International Journal of Advances in Computer Networks and Its Security
Volume 6 : Issue 1 *[ISSN 2250-3757]*

Publication Date : 18 April, 2016

Detecting and Focalizing Spoofing Attacks in Wireless Networks

Neelavathy Pari S, Siva Kumar G R , Vignesh P

***Abstract*— An important problem in wireless network security is node authentication. The existing schemes for node authentication are based on IP and MAC address which can be easily spoofed by the adversaries. Wireless spoofing attacks are easy to establish and significantly affects the functionality of the network. In the proposed approach, log files are used for authenticating each node which is hard to falsify and difficult to modify or delete the contents. The proposed system determines the spoofing attacks and localize the adversaries using spatial correlation of received signal strength (RSS). In this paper, the problem of identifying the number of attackers is determined by Partitioning Around Mediods (PAM), a cluster-based analysis method and Euclidean distance between successive packets. The simulation results show that the proposed approach over performs all other existing approaches with high detection ratio.**

***Keywords*— Spoofing attacks, RSS, PAM, Euclidean distance.**

I. Introduction

Due to the receptiveness of the wireless transmission medium, assaulters can monitor any transmission. Security has become an elementary concern in order to provide invulnerable communication between mobile nodes in an uncongenial environment. Among the various types of attacks, individuality-based spoofing attacks are peculiarly easy to launch but causes significant damage to network performance. For instance, in an 802.11 network, it is easy for the attacker to gather MAC address information during passive monitoring and tend to modify its MAC address by simply issuing the ipconfig command to masquerade as another device. Spoofing attacks are a grievous threat as they constitute a form of identity compromise. It is thus important to discover spoofing and eradicate them from the network. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or 802.11i (WPA2), the data frames alone can be protected. Spoofing attacks can promote a variety of injection attacks [1], [2].

Although the existing IBA (Identity Based Attacks) detection schemes work well in a static network, they tend to raise excessive false alarms in the mobile environment where the RSS profiles changes over time due to node mobility. Most subsisting approaches to detect spoofing attacks are based on RSS (Received Signal Strength) [3], [4], [5]. However, all the existing system assumes that original node should be in the network when the spoof node enters into the network. This is not possible in all the cases especially when a spoof node enters into the network prior to original node, the network identifies the spoof node as original node. Hence all the existing approaches fail to identify the spoof node when the original node is not participating in the network, the proposed system aims to rectify this problem. The another major issue confronted is, when the original node is not present in the network there is more possibilities for more than one spoof node to intrude the network by taking the identity of the original node.

Therefore, it is important to detect and localize the adversaries in the wireless network. The proposed work uses network log files for monitoring the behavior of the wireless nodes and uses received signal strength (RSS)-based spatial correlation[6], a physical property associated with each wireless node that is hard to warp and not dependent on cryptography, as the basis for localizing spoofing attacks. Since we are implicated with assaulters having different locations than licit wireless nodes, the RSS information is used to identify the spoofing attacks and to focalize the assaulters. RSS will not require any additional cost or modification to the wireless devices which is an added advantage. Typically, a wireless device does not often change its transmission power, therefore a drastic change in RSS measurements of received frames from the same MAC address suggests a possible spoofing attack. The farther the attacker is far away from its victim, the more likely their RSS patterns differ significantly and it is easier to detect the spoofing attacks. Although various authentication frameworks are

Neelavathy Pari S
Assistant Professor
MIT Campus, Anna University

Siva Kumar G.R
PG Scholar, MIT Campus, Anna University

Vignesh P
BE III year Student, MIT Campus, Anna University

existing such as hop-by-hop authentication protocol [7], still identity-based attacks are easier to launch since authentication is provided only for data frames.

The paper is organized as follows: Section II describes the related work in broader context. Section III, specifies the attack detection model and presents the theoretical approach used in the proposed system. Section IV describes the localizing of identity-based attacker.

II. Related Works

Recently, there has been live researches are taking place dealing with spoofing attacks as well as those facilitated by adversaries masquerading as another wireless device. Rather, we give a short overview of traditional approaches and several new methods. We then describe the works most closely related to our work. Cryptographic authentication for fraud identification has been used in traditional approaches. An authentication framework for hop-by-hop authentication protocol was presented in [7], which works for data frames but not for node identification. Additional infrastructural overhead and computational power are needed to distribute, maintain and refresh the key management functions required for authentication. A practical approach for landmark deployment in indoor localization has introduced [8] which described the localization of mobile node in indoor environment. A novel RSS based technique, Reciprocal Channel Variation-based Identification (RCVI) has been used to detect identity-based attacks in mobile environment [9] where pairing frames and RSS traces are the mixer of victim and attacker node. The most relevant work to our paper is [10], which proposed the use of matching rules of signal prints for spoofing detection. Although these methods have diverging detection and false alarm rates, none of these techniques provide the ability to focalize the positions of the spoofing attackers after detection. Further, this work is novel in that we have integrated our spoofing detector into a real-time localization system which can both detect the spoofing attacks, as well as focalize the assaulters in wireless and sensor networks. The works [11], [12] used RSS value and path loss exponent for detecting and focalizing the attackers. Path loss and shadowing effect are considered during the recording of RSS traces from each node.

The existing approaches detects the attackers based on cryptographic schemes or they highly depend on the spatial information such as RSS value whereas the proposed work uses log files for assaulter detection. The proposed method differs from the fact that all of the existing approaches detects the spoof node only when the original node is participating in the network. The existing approaches are based on the assumption that when the spoof node enters into the network, the original should be in the network. But what happens when the spoof node enters into the network before the original node. Our detection approach solves this problem with help of log files which is briefly discussed in Section III.

III. Attack Detection Model

In this section, we describe our Attack Detection Model (ADM), which has two phases: attack detection, which detects the presence of an attack, and focalizing the assaulter, which determines the location of the adversary. The focalizing the assaulter phase will be presented in Section 4.

A. Log File Creation

A log file is a file in which a computer system handles a record of its activities. Log files are used to discover where nodes are originated from, how often they turn back, and how they navigate through a network. A log file contains symptomatic information about interoperability, loading the program, and networking. In networking, mobility and behavior of the nodes are monitored and recorded. A log file is created for each and every individual node for monitoring its transmission. Log file details are gathered from each node during transmission. Since log files are write protected, modifying or deleting the data is a hectic work. Log files are used as parameter for authenticating the mobile nodes in the wireless environment. Log file contains complete details such as sent node, packet delivery time and its sequence number. Our approach is novel because none of the existing methods can determine the attacker, when the original node is not present in the network. Using this log file details spoof node can be detected based on the packet delivery time for each packet where packet delivery time is calculated as

$$P_{time} = P_{rt} - P_{st} + P_d \quad (1)$$

where P_{rt} is the time at which the receiver node receives the packet and P_{st} is the time at which sender node sends the packet and P_d is the propagation delay. All these factors are integrated as packet delivery time. If the calculated packet delivery time is greater than the threshold value τ, then that node is

predicted as spoof node. Structure of log file is given in the Fig. 1.

Sent Node	Sent Time	Intermediate Node	Forward Time	Packet Delivery Time	Receive Node	Packet Delivery Time	Sequence Number

Figure 1. Structure of the log file

B. Conceptualization of Attack Detection

Attackers can affect the network in various ways. In this work following scenarios are considered.1) Spoof node enters the network when the original is not present in the network. 2) Multiple spoof nodes enter the network when the original node is not participating in the network. 3) Spoof node enters the network when the original node is present in the network. 4) Multiple spoof nodes enter when the original node is present in the network

First scenario is rectified by using the information provided in the log files. Outline of log file is depicted in Fig. 1 where packet delivery time for each packet is calculated and verified whether it is greater than threshold or not. If the packet delivery time is greater than the threshold, then the node which forwarded the packet is suspected and verified whether the delay due to network congestion or traffic. If the delay is not due to network congestion or traffic then that node is predicted as spoof node or attacker.

The second scenario is depicted in the Fig. 1 where more than one spoof nodes are present in the network but the original node is not taking part in the network. If a spoof node is predicted using the information provided by the log file, Euclidean distance between successive packets are measured, in order to make that only one attacker present in the network. In Fig. 2 both attacker 1 and attacker 2 share the same MAC address but the authentic node corresponding to that MAC address is not active. Since authentic node is not active, the victim node believes that attacker 1 is an authentic node but this problem is sorted out using log file as described in the Section III earlier. But what happens when there is more than one spoof node sharing the same MAC address and communicating with the victim node. When there are more than one attacker then the Euclidean distance between the successive packets are measured [13] as

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}. \qquad (2)$$

where x_1, x_2 are the x coordinate values of successive packets and y_1, y_2 are the y coordinate values of successive packet. If the Euclidean distance between two successive packet is greater than the threshold then it resembles more than one attacker is present in the network. Since the nodes are geographically separated, the distance between successive packets should be uniform. But this metric works well only when the nodes are geographically separated by far distance. If the nodes are extremely closer and using the same power levels. In this case the attackers bypass the detection technique since they are localized to same location.

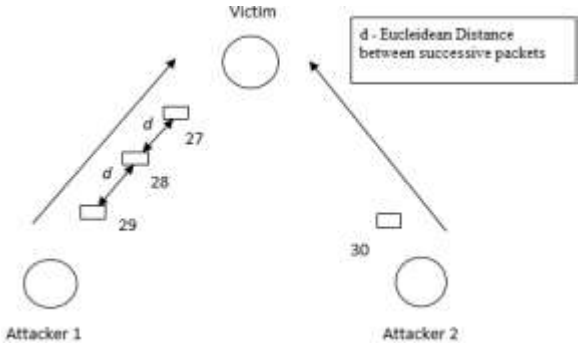

Figure 2. More than one attacker in the network sharing the same MAC address and both communicates with the victim node at the same time.

If two spoof nodes communicate with the victim node, since the nodes are geographically separated the Euclidean distance between successive packets will not be uniform. In Fig. 3 the Euclidean distance d_1 of attacker 1 for successive packets is uniform and less than the threshold value τ. But it is greater than the threshold ($d_2 > \tau$) for attacker 2 since it is geographically separated from attacker 1 by far distance.

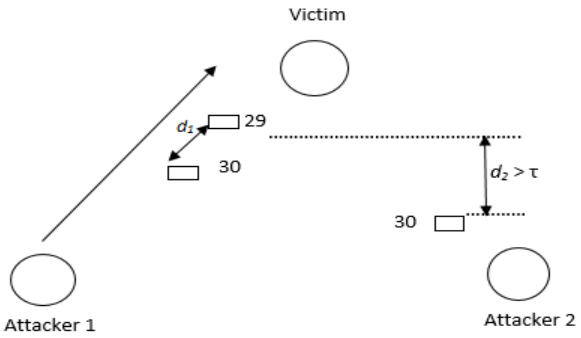

Figure 3. Both attacker 1 and attacker 2 sending the same packet to the victim and the Euclidean distance between successive packets is less than the threshold for attacker 1 but greater than threshold for attacker 2

Therefore using Euclidean distance between successive packets the second scenario is resolved. Next scenario, the spoof node enters the network when the original is actively participating in the network. Since concerned with attacker having different location, we proposed to use receive signal strength (RSS). RSS information is the strength of signal at the receiver. During generation of signals from sender to receiver various environmental phenomena can interfere the original signal either in constructive or destructive way. Transmitted signal also sustain from absorption and attenuation which further reduces receive signal strength. Aggregated effect of all this that RSS value reduces exponentially with distance. RSS value is highly reliant on environmental phenomena such as walls, obstacles, so this value fluctuates due to noise and fading effect. Since RSS information is highly dependent on environment which makes it laborious for attackers to spoof the RSS value.

Although affected by random noise, multipath and fading effect, RSS value for each node at a particular distance changes only small amounts. RSS value of a mobile node [10] are distinctive at different locations. When there is no identity-based attack, the sequence of RSS sample vector will oscillate around a mean value. If a node is spoofed then the RSS value of that node will be mixer of both original node and spoof node. Since spoof node is geographically separated by far distance from the original, the recorded RSS value will have immense variation. But variation may be because of node mobility or due to interference of environmental phenomena. By varying the threshold value, check for the accuracy and false positive rate. RSS vector values from same node is recorded if the variation is greater than threshold value then partition the vector values into 2 vectors. Using these vector values cluster analysis is made on top of it. Partitioning Around Mediod (PAM) cluster analysis method is utilized for cluster formation [link]. RSS value is recorded for each t times, if the difference between RSS value at t_1 and RSS value at t_2 is highly varying then two nodes or more than two nodes are sharing same node identity as shown in Fig. 4. These RSS traces are clustered using PAM algorithm where mediods are identified in a iterative manner. Mediods are the instance object of a cluster with a data set whose average dissimilarity to the other objects are minimal. Mediods are calculated iteratively based on the minimal cost as :

$$C_{min} = \sum_{i=1}^{n} \sum_{r_m \in r_i} \| r_m - M_i \|^2 \quad (3)$$

Where M_i is the initial mediod and r_m is the RSS trace obtained. Mediods are calculated based on the cost calculated based on "(3)". RSS traces are separated into two classes (i.e n =2) so two cluster are formed. If the distance between the mediods are larger than spoofing attack is present in the network. Distance between two mediods are calculated as follows:

$$D_c = \| M_i - M_j \| \quad (4)$$

Where Mi and Mj are mediods of two cluster C_1 and C_2. Initial mediods are chosen from "(3)". This section determines the detection of identity-based attack and localizing the attackers is described in section IV.

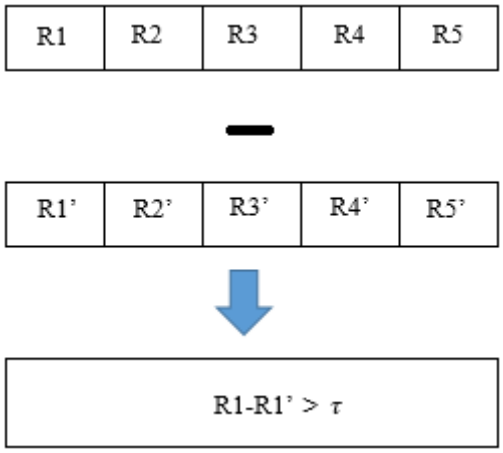

Figure 4. RSS value is recorded for each t time and R1 is the RSS value at time t_1 and R1' is the RSS value at time t_2.

C. Theoretical Analysis of RSS

Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks [8]. The RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics. According to the propagation model, the RSS at a landmark from a wireless node is given by [12]

$$P(di)\ [\text{dBm}] = P_i(d_0)\ [\text{dBm}] - 10\gamma \log(d_i/d_o) + S_i \quad (1)$$

where *i* is the *i*th wireless node, *Pi*(*d*0) represents the transmitting power of node *i* at the reference distance *d*0, *di* is the distance between the wireless node and the landmark, γ is the path loss exponent, and *Si* is the shadow fading that follows zero-mean Gaussian distribution with δ standard deviation. Assume that the wireless nodes have the same transmission power.

IV. Localizing Adversaries

A. Localization System

We have developed a general-purpose localization system to perform real-time indoor positioning. This system is designed with fully distributed functionality and easy-to-plug-in localization algorithms. In the beginning of the localization algorithm, a legitimate node or landmark broadcasted a "*discover*" packet to find surrounding attacker node with accurate coordinates. The attacker nodes would send a "*reply*" packet containing node ID in response to the landmark node node if they received a *discover* packet. Then, the landmark node would compute its coordinate according to the distances translated from the RSSIs of the *reply* packets from at least three reference nodes.

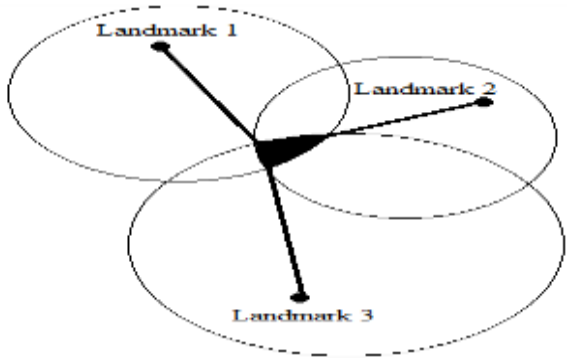

Figure 5. Illustration of localization of mobile nodes

V. Results And Discussion

Fig. 6 presents the packet delivery time of both original and spoof node. Packet delivery time for each packet is calculated and recorded in log file. As observed, after sequence number 27, packet delivery time of spoof node differs from original node. The maximum time taken for original to transmit a packet is 0.4 but for spoof node the maximum time taken is 0.8. After running many simulation, packet delivery time for each packet is calculated and average of these values are considered as threshold value. Average threshold value obtained is 0.6 using various simulation results. In Fig.5, spoof node's packet delivery time is greater than the threshold value

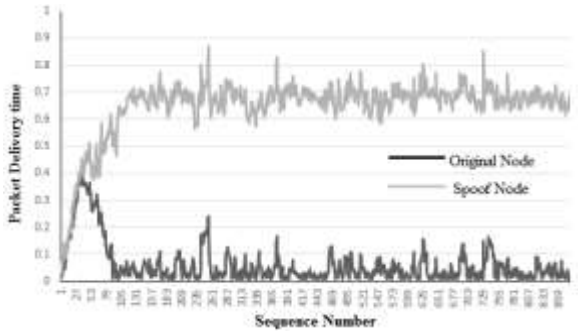

Figure 6. Packet delivery time for original and spoof node

In Fig. 7 by varying the position of mobile node packet delivery time are recorded. As mobile nodes moves randomly in the hostile environment packet delivery time is varying for both original and spoof node. Although packet delivery time for original node are varying still the time taken for spoof node are greater than the packet delivery time of original node.

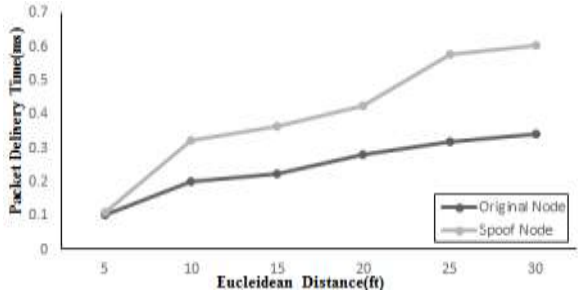

Figure 7. Packet delivery time vs Euclidean distance

VI. Conclusion

MAC spoofing attacks in 802.11 networks exploit a fundamental vulnerability of the 802.11 protocol: the MAC addresses of wireless frames can be easily forged, imposing a serious security challenge. Physical-layer information, such as Received Signal Strength (RSS), is hard to forge arbitrarily and can be used to detect such spoofing. Existing RSS-based spoofing detection methods suffer from large RSS variations due to common antenna-diversity technology. In this paper we propose to use log files and RSS profiling, and show how to use it to detect spoofing attacks. A key element of future work is to apply cluster-based analysis on the obtained RSS values.

References

[1] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. USENIX Security Symp., pp. 15-28, 2003.

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2004.

[3] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM, pp. 2441-2449, Apr. 2008.

[4] J. Yang, Y. Chen, and W. Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.

[5] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), pp. 193-202, May 2007.

[6] Jie Yang and Wade Trappe, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 24, no. 1, 2013

[7] A. Wool, "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.

[8] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), pp. 365-373, Sept. 2006.

[9] Kai Zeng, Kannan Govindan, Daniel Wu, and Prasant Mohapatra, "Identity-Based Attack Detection in Mobile Wireless Networks," Proc. IEEE INFOCOM, pp. 1880-1888, 2011.

[10] Sudip Mishra, Ashim Ghosh and A.P.Sagar, "Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signalprints," Proc. IEEE Int'l Conf. on Cyber, Physical and Social Computing, pp. 35-41, 2010.

[11] Naveed Salman and Mounir Ghoghoi, "On the Joint Estimation of the RSS-Based Location and Path-loss Exponent," Proc. IEEE Wireless Communication Letters, Feb. 2012.

[12] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A Survey of Various Propagation Models for Mobile Communication," IEEE Antennas and Propagation Magazine, vol. 45, no. 3, pp. 51-82, June 2003.

[13] Gayathri Chandrasekaran, Wade Trappe and Marco Gruteser, "Detecting Identity Spoofs in IEEE 802.11e Wireles Networks," Proc. IEEE "GLOBECOM", 2009.

[14] Q. Li and W. Trappe, "Light-weight detection of spoofing attacks in wireless networks," in Proc. of the 2nd I Int'l Workshop on Wireless and Sensor Network Security (WSNS), October 2006.

[15] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS), 2006.

[16] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.

[17] A. Krishnakumar and P. Krishnan, "On the accuracy of signal-strengthbased location estimation techniques," in *Proc. IEEE INFOCOM*, Mar. 2005, pp. 642–650.

[18] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: A quantitative comparison," *Comput. Netw.*, vol. 43, no. 4, pp. 499–518, Nov. 2003.

[19] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in *Proc. 3rd IPSN*, Apr. 2004, pp. 259–268.

[20] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in *Proc. 3rd IEEE SECON*, Sep. 2006, pp. 50–59.

[21] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the third ACM conference on Wireless network security, WiSec '10*, 2010, pp. 89–98.

[22] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, "The robustness of localization algorithms to signal-strength attacks: A comparative study," in *Proc. DCOSS*, Jun. 2006, pp. 546–563.

[23] J. Yang, Y. Chen, and W. Trappe, "Detecting Sybil attacks in wireless and sensor networks using cluster analysis," in *Proc. 4th IEEE Int. Workshop Wireless Sensor Netw. Security*, Sep. 2008, pp. 834–839.

[24] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks WOWMOM*, 2006, pp. 564–570.

S. Neelavathy Pari is a Assistant professor in the Department of Computer Technology at Anna University, Chennai, India. She received her Ph.D. degree in the Faculty of Information and Communication Engineering, Anna University in 2014 and has extensively published in the areas of security in MANET. She is the active member of ACM and CSI.

Sivakumar G R received his BE degree from Anna University in 2011 and currently PG student in the Department of Computer Technology, Anna University, India. His research interest is security in wireless networks.

Vignesh P currently doing his BE degree in the Department of Computer Technology, Anna university, India. His research interest is cryptography and network security.