Active Attacks Detection Mechanism using 3-Phase Strategy

Sobia Aslam[1], Saleem ullah[2,*], M. Abubakar Siddique[3], Abdul Sattar[4]

[1] Department of Computer Science & IT, The Islamia University of Bahawalpur, Bahawalpur, Pakistan
[2,3,4] Department of Computer Science & IT, Khwaja Fareed University of Engineering & Information Technology, Abu Dhabi Road, Rahim Yar Khan, Pakistan

Summary

To protect the network systems from the incident of happening of attacks, it is very necessary to create different prevention and detection techniques. To observe and examine outdoor, indoor and complex systems, there is a big need to create efficient monitoring systems. However, Security is a big challenge in this era due to increase in the number of security threats, these severe security threats are also known as Security attacks that affect the functioning of networks. In my research the main focus is on the classification and analysis of Active attacks and their detection to protect the networks from malfunctioning caused by them as we know that particularly most irritating and upsetting attacks are known as Active Attacks. So, I propose to use a firewall system to detect and prevent these network attacks by using packet filtering technique and providing a mathematical model for the detection of active attacks. My research work is proposing to use a packet filtering as a tool to model and analyze the security properties of a detection model. Usage of packet filtering algorithm for modeling and analysis of detection technique and firewalls provides the possibility to check and mathematically prove some security belongings. This research is presenting an approach to detect network attacks, as the network attacks are continue to plague the internet environment, existing anti-viruses and intrusion detection systems are insufficient to defend against these worst attacks.

Keywords:
Active attacks, Classification, Attack detection techniques, Security

1. Introduction

The main purpose of Detection Systems is to alert and secure the networks from suspicious activities and threats. Detection Systems cover the many areas but this section is just focusing on the Detection andsecurity from Active Attacks. Active attack detection can be defined as “the problem of identifying the individuals/programs who are utilizing the computer systems and their resources without legal authorizations and registrations, they not only use these systems and resources even produce alteration and disruption in the private data of organizations and network systems”. To make secure our systems it is very necessary to develop efficient detection systems to prevent damages and unauthorized accesses to private information zones. Furthermore an active attack is an internet abuse in which an attacker tries to make modifications to the data on the mark or data in direction to the mark. An asset as well as logical or physical is called as a resource of any security system, which can contain one or more threats that can be utilized through vulnerability or vulnerable driving force in a vulnerary action. So, Detection Systems are biggest need of this era to remain alert from severe and suspicious activities in our network systems. The Paper is organized as follows; Section 2 is introducing about related work, Section 3, 4 are giving a review on Types and Classification of Active Attacks, Section 5, 6 are introducing about Network Security and detection Systems, Section 8 is elaborating Proposed Detection Model while Section 9 and 10 concludes the paper with a Future Work review.

2. Related Work

The requirement of Security is confidential, undisclosed, secretive and even strategic information or data. The most important step that an organization can take to guard its network is the application of an effective and strong security policy [1].

Main purpose is to stress the various attacks and dangers that network administrators face and essential of locating a suitable network security guideline. When an attack is detected the analyst requires some time to set up the attack nature. Active attacks are very dangerous and risky because they change the condition and position of data or information [2].

We can use term attack as virus and the term virus is also utilized for worm that replicates itself to other codes or programs to make system vulnerable. In the communication path, data stream is monitored, listened and altered by illegal attackers, these illegal attackers are known as active attacks [3].

Particularly shocking attack is known as active attack, where two or more malicious smash nodes produce a higher level virtual channel in the network. It is employed to transmit data packets between the channel end points or nodes, these channels imitate shorter links in the network [5].

These types of attacks are assumed as hackers are transmitting data to the targeted environments, attempting to access a system or environment by cracking its security

*Corresponding author:
Dr. Saleem Ullah (saleem.ullah@kfueit.edu.pk)

paper receiving date : 10 October 2016
Paper acceptance date: 20 jan 2017

and limitations and taking out information, these attackers can also try to split the outskirts just to create a service delay or interrupt. The issue of attack detection is very tough. The detection technology is at beginning stage these days. Whenever attack is detected, attacker remains unrecognized. After the detection of attack or threat, analyst requires some of time to develop the attack type [6].

Current detection methods use passive approaches and strategies to detect and monitor the ARP traffic looking for inconsistencies in the Ethernet address IP mapping. There is a major drawback of using passive approach that is time pause or wrap between the learning and detecting spoofing, that mostly directs to the threat being discovered long after it has been caused destruction. So we are proposing an active technique to detect and monitor the ARP spoofing, that is so much faster, reliable, intelligent and more scalable in detecting threats or malicious behaviors [8].

Many researchers are busy in progressing and improving old approaches of detection and prevention, finding and developing new approaches that are well suited and effective for the safety of MANETs. Almost all the intrusion detection systems are structured in two architectures which are distributed and cooperative. The main purpose to propose and develop effective approaches of intrusion detection systems is that attacks must be detected before they can do any danger or malware activity in the system to spoil and disrupt the data [9]. In [5] [6] [9] [11] [12] [18] [22] [23] a large number of active attacks, their analysis and detection techniques have been discussed.

3. Active Attacks

3.1 Impersonation Attacks

It refers to carry out illegal or unauthorized action or attempt by impersonating a legal or justifiable user of the security system.

3.2 Piggybacking

It means to intercept interaction or exchanges (communication) between the operating system and user through the modifications or substitutions of new messages.

3.3 Spoofing

It refers to penetrators that make fool users into thinking that they are interacting with the operating system. It cause duplication of logon procedure and capture the user password.

3.4 Backdoors/Trapdoors

These types of active attacks refer to utilization of the opportunities and facilities of operating systems without being part to control. Users execute the Trojan horses (programs written by the cracker or penetrator), these programs initiate the unauthorized or malicious activities e.g. copy of most sensitive and private data.

4. Classification of Active Attacks

These attacks can be classified into four main categories;

4.1 Snooping

Simply it refers to gain the private information which can be used as a personal benefit by the thief such as accessing organization secrets to motivate his own personal business or market decisions. This type of attack is mostly used for blackmailing.

4.2 Modification

Modifications of data or information can be gained by using different ways or techniques. When we think about the modification attacks then we consider a modifier modifying emails messages with malicious content or modifying the numbers in an electronic bank transfer.

4.3 Masquerading

This term refers to an attacking network device impersonating a valid device. It is a perfect approach in which attacker tries to remain undetected. If the device can easily and successfully fool the target network into validating it as a registered or authorized device then the masquerader gains the entire access rights that a registered or authorized device recognized during logon, moreover there will be no security and protection warnings.

4.4 DOS (denial of service)

DOS attacks are almost different from the other three categories with respect to their techniques and objectives, other three categories expand extra concession to the attacker, usually a dos attack blocks out every person including attacker itself. The main objective of dos attacks is to cause destruction to the target by preventing functioning of the network.

5. Network Security & Security Mechanisms

It is a security policy that explains what persons can and can’t do with network components and resources.

5.1 Cryptographic authentication

This type of authentication can provide a complete secure and defense against active attacks.

5.2 Public key techniques

These techniques are mostly utilized for source authentication, to authenticate persons and devices. These techniques ensure that communication between the groups secure and with the valid party. These prevent man-in-the-middle and rewrite attacks. Information or data is often authenticated with a hashed message authentication code to maintain the data integrity security and protection.

5.3 Hybrid cryptosystems

Such systems that link different cryptographic strategies are known as Hybrid cryptosystems.

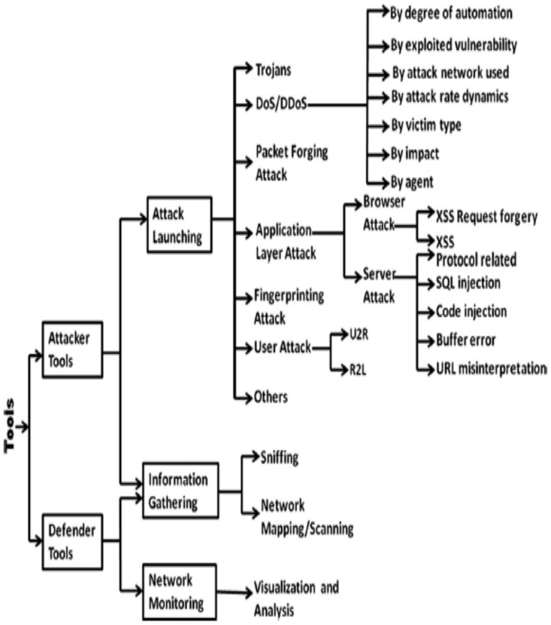

Figure 1: Taxonomy of Security Tools

6. Need for Network Security

6.1 In the past zones, attackers were efficiently skilled and trained programmers and coders who understood the computer communication details and how to take advantage of threats and vulnerabilities.

6.2 These days every person can become a hacker by downloading tools from the internet. Generally, these complex attack tools and open networks have produced an enhanced need for network security and vibrant security policies.

6.3 The easy method of providing protection to a network from an outer threat is to close it off fully from this outside world.

6.4 Only trusted known parties and websites are provided connectivity. A connection is not allowed by the closed network to public networks. This causes enhanced internet security and safety from threats.

6.5 But the problem is that internal attacks still exist.

7. Attack Detection & Detection Techniques

- ✓ Really it is possible to detect an active attack on network but it is very tough to recognize an attacker.
- ✓ Simply it is not possible to maintain a passionate attacker out of your network.
- ✓ Suddenly, this challenge cause a quick shifting to network attack detection, finding attacker before destruction or theft can occur.
- ✓ To search an active attacker needs behavioral profiling of all users and devices working on the internet. Having knowledge that what is relevant, good and useful for your network systems can help you to find an attacker or malicious activities.

7.1 Monitoring

It is also an attack detection technique. It is a common attack detection technique in the hostile environment. The purpose of monitoring based detection mechanisms in open MAS is to detect the misbehaving nodes to find the system anomalies; in **[10]** a complete article on Detecting Misbehaving nodes has been presented.

7.2 Information monitoring

Monitoring printed information in agent communications and maintaining the path of transmitted messages smooth the progress of detection of some attacks that are information centered for example active probing and ontology attacks.

7.3 Activity monitoring

This type of approach is same like the concept of activity profiling to detect the denial of service attacks in computer network literature. Calculation of the average traffic rate for the whole communication between two nodes is the basis for activity monitoring.

7.4 Attack modeling

Modeling attacks or attackers is an efficient approach to detect the attacks on MASs. You can find many informal/formal attacker modeling strategies for achieving many purposes in security literature.

7.5 Security modeling

Generally, security modeling is an approach that is used to analyze various aspects of security such as confidentiality and integrity of a system.

7.6 Anomaly detection approach

In this type of approach, patterns of data that do not obey the expected behavior and manners are detected. Statistical or clustering and classification approaches are the best example of anomaly detection technique that can be accomplished in the detection of attacks in open MAS. Anomalies or threats are detected by monitoring the current MAS state differs from the trained classifier model.

7.7 Intrusion Detection techniques

This detection technique is widely used to detect the intruder or an attack that cause malicious activities in the systems. It is very necessary and important that the security mechanisms of any system are designed and planned to avoid and prevent unauthorized access to system resources and information, in **[7] [14] [15] [16] [17]** complete surveys on Intrusion Detection have been presented.

7.8 Malware detection techniques

Malware is a worldwide contagion, research studies suggests that the effect of malware is getting worse and severe. Against malware detection, detectors are the best tools. Quality of detectors is always determined by the techniques which we use. Malware detector is the accomplishment of some malware detection techniques. In **[21] [24]** complete survey on Malware Detection Techniques have been presented.

7.9 Following activities may be considered as signs of Network Brutality by active attacks

- ✓ Unexpressed low performance of system.
- ✓ Occurrences of system crashes.
- ✓ High activity on an earlier low utilized. account or new user profiles or accounts.
- ✓ New files such as with novel or strange files for example data.xx or k .xx.
- ✓ Secrets discrepancies.
- ✓ Modifications in the names of files or date modifications.
- ✓ Unauthorized tries to write the system.
- ✓ Files disappearance like deletion of files.
- ✓ Data or information substitution or changes.
- ✓ Unexplained beeps and anomalies.
- ✓ Denial of services.
- ✓ Multiple unsuccessful logon attempting from another point.
- ✓ Suspicious activities.
- ✓ Suspicious browsing.

8. Proposed Model for Detection of Active Attacks & Methodology

The methodology providing a brief description in detail how the study was conducted including dependence of volume of data traffic on the kinds of active attacks, efficiency and effectiveness of methods of packet filtering and detection. Attacks can effectively and efficiently distich themselves by the distribution of basic communication path in to many virtual paths, that will permit to make other network interfaces in the situation of crush of the channel. Firewalls are sensible to strengthen the network systems and regulate so that private network services unavailable to public organizations. It is very useful to analyze network traffic; value of its parameters permits the identification of initialization of attacks, timely. Initialization of threats bots progressively causes increment in the flow of packets on firewall. So, a regular observation over the firewall connected to external networks is very necessary. The effectiveness of my proposed detection and protection method directly depends on packet filtering firewall that is connected among a private network, public network and directly to internet, handling and filtering information by using the rule set, constraints and a policy. This packet filtering will decrease the chances of hitting against the networks active attacks to increase the protection and defense of transmission. Several malicious activities cause destructions in the functioning of networks systems. To protect the networks from these destructions and malfunctioning, packet filtering technique is used against the threats in this model. This proposed detection method is the combination of three main phases: As shown in the following Figure 2;

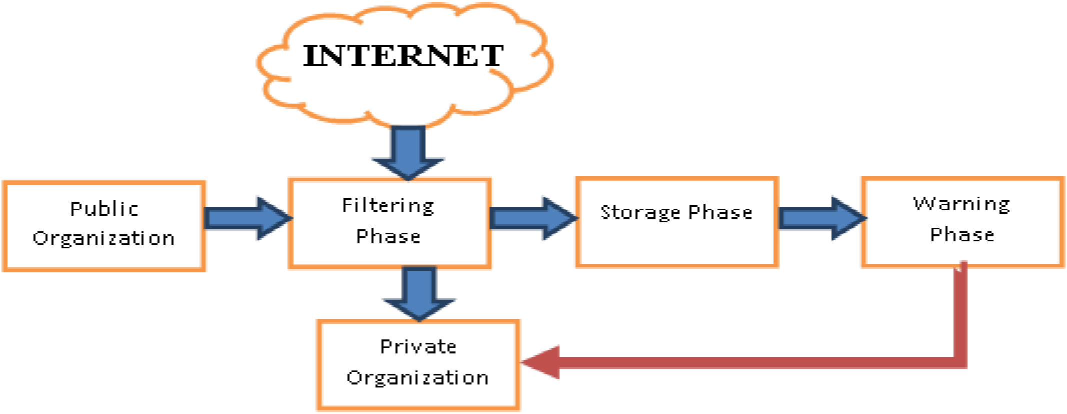

Figure 2: Proposed Active attack detection Model based on Three Main Phases

(A) Filtering Phase (B) Storage Phase (C) Warning Phase

The main purpose of using a firewall in this proposed detection model is to make sure threat less transmission and detection of malicious IP's, data containing vulnerabilities and attacks to maintain the privacy and security of network systems. In this model volume of traffic over the network is controlled by using packet filtering that will cause decrease in the volume of active attacks and other vulnerable activities.

Firewall is used in packet **Filtering Phase**; its behavior is controlled by policy. The policy is consisted of specific rules; these rules in the context of packet filtering can be called as "Filters", while rules are consisting of some specific conditions and actions. Conditions are the criteria for matching data packets individually while actions are the activities after matching the criteria developed for checking the conditions. The main conditions contain tests, matching packets individually such as source address, packet type etc.

This model is using a multi-trigger firewall that will control the volume of transmission over the network system, as all the rules will be matched for a data packet then an action will be taken. It is also using a knowledge based rule set as it is clarifying from which source addresses are data packets to this destination are allowed? Or what conditions allow data packets from this network? Or what are the total allowed data traffic from source address=A to destination address=Z? Or it may be "will a traffic flow with a source address=A, destination address=Z, protocol= UDP, port=80 be allowed? IP address may be as 192.168.1.J where "J" may be {0, 1, 2, 3} while source port and destination port are integer numbers in the range {0……65535} which is showing source and destination ports if protocol = {TCP, UDP}, in **[20]** a detection systems for security is discussed which is protected by a Firewall.

So, the main purpose of **Filtering Phase** is to filter data on the basis of rule set and take decision if they are allowed or not allowed. If data packets matches the criteria allow and pass, if they don't match with criteria not allow and pass them to **Storage Phase**. In the second phase, the not allowed data packets will be stored or saved, not pass to the private network system but to the third phase which is "**Warning Phase**". The last warning phase will alarm the main service to block the specific not allowed data packets, which may contain malicious codes, vulnerabilities and threats for the system. This proposed detection technique is using a mathematical model and filtering algorithm. It is measurement to determine the parameters regulating the amounts of packets transmitted on communication channel and total amount of data packets transmitted during the connection establishment of firewall.

8.1 Mathematical Model for Proposed Detection Model

Total volume of traffic is:

❑ Total volume of Traffic is

$$V_{td} = \frac{P_f}{T_{td}} \tag{1}$$

Where,

P_f = Total traffic of data packets, and

$$P_f = P_{fi} + P_{fo} \tag{2}$$

P_{fi} = Ingoing Traffic, P_{fo} = Outgoing Traffic

T_{td} = Total time of traffic

❑ While, Total volume of data traffic transmission allowed over the network system is

Total Volume of transmission allowed is=

$$V_t = \frac{P_{ft}}{T_{tr}} \tag{3}$$

Where,

P_{ft}= transmitted data packets or flow of transmission over the network

P_{ft}= P_{fti}+ P_{fto}

P_{fti}= Ingoing flow of transmission,

P_{fto} = Outgoing flow of transmission

T_{tr}= Time for flow of transmission over the network

8.2 Filtering Algorithm for Proposed Detection Model

```
Procedure Packet Filtering ($P_f$ :{$P_{fi}$ + $P_{fo}$}: Total Traffic over the Network)
$P_{fi}$ := In_$P_f${incoming Traffic}
$P_{fo}$ :=On_$P_f${Outgoing Traffic}
    While
$P_{fti}$:= In_$P_{ft}$
{Incoming Transmission allowed}
$P_{fto}$ := Ou_$P_{ft}$
{Outgoing Transmission allowed}
$P_{ft}$:= $P_{fti}$+ $P_{fto}$
{Total Transmission Allowed}
$P_{fbi}$:= In_$P_{fb}$
{Incoming Transmission Blocked}
$P_{fbo}$:= Ou_$P_{fb}$
{Outgoing Transmission Blocked}
$P_{fb}$:= $P_{fbi}$+ $P_{fbo}$
{Total Transmission Blocked}
    $P_f$ := $P_{ft}$ + $P_{fb}$
{Total Traffic over Firewall}
        Begin
If $P_f$ match Firewall ruleset "R" = {$r_1$,$r_2$,$r_3$,$r_4$}  then $P_f$ := "Allow"
    else $P_f$ := "DisAllow"
    end
    If $P_f$ := "Allow" then Action := "pass  to network as $P_{ft}$"
    If $P_f$ := "DisAllow" then Action := "pass to Storage Phase as $P_{fb}$ for blockage"
```

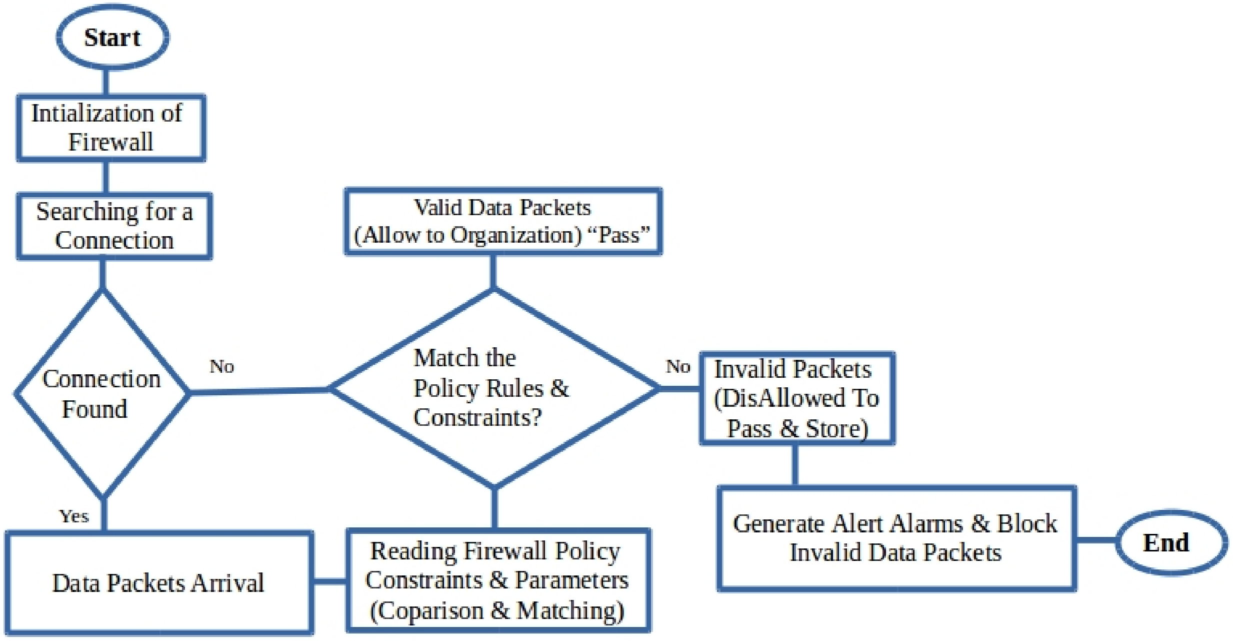
Start
Intialization of Firewall
Searching for a Connection
Connection Found
No
Yes
Data Packets Arrival
Reading Firewall Policy Constraints & Parameters (Coparison & Matching)
Match the Policy Rules & Constraints?
Valid Data Packets (Allow to Organization) "Pass"
No
Invalid Packets (DisAllowed To Pass & Store)
Generate Alert Alarms & Block Invalid Data Packets
End

Figure 3: Flowchart for Proposed Model of Detection of Active Attacks

9. Conclusion

This research paper is showing how well a security and attacks are a great challenge for the researchers and developers in the fields of information security. We have proposed a security mechanism that is providing a quite efficient mathematical model for the detection of active attacks comprising of three main phases and a filtering algorithm. An attack detection technique was proposed for the network systems to overcome the network risks by the utilization of a packet filtering firewall. In this detection technique the firewall is utilized in the first phase that controls gain to the resources of networks through a helpful and optimistic proposed detection model that is following a packet filtering algorithm. This technique employs a mathematical model and attack detection algorithm; both are light-weighted and can be easily run on the device itself.A new technique for real-time and short-term response to attack that is utilizing a packet filtering firewall in its model as the firewalls are broadly implemented for the protection of personal networks by the utilization of packet filtering to filter out unwanted network traffic incoming and outgoing of the safe network. Confirmation and authentication of firewalls is grand challenge because of the vibrant features of their function, their design is extremely miscalculation prone, finally, these are regarded as first defense to make proposed detection technique more efficient to protect and detect the network systems against the unauthorized access, attacks and illegal activities. Data generation as a result of network traffic monitoring has a tendency to contain a high volume, dimensionality and heterogeneity that make the performance of data filtering algorithm very deplorable for the analysis. We hope that proposed prototype implementation will be given the essential approach in this direction.

References

[1] Lupu T.G, "Main types of attacks in wireless sensor networks," in WSEAS International Conference Proceeings, Timisoara, 2009.

[2] Ion Tutanescu & Emil Sofron, "Anatomy and types of attacks against computer networks," in Proceedings of the second RoEduNet International Conference, ROMANIA, 2003, pp. 265-270.

[3] Mrs.D. Shanmugapriya Dr.G.Padmavathi, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol. 4 No.1&2, pp. 1-9, Sep 2009.

[4] Isabella Mastroeni Musard Balliu, "A weakest precondition approach to active attacks analysis," in proceedings of ACM SIGPLAN Fourth Workshop on Programming Languages and Analysis for Security, New York, 2009, pp. 59-71.

[5] CH.Rajya Lakshmi G.M.Padmaja, "Analyzing the Detection of Active Attacks in Wireless Mobile Networks," International Journal of Reviews in Computing, vol. 9, pp. 34-38, April 2012.

[6] Shahriar Bijani & David Robertson, "A review of Attacks and Security Approaches in Open multi-agent systems,"

Artificial Intelligence Review, vol. 42, no. 4, pp. 607-636, December 2014.

[7] Bhushan H.Trivedi Monika Darji, "Detection of Active Attacks on Wireless IMDs Using Proxy Device and Localization Information," Springer-Verlag Berlin Heidelberg2014, pp. 353-362, 2014.

[8] Vivek Ramachandran & Sukumar Nandi, "Detecting ARP Spoofing: An Active Technique," In Information Systems Security, vol. Springer Berlin Heidelberg 2005, pp. 239-250, 2005.

[9] Tiranuch Anantvalee & Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," In Wireless Network Security, vol. Springer US, pp. 159-180, 2007.

[10] Elhadi M. Shakshuki & Terek R. Sheltami Nan Kang, "Detecting Misbehaving Nodes in MANETs," in iiWAS '10 Proceedings of 12th International Conference on Information Integration and Web-based Applications & Services, ACM New York, NY, USA, 2010, pp. 216-222.

[11] S. KoilaKonda & A. Ukil J.Sen, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," in In Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference IEEE, Kuala Lumpur, 2011, pp. 338-343.

[12] G. Bakos & R. Morris V. Berk, "Designing a Framework for active worm detection on global networks," in Information Assurance, 2003. IWIAS 2003. Proceedings. First IEEE International Workshop, Germany, 2003, pp. 13-23.

[13] Marc Dacier & Andreas Wespi Herve Debar, "Computer Networks," Towards a Taxonomy of Intrusion Detection Systems, vol. 31, no. 8, pp. 805-822, April 1999.

[14] K. Nadkarni & A. Patcha A. Mishra, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, vol. 11, no. 1, pp. 48-60, February 2004.

[15] Steven T, Vigna, Giovanni,Kemmerer & Richard A. Eckmann, "STATL:An Attack Language for state-based Intrusion Detection," Journal of Computer Security, vol. 10 no. 1,2, pp. 71-103, 2002.

[16] Aurobindo Sundaram, "An Introduction to Intrusion Detection," Published in Crossroads-Special Issue on Computer Security, vol. 2, no. 4, pp. 3-7, March 1996.

[17] Douglas S. Reeves, S. Felix Wu & Jim Yuill Xinyuan Wang, "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework," In Trusted Information, vol. 65 of the series of IFIP, pp. 369-384, 2001.

[18] Parth Trivedi & M. B. Potdar Dhruva Patel, "A brief Analysis on Detection and Avoidance Techniques of Wormhole Attack in MANET," International Journal of Computer Applications, vol. 117, May 2015.

[19] Sandeep Kumar & Eugene H. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection," Department of Computer Science , Purdue University, West Lafayette, Computer Science Technical Reports Report Number 94-071, 1994.

[20] Ray Hunt, "Internet/Intranet Firewall Security-Policy, Architecture and Transaction Services," Computer Communiications, vol. 21, no. 13, pp. 1107-1123, September 1998.

[21] Nwokedi Idika & Aditya P. Mathur, "A Survey of Malware Detection Techniques," Department of Computer Science, Purdue University, West Lafayette, 2007.

[22] Yassine Maleh & Abdellah Ezzati, "A Review of Security Attacks and Intrusion Detection Schemes in Wireless Sensor Networks," International Journal of Wireless & Mobile Networks , vol. 5, December 2013.

[23] Monowar H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya & Jugal K. Kalita N. Hoque, "Network Attacks: Taxonomy, Tools and Systems," Journal of Networks and Computer Applications, vol. 40, pp. 307-324, April 2014.

[24] Uri Kanonov, Yuval Elovici, Chanan Glezer & Yael Weiss Asaf Shabtai, "Andromaly: A behavioral Malware Detection Framework for Android devices," Journal of Intelligent Information Systems, vol. 38, no. 1, pp. 161-190, February 2012.

Sobia Aslam is currently working as a senior elementary school teacher at Govt. Girls Middle School, Layallpur, Kehror Pacca, Lodhran, Pakistan. She earned her MSCS degree in 2016 from Department of Computer Science, The Islamia University of Bahawalpur, Pakistan. Her research interests include Network Security, Information Security, Communication and Security System.

Saleem ullah is working as Assistant Professor in Khwaja Fareed University of Engineering & IT since Feb 2016. He completed his PhD degree from ChongQing University, China in 2012. He has almost 11 years of Industry experience in the field of IT. He is an active researcher in the field of Adhoc Networks, Congestion Control, and Security.

Muhammad Abubakar Siddique received his B. Sc degree in Computer Science and Master in Information Technology (MIT) degree from Bahauddin Zakariya University, Multan-Pakistan in 2003 and 2005. He completed his Ph.D degree from College of Computer Science, Chongqing University, China in 2015. Currently, he is working as Assistant Professor in Khwaja Fareed University of Engineering & IT. His research interests include video mining and pattern recognition.

Abdul Sattar is working as a Lecturer in Khwaja Fareed University of Engineering & IT since Jan 2017. He completed his MS(CS) degree from Bahauddin Zakariya University, Pakistan in 2012. He has almost 7 years of working experience in the field of IT.