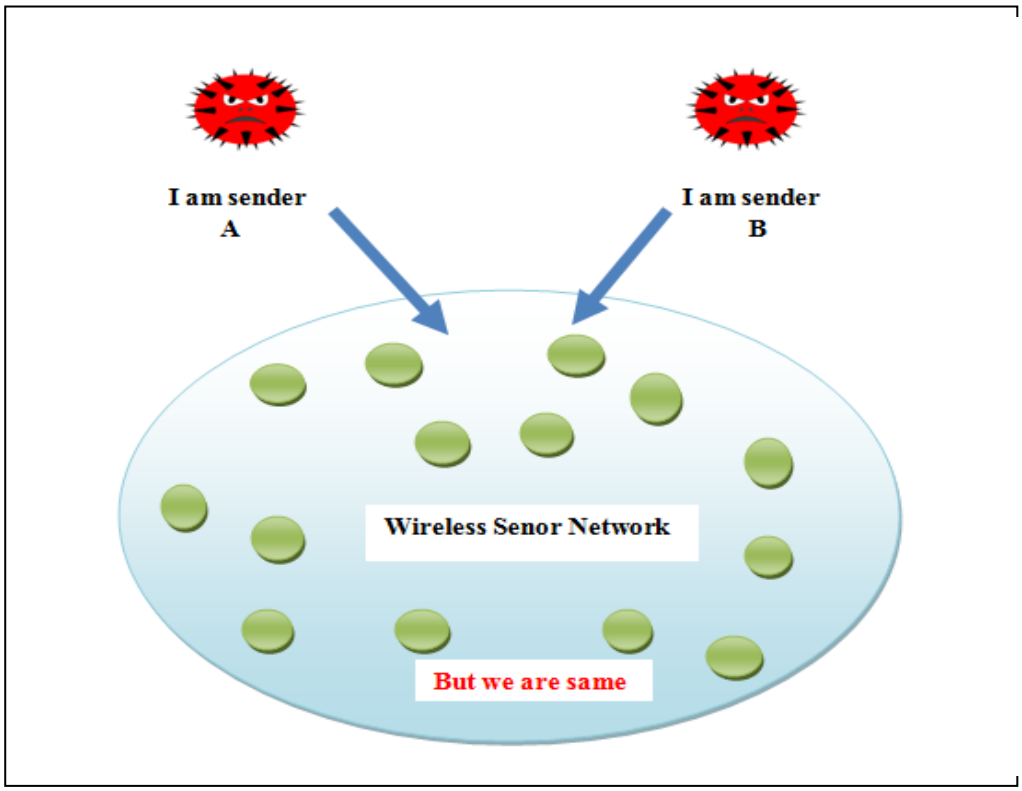

Figure 2. Impersonation Attack in Wireless Senor Network

4. Risk of Impersonation Attack

In understanding the risks, knowledge of the real threats helps place in context the complex landscape of security mechanisms [1]. Impersonation takes the form of device cloning, address spoofing, unauthorized access, rogue base station (or rogue access point) and replay.

- Device cloning consists of reprogramming a device with the hardware address of another device. This can be done also for the duration of one frame, which an operation termed MAC address is spoofing. This is a known problem in unlicensed services such as Wi-Fi/802.11. It is an enabler for unauthorized access and various attacks such as the de-association or de-authorization attack. It is interesting to note that a recent case of CDMA phone cloning occurred in India
- In Wi-Fi/802.11 networks, the identity of a device, i.e. its hardware address, can be easily stolen over the air by intercepting frames. Presently, no wireless access technology offers perfect identity concealment over the air. Presently, no wireless access technology offers perfect identity concealment over the air
- Impersonation of a legitimate user can be done to obtain unauthorized access to a wireless network [2]. Authorization at user level has been introduced in both

Copyright ⓒ 2017 SERSC

WiFi/802.11 and WiMax/802.16 to mitigate the threatThere are three options for authorization:

- **Device list-based:** If device list-based authorization is used only, then the probability of a subscriber impersonation attack is likely.
- **X.509-based:** X.509-based authorization uses certificates installed in devices by their manufacturers. X.509- based authorization is used, the probability for a subscriber to be the victim of impersonation is possible in particular if certificates are hard coded and cannot be either renewed or revoked.
- **EAP-based:** The Extensible Authentication Protocol (EAP) is a generic authentication protocol can be actualized with specific authentication method, If EAP-based authorization is used, we believe that at this time it is safe to say that the probability of a subscriber impersonation attack is possible[4].

- A rogue base station (or access point) is an attacker station that imitates a legitimate base station. The rogue base station confuses a set of subscribers trying to get service through what they believe to be a legitimate base station. It may result in long disruptions of service [3].
- The signal of the attacker, however, must arrive at targeted receiver subscribers with more strength and must put the signal of the impersonated base station in the background, relatively speaking. Again, the attacker has to capture the identity of a legitimate base station. Then it builds messages using the stolen identity.
- The scope of management messages to which authentication is applicable is limited in earlier versions of 802.16. Hence, with earlier versions of 802.16 the management messages are not subject to integrity protection. Weaknesses in management messages authentication open the door to aggressions such as the man in the middle attack or rogue base station attack.

The risk of impersonation in wireless networks is critical since the threat can be materialized into several forms of attack. Countermeasures are needed to address the threat.

5. Detecting Impersonation Attacks Using Device and User Profiles

One of the well known instantiations of identity theft, in WiFi/802.11 networks, is referred to as device cloning or Media Access Control (MAC) address spoofing. As aforementioned, this attack is carried out by obtaining the MAC address of a legitimate device, using tools that are readily available, *e.g.*, NetStumbler. This address is programmed into another device and subsequently used for obtaining unauthorized access to a Wireless Local Area Network [4].

- The continued use of an access control list (ACL), based on MAC addresses, which are easily supple, is no longer a viable strategy.
- In order to address device cloning and MAC-address spoofing, authentication based resolution strategies and intrusion detection-based countermeasures have been proposed [5].
- The use of public-key cryptography, the use of intruder location or user mobility patterns, is less susceptible to forgery and impersonation attacks. For one thing, as

Copyright ⓒ 2017 SERSC

intrusion detection mechanisms, both exploit behavioral characteristics or features, which are more difficult to forge or replicate.

- Both strategies require that an association, between a given MAC-address and its corresponding profile, be maintained for the purpose of detecting MAC-address spoofing. Essentially, it exemplifies the concept of using two or more pieces of identification for corroborating the identity of individuals.
- Air Defense does prevent MAC address spoofing by looking at the address prefix. Nevertheless, this approach is limited in that the IDS make a distinction between devices based only on the manufacturer's identification [7].
- The need to identify devices, there is an opportunity to further explore the use of device-based and user-based features for addressing the aforementioned problem.

In light of these circumstances, there is an opportunity to further explore the use of device-based and user-based features for addressing the aforementioned problem. The application of Radio Frequency Fingerprinting (RFF) and UMPs for Anomaly-Based Intrusion Detection (ABID) is presented in below Table 1.

Table 1. Defenses Mechanism Against Impersonation Attack

S.No	Defenses Mechanism	Description
1.	Radio Frequency Fingerprinting (RFF)[8]	RFF is a technology, which has been designed to capture the unique characteristics of the radio frequency energy of a transceiver, in RF-based wireless devices. a profile of each transceiver (using transceiverprints) is first created, followed by the classification of an observed transceiver print as normal or anomalous.
2.	User Mobility Profiling (UMP)[9]	UMPs have been used to address the inefficiencies of location-area based update schemes and to enhance routing in wireless mobile ad hoc networks its uses Instance-Based Learning (IBL) classifier .It compares an observed set of mobility sequences of a user to the training patterns in his/her profile.

6. Related Work

In order to detect and prevent impersonation attacks, many approaches are being researched. This section explains the related work. The traditional approach to prevent impersonation attack is to use cryptographic based authentication. Introduced a key management framework to apply secret sharing scheme and multicast server group. Due to limited resource on wireless devices cryptographic authentication may not be applicable. New approaches utilizing physical properties associated with wireless transmission to detect impersonation attack.

Generalized Attack Discover Model (GADE)

A generalized attack discover model that may each detect spoofing attacks in addition as verify the amount of adversaries victimization cluster analysis ways grounded on RSS-based spacial correlations among traditional devices and adversaries also use EPPM[12].

 Copyright ⓒ 2017 SERSC

Integrated Detection and Localization Framework (IDOL)

Integrated systems that can detect impersonation attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels [13].

RSS using EPPM

Ms. B. Lakshmi, Ms.B.Sanmuga Lakshmi, Mr.R.Karthikeyan proposed method that a spacial correlation of received signal strength (RSS) transmitted from wireless nodes to sight the impersonation attacks and using EPPM (efficient probabilistic packet marking) to detect the adversaries. Cluster-based mechanisms square measure developed to work out the amount of attackers. Once the coaching knowledge is accessible, we have a tendency to explore exploitation Support Vector Machines (SVM) methodology to improve the accuracy of crucial the amount of attackers. Additionally, we have a tendency to develop an integrated detection and localization system which will localize the positions of multiple attackers [11].

Location Spoofing Attack Detection

In [17], address the issues associated with location spoofing attack detection by examining relative location error rather than its absolute value. Specifically, the novel statistical and pattern matching techniques called relative error detection (RED) and topological residual fingerprint matching (TRFM) for detecting both signal strength and beam forming attacks. Also, the concept of geometric filtering is developed to considerably improve location reliability by exploiting the geometry of nodes

Bloom Filters and Dispersed Data Transmission

Wireless Sensor Networks consist of sensor nodes with wireless communication devices and sink nodes (destination nodes). Intermediate nodes relay the source nodes data packets to destination nodes. When an intermediate node steals a source node's ID within relayed data packets, it can impersonate the source node. In this paper, we have proposed a new detection method against such impersonation attacks using Bloom Filters and a Secret-Sharing-Scheme-based Dispersed Data Transfer method. In addition, we simulated this scheme to confirm its effectiveness [18].

We described the safety measure routing protocol against impersonation attack proposed by the various authors [4].

Table 2. List of Protocols that Prevent and Detect Impersonation Attack

S.No	Protocol	Description
1.	Secure Ad hoc On-Demand Distance Vector (SAODV)[21]	Secure Ad hoc On-Demand Distance Vector (SAODV) is an extension of the AODV routing protocol that can be used to prevent impersonation attack. In this attack, the attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes.
2.	Authenticated Routing for Ad hoc Network (ARAN)[19]	The authenticated routing protocol (ARAN) detects and defends against malicious activities by third party and peers in an ad hoc network. There are two different stages of ARAN consists of a preparatory certification process and then it performs a path instantiation

Copyright ⓒ 2017 SERSC

		process which assures and guarantees end-to-end authentication
3.	Timed Efficient Stream Loss-Tolerant Authentication (TESLA)[20]	TESLA provides delayed per-packet data authentication and integrity checking. The key idea to providing both efficiency and security is a delayed disclosure of keys. The multilevel TESLA proposed in to prolong hash chain lifetime.But it is still desirable to update hash chains online when impersonation is detected.
4.	A Secure On-Demand Routing Protocol for Ad Hoc Networks (ARIADNE)[22]	Ariadne can authenticate routing messages using schemes shared secret keys between communicating nodes combined with broadcast authentication, or digital signatures.
5.	Secure Efficient Ad hoc Distance Vector (SEAD)[23]	SEAD performs against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.
6.	Security Aware Routing **(**SAR)[25]	SAR enables the discovery of secure routes in a mobile ad hoc environment. Its integrated security metrics allow applications to explicitly capture and enforce explicit binding between the identities of the user with the associated trust level. With this binding, any user can impersonation attack is prevented.
7.	Secure Routing Protocol (SRP)[24]	Secure routing protocol for mobile ad hoc networks that guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes.
8.	Cooperation Of Nodes Fairness In Dynamic Ad-Hoc Networks (CONFIDENT)[26]	CONFIDANT protocol detect and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes.
9.	Novel Approach for Secure Routing Protocol **(**NASRP)[27]	NASRP enhance the security levels in the routing protocol by introducing peer review process has been introduced to check the integrity and non-repudiation of the routing packets and key exchange packets.

The above Table 2 lists various secure protocols that detect and prevent impersonation in wireless network

7. Conclusion

Impersonation attacks to acquire some confidential information that should be kept secret during the communication. The information may include the location, public key private key or even password of the nodes. An adversary node may preset multiple identities to a peer to peer network in order to appear and function as distinct node. By turning into part of the peer to peer network the adversary may the take in communication. The introduction of impersonation attack in any network there is a reduction of throughput in the network. Packet delivery ratio also drops and there is an increases checksum error and packet loss ratio. It is therefore required to have an efficient protection mechanism that can mitigate the severity of these attacks and provide seamless authentication scheme with least possible overhead. Thus this survey presents about causes of impersonation attack, their vulnerable effects which give chance to a malicious

 Copyright ⓒ 2017 SERSC

node for doing other attacks and protection mechanisms, discuss various security protocol that prevent and detect impersonation attack in wireless network.

References

[1] Michel Barbeau, Jyanthi Hall, and Evangelos Kranakis "Detecting Impersonation Attacks in FuturWireless and Mobile Network",MADNES 2005, LNCS 4074, pp. 80–95, Springer-Verlag Berlin Heidelberg 2006.
[2] IEEE Computer Society. IEEE Std 802.11i-2004 IEEE standard for information technology-telecommunications and information exchange between systems- local and metropolitan area networks-specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 6: Medium access control (MAC) security enhancements. Standard Number IEEE Std 802.11i-2004, 2004.
[3] IEEE Computer Society. ANSI/IEEE std 802.11 - wireless LAN medium access control (MAC) and physical layer PHY specifications, 1999.
[4] Nidhi Gour1,Monika Agarwal ,Heena Singh,Ajay Kumar, "A Review on Impersonation Attack in Mobile Ad-Hoc Network"International Journal of Computer Trends and Technology (IJCTT) – volume 8 number 1– Feb 2014
[5] B. Sun and F. Yu. Mobility-based anomaly detection in cellular mobile networks. In International Conference on WiSe 04, pages 61–69, Philadelphia, Pennsylvania,USA, 2004.
[6] Aakansha Jain, Khushboo Sawant "Effect ofImpersonation Attack on Mobile Ad Hoc Network"Indian Journal of Research,2(3), March 2013, 17-19.
[7] Frank Adelstein, Prasanth Alla, Rob Joyce, and Golden G. Richard III. Physicallylocating wireless intruders. In Proceedings of the International Conference onInformation Technology: Coding and Computing (ITCC'04), pages 482–489, 2004.
[8] K.J. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. Radio Science, 36:585–597, 2001.
[9] K. Wu, J. Harms, and E.S. Elmallah. Profile-based protocols in wireless mobile ad hoc networks. Local Computer Networks, pages 568–575, 2001.
[10] Latha Tamilselvan and Dr. V. Sankaranarayanan "Prevention of Impersonation Attack in Wireless Mobile Ad hocNetworks" IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007
[11] Ms.B.Lakshmi, Ms.B.Sanmuga Lakshmi, Mr.R.KarthikeyanDetection and Prevention of Impersonation Attack in Wireless networks International Journal of Advanced Research in Computer Science & Technology Vol. 2 Issue Special 1(IJARCST 2014)
[12] Lamia Fattouh Ibrahim, " Using of Clustering and Ant-Colony Algorithms CWSP-PAM-ANT in Network Planning",International Conference on Digital Telecommunications(ICDT 2006), Cap Esterel, French Riviera, France, 26-31 August 2006.
[13] R.Tamilarasi Jaharlal Sarkar "Multiple Spoofing Attackers Detection and Localization in Wireless Networks",International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 9, March 2014
[14] Er. Aakansha Jain ,Er. Khushboo Sawant "Effect of Impersonation Attack on Mobile AdHoc Network ",Paripex - Indian Journal of Researchissn - 2250-1991 Volume : 2 Issue : 3 March 2013
[15] Nidhi Gour,Ajay Kumar "Efficient Detection and Prevention of Impersonation attack in MANET",International Journal of Advance Research in Computer Science and Management StudiesVolume 2, Issue 9, September 2014
[16] Shish Ahmad "Energy Efficient Public Key Framework in Adhoc Sensor Networks ",2014
[17] Jeong Heon Lee ; Buehrer, R.M., "Location Spoofing Attack Detection in Wireless Networks", IEEE, 2010.
[18] Besancon,"An Impersonation Attack Detection Method Using Bloom Filters and Dispersed Data Transmission for Wireless Sensor Networks", 2012 IEEE International Conference on Green Computing and Communications
[19] Ravi Raval, Ketan Sarvakar A Security Survey of Authenticated Routing Protocol "International Journal of Innovative Research in Science,Engineering and Technology" ISSN: 2319-8753 Vol. 2, Issue 12, December 2013
[20] Ying Huang, Wenbo He, Klara Nahrstedt " ChainFarm: A Novel Authentication Protocol for High-rate Any Source Probabilistic Broadcast" IEEE 2009
[21] Manel Guerrero Zapata "Secure ad hoc on-demand distance vector routing " Volume 6 Issue 3, July 2002 Pages 106-107
[22] Yih-Chun Hu and Adrian Perrig "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks"Springer Science Business Media, Inc. Manufactured in The Netherlands 2005 .
[23] Yih-Chun Hu a, David B. Johnson "Adrian Perrig aSEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Published by Elsevier B.V 2003.

Copyright ⓒ 2017 SERSC

[24] Panagiotis Papadimitratos and Zygmunt J. Haas "Secure Routing for Mobile Ad hoc Networks ,SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)", San Antonio, TX, January 27-31, 2002
[25] Seung Yi, Prasad Naldurg, Robin Kravets "A Security-Aware Routing Protocol for Wireless AdHoc Networks
"Urbana,Report No. UIUCDCS-R-2001-2241, UILU-ENG-2001-1748 ,August, 2001
[26] Sarvesh Acharya ,Gulshan Kumar ,Vikas SinghM-CONFIDANT: A Multicast based Cooperation of Node Fairness in Dynamic Ad hoc Network International Journal of Computer Applications (0975 – 8887) Volume 73– No.19, July 2013
[27] Faruk, Imran Hossain "A Novel Approach of Secure Routing Protocol for Mobile Ad Hoc Network "Thesis Report NIT Rourkela 2013
[28] Sanmuga Lakshmi.B, Tamizh Arasan.P "Detection and Prevention of Impersonation Attack in Wireless networks "IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
[29] Anna Saro Vijendran,J.Viji ripsy"Meticulous Investigation Of Impersonation Attackson Manets Using Different Routing Protocols"International Journal of Computer Engineering and Applications, Volume V, Issue I, Jan.14
[30] Sandhya Khurana,"Handling Attacks on Routing Protocols in Ad hoc Networks"thesis submitted to University of Delhi,June, 2011.
[31] Margam,K. Suthara “Survey of Various Attacks against Wireless ad hoc networks “International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 1, 2015
[32] Shikha Sharma , Manish Mahajan “A Study of Attacks at Different Layers in Mobile Ad-Hoc Network” ,International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 6, June 2016

Authors

R. Regan, is working as an Assistant Professor in the department of Computer Science and Engineering at University College of Engineering Villupuram, Anna University, India. He acquired B.E. Degree in Electronics and Communication Engineering from Mailam Engineering College, Mailam in 2006. He received M.Tech Degree in Computer Science and Engineering from Bharath University, Chennai in 2010. He is pursuing Ph.D Degree in the Faculty of Information and Communication Engineering at Anna University, Chennai. He has over 5 years of experience in educational institution. He has to his credit 11 publications in National/International conferences and journals. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Wireless security.

J. Martin Leo Manickam, is working as Professor in the Department Electronics and Communication Engineering at St. Joseph’s College of Engineering, Chennai. He acquired B.E. Degree in Electronics and Communication Engineering from Alagappa Chettiar College of Engineering and Technology, Karaikkudi in 1995. He received M.E. Degree in Optical Communication and Ph.D degree in the Faculty of Information and communication Engineering from the College of Engineering, Anna University, Chennai. He has over 16 years of experience in teaching and guiding projects for Undergraduate and post graduate students. Under his guidance, One scholar had got Ph.D degree and 12 research scholars are pursuing their Ph.D programme. He has to his credit 15 publications in National/International conferences and journals. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Digital Communication and Network Security.

 Copyright ⓒ 2017 SERSC