Global Journal of Computer and Internet Security

Volume No. 12

Issue No. 1

January - April 2024

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

Global Journal of Computer and Internet Security

Aims and Scope

The Journal of Computer and Internet Security presents research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems. It also provides a forum for ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community.

Global Journal of Computer and Internet Security

(Volume No. 12, Issue No. 1, Jan - Apr 2024)

Contents

A Review on Types of Attacks in MANET

[1]Asma Khatoon & [2]Nida Afreen

M. Tech. Scholar, Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Al-Falah University Dhauj,
Faridabad, Haryana, India.
E-mail:nida.afreen10@gmail.com

ABSTRACT

Mobile Ad-hoc network (MANET), a recent type of Ad-hoc Network has increase the awareness of today's research. MANET has no clear line of defence, so, it is accessible to equally legal network users and malicious attackers. In the existence of malicious nodes, one of the main challenges in MANET is to design the strong security solution that can protect MANET from various routing attacks. Many forms of attacks against MANET have come into sight recently that attempt to compromise the security of such networks. Such security attacks on MANET may lead to catastrophic results such as the loss of lives or loss of revenue for those value—added services. In this paper, we examine some of the main types of attacks that can be exploited in MANET.

Keywords: Mobile ad hoc network, routing protocols, wireless network.

I. INTRODUCTION

In literature we study, that with fast growth of wireless technology, the Mobile Ad-hoc Network (MANET) has come out as a new type of wireless network.[3].MANETs are new type of networks which are likely to carry a large gamut of mobile spread applications. A mobile ad-hoc network is a group of mobile nodes or routers linked with an automatic system. MANET is type of wireless network so it uses the wireless links. The combination of this structure makes the random graph having vertices and links. Here node can freely moves anywhere in the network so it also change the location of node in graph [2]. This is a major cause by which the network can use without pre analysis [4]. It is also called the ad-network. Due to its Dynamic topology property MANET has various applications such as military area, rescue operations, natural disaster recovery etc. apart from that it can also install in the office, home or a small area of city [5]. MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive computing environments [1].

A MANET is a most capable and rapidly increasing technology which is based on a self-organized and rapidly set up network. Due to its great characteristics, MANET attracts different real world application areas where the networks topology changes very quickly [6]. However, in [7,8] many researchers are trying to eliminate main limitation of MANET such as limited bandwidth, battery power, computational power, and security. Even though a lot of work under progress in this subject particularly routing attacks and its existing counter measures[6]. The existing safety solutions of wired networks cannot be apply directly to MANET, which makes a MANET much more vulnerable to security attacks[6]. In this paper, we have discussed current routing attacks in MANET. Some solutions that rely on cryptography and key management seem capable, but they are too costly for resource constrained in MANET. They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions in [7, 8, 9] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol [6]. The malicious node(s) can attacks in MANET using different ways, such as distributing fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following section, current types of routing attacks in MANET protocols are discussed in details.

This paper is divided into four section the first part gives the introduction, in second part types of attack, third conclusion and last future work.

II. TYPES OF ATTACKS

A. Passive Attacks

A passive attack obtain data exchanged in the network without disrupting the operation of the communications.. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (Dos), and message replay[2].

B. Active Attacks

An active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Active attacks involve some modification of data stream or creation of false stream [2]. Active attacks can be internal or external.

- External attacks are carried out by nodes that do not belong to the network.
- Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication [6].

ACTIVE ATTACKS

Black hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. [10] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packet that it receive instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol [2].

Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole [2] .In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network [6].

Byzantine attack

A compromised with set of intermediate, or intermediate nodes that working alone within network carry out attacks such as creating routing loops ,forwarding packets through non -optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network[6].

Rushing attack

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunnelled packets can propagate faster than those through a normal multi-hop route [6]. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [11].

Replay attack

An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [8].

Location disclosure attack

An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [13], or with simpler probing and monitoring approaches [14]. Adversaries try to figure out the identities of communication parties and analyse traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security [6].

Flooding

Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on ad hoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage cost [6].

Sinkhole

In a sinkhole attack, a compromised node tries to attract the data to itself from all neighbouring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighbouring nodes. Sinkhole attacks can also be implemented on Ad hoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate [6].

Spoofing Attack

In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node[6].

RERR Generation

Malicious nodes can prevent communications between any two nodes by sending RERR messages to some node along the path. The RERR messages when flooded into the network, may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures[6].

Jamming

In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered[6].

Replay Attack

The attacker collects data as well as routing packets and replays them at a later moment in time. This can result in a falsely detected network topology or help to impersonate a different node identity. It can be used to gain access to data which was demanded by replayed packet[6].

Sybil attack

The Sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information [6]

Sinkhole attack

The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack [6]

DE synchronization attack

In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in network in an end-less synchronization-recovery protocol[6].

Overwhelm attack

In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy[6].

Blackmail

A black mail attack is relevant against routing protocols that uses mechanisms for identification of malicious nodes and propagate messages that try to blacklist the offender[6].

Denial of service attack

Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network[6].

Gray-hole attack

This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability[6].

Selfish Nodes

In this a node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power.

Man-in-the-middle attack

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Fabrication

The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbour can no longer be contacted [12].

Impersonation

Impersonation attacks are launched by using other node's identity, such as IP or MAC address. Impersonation attacks are sometimes are the first step for most attacks, and are used to launch further ,more sophisticated attacks[6].

PASSIVE ATTACKS

Traffic Monitoring

It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities[6].

Eavesdropping

The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network[6].

Traffic Analysis

Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed[6].

Sync flooding

This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes[6].

III. CONCLUSION

Security solution is important issue for MANET, especially for those selecting-sensitive applications, have to meet the following design goals while addressing the above challenges[1].

Availability: ensures the survivability of the network services despite Denial of Service (DoS) attacks. A DoS attack could be launched at any layer of ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. The security service is highly available on the network layer at anytime and at anywhere. On the higher layers, an adversary could bring down high-level services[1].

Efficiency: the solution should be efficient in terms of communication overhead, energy consumption and computationally affordable by a portable device[1].

Authentication: enables a mobile node to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes[1].

Integrity: guarantees that a message being transmitted is never corrupted. A message could be corrupted because of being failures, such as radio propagation impairment, or because of malicious attacks on the network.

Confidentiality: ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality[1].

Non-repudiation: ensures that the original message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised mobile nodes[1].

After the analysis it appear that there are so many attacks are available in order to do the malicious activity in the mobile ad-hoc network. Some of these problems has sort out by many researchers. This paper gives concise on the different types attacks in MANET in order to check from these attacks we should make our network more secure we need to implement different types of security breaches in our MANET.

IV. FUTURE WORK

In future we will provide the details of each attack and also give them preventing method for each attacks

REFERENCES

[1]. A Review of Current Routing Attacks in Mobile Ad Hoc Networks, Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, International Journal of Computer Science and Security, volume (2) issue (3), Malasia.

[2]. A Review: Attacks and Its Solution over Mobile Ad-Hoc Network, Ankit Mehto, Hitesh Gupta, International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013

[3]. I. Khalil, S. Bagchi, N.B. shroft "LiteWorp: Detection and isolation of the wormhole in static mulihop wirelessnetwork. Journal," Acm: The international Journal of Computer and Telecommunications Networking Archive,Vol. 51, Issue 13, September 2007.

[4]. H. Vu, A. Kulkarni, N. Mittal, "WOMEROS: A new framework for defending against wormhole attacks on wireless ad hoc networks," in W ASA 2008, LNCS 5258, pp. 491-502, 2008

[5]. Y. C. Hu, A. Perrig, and D. B. Johnson," Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp.370-380, 2006.

[6]. A Literature Review of Security Attack in Mobile Ad-hoc Networks, Prinyanka Goel, Sahi Batra, Ajit Singh, http://ijcaonline.org/ Volume 9– No.12, November 2010

[7]. Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005

[8]. S. Kurosawa et al., "Detecting Blackhole Attack on AODV Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[9]. M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

10]. Jyoti Raju and J.J. Garcia-Luna-Aceves, " A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless networks'," in Proceeding of IEEE ICC, June 2000

[11]. C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999

[12]. M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10

[13]. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2000

[14]. C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999

Analysis of Warm-Hole Attack in Mobile Ad hoc Network (MANET)

[1]Nida Afreen & [2]Asma Khatoon

M. Tech. Scholar, Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Al-Falah University Dhauj,
Faridabad, Haryana, India.
E-mail:nida.afreen10@gmail.com

ABSTRACT

Mobile Ad-hoc network (MANET), a latest form of Ad-hoc Network has gained the attention oftoday's research efforts and automotive industries to improve road safety and enable a wide variety of value added services. It needs security to implement the wireless environment and serves users with safety and non safety applications. Many forms of attacks against MANET have emerged recently that attempt to compromise the security of such networks. Such security attacks on MANET may lead to catastrophic results such as the loss of lives or loss of revenue for those value—added services. In this paper, we discuss some of the main security threats that can be exploited in MANET and present the corresponding security solutions that can be implemented to thwart those attacks.

Keywords: MANET, Ad-hoc network, Security, attacks.

I. INTRODUCTION

With rapid development of wireless technology, the Mobile Ad-hoc Network (MANET) has emerged as a new type of wireless network. The world today is living a combat, and the battle field lies on the roads, the estimated number of deaths is about 1.2 million people yearly worldwide [1].MANETs are new type of networks which are expected to support a large spectrum of mobile distributed applications. A mobile ad-hoc network is a collection of mobile nodes or routers connected with an automatic system. There nodes does not user any wired media as a link. MANET is type of wireless network so it uses the wireless links. The combination of this structure makes the random graph having vertices and links. Here node can freely moves anywhere in the network so it also change the location of node in graph. This is a major cause by which the network can use without pre analysis [2]. It is also called the ad-network. Due to its Dynamic topology property MANET has various applications such as military area, rescue operations, natural disaster recovery etc. apart from that it can also install in the office, home or a small area of city [3].

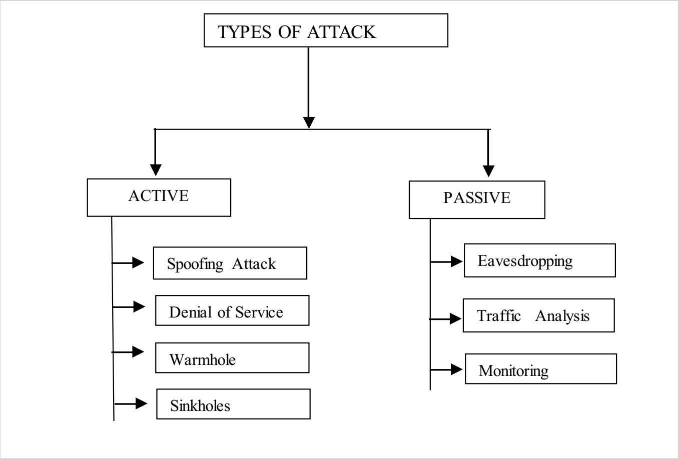
II. EXTERNAL VS INTERNAL ATTACKS

The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Nodes that do not belong to the domain of the network carry out external attacks. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more harmful when compared with outside attacks since the insider knows valuable and secret information, and possesses confidential access rights

III. ACTIVE VS PASSIVE ATTACK

The attacks in MANET can generally be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring.

Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.



IV. WORMHOLE ATTACK

Mobile ad hoc network [4] is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is prepared with a wireless transmitter and receiver, which allow it to communicate with other nodes in its range. In order for a node to forward a packet to a node that is out of its radio range, the support of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology normally changes due to the mobility of mobile nodes in the network.

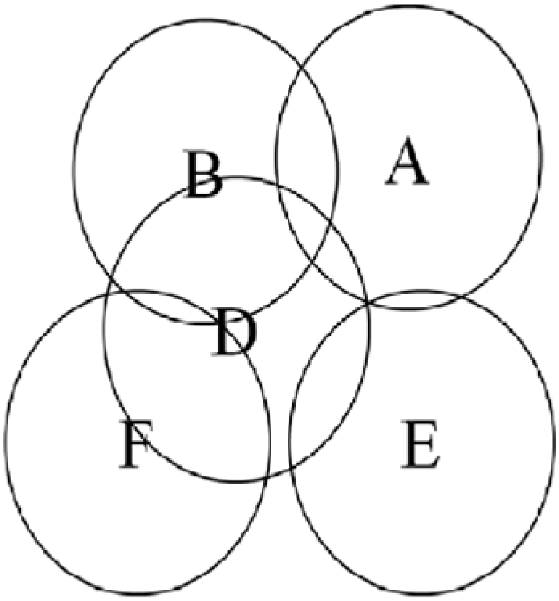


Figure 1 Mobile Ad-hoc Network

In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network. Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and due to this reason this attack is serious. We can use 4 steps to explain about a general wormhole attack [5, 7].

1. An attacker has two trusted nodes in two different locations of a network with a direct link between the two nodes.
2. The attacker records packets at one location of a network.
3. The attacker then tunnels the recorded packets to a different location.
4. The attacker re-transmits those packets back into the network location from step 1.

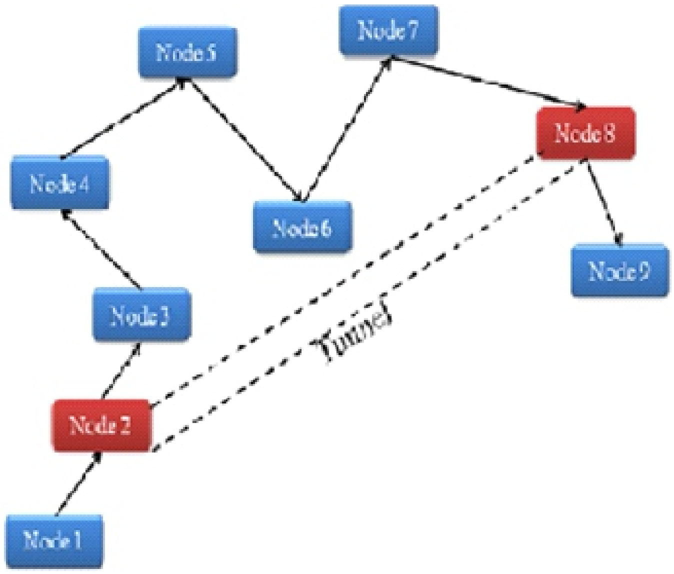


Figure 2 shows the simple worm hole in the network. Here node 2 and node 8 create the tunnel in order to work as a malicious node. Both nodes give the illusion to another node that there is a shortest path. But this shortest path does not exist and attack can easily perform by the attacker. There are three types of wormhole attacks are available [6]. There are classified on the basis of its Nodes. There are open wormhole attack, half open wormhole attack and closed wormhole.

A. *Open Wormhole Attack:* In this type of attack both nodes are available in the network in order to complete the communication in the network. Here both nodes can change the data as well as show them self in route discovery path.

B. *Half Open Wormhole Attack:* In this type of attack one node is open in network in order to spoil the integrity of data.

C. *Closed Wormhole Attack:* When the tunnel has formed then both node hide then self from the network but act for modifying the data. They show that the shortest path to the send the data

V. WORMHOLE DETECTION TECHNIQUES

This section presents some previous work related to detection of wormhole in mobile ad-hoc network. There are four basic methodologies or solutions to detect the wormhole [7].

Graph based: In this types of techniques the whole network is considered as the graph. So, it is possible to apply the rules related to graph theory. As far as detection is concert we need to calculate the some parameters to find the wormhole.

Statical based: This type of detection is based on mathematical data or statistics. Hope count is very popular approach of Statical based detection. In such technique we assume some pre-decided hope count then take design against the wormhole.

Location based: In this Approach the location of nodes plays an important role. In this type of methods geographical leash used. It has the address with location. Here we also has to focus on the distance between nodes with respect to transmission range.

Time based: This type of methodology work with temporal approach. Here we fix the time in order to exist the packet into the network.

VI. SECURITY THREATS

The wireless Channel is accessible to both legitimate network users and malicious attackers [11]. There is no well defined place where traffic monitoring or access control mechanism scan be deployed so the boundary that separates the inside network from the outside world becomes blurred.

- The existing ADHOC routing protocols such as ADHOC on Demand distance vector (**ADDV**), Dynamic Source Routing (**DSR**), Wireless MAC protocols such as **(802.11)**do not provide a trusted environment so a malicious attacker can readily become a router and disrupt network operations by disobeying the protocol specifications.
- The attacker may advertise a route with a smaller distance metric than the actual distance to the destination.
- By attacking routing protocol the attacker can attract traffic towards certain destination in the nodes under their control and cause the packet to be forwarded along a route that is not optional
- The attacker can create routing loops in the network and introduce severe network congestion and channel contention in certain areas.
- Many colluding attracters may even prevent a source node from finding any route to the destination and partition the Network.
- The attacker may further subvert existing nodes in the network or fabricate its identity and impersonate.
- A pair of attacker nodes may create a wormhole and shortcut the normal flows between each other
- The attacker may target the route maintenance process and advertise that an operational link is broken.
- One more problem is the attacker along an established route may drop the packet, modify the content of packet or duplicates the packets it has already forwarded.
- Denial of service: Attack via network layer packet blasting ,in which the attacker injects a large amount of junk packets in to the network, these packets waste a significant portion of the network resources and introduce severe wireless channel contention and network congestion in MANET .The wireless Channel is a band width constraints and also shared among multiple networking entities. The computational capacity of the mobile node is also a constrained. Because mobile devices have very limited energy sources. The main issue for MANET is to maintain proper security and no compromise with the network performance.

VII. MANET'S SECURITY SERVICES

A MANET is a network consisting of a collection of nodes capable of communicating with each other without help from infrastructure of the network [11]. There are mainly five security services:

Authentication: Correct identity is known to the communicating partner.

Confidentiality: Message information is kept secure from unauthorized party.

Integrity : Message is unaltered during communication.

Non Repudiation: The origin of the message cannot deny having sent the message.

Availability: The normal service provision in face of all kind of attacks. Security means the security mechanism for all protocols involved in this (MANET) service to protect the basic function of MANET means security during bit transfer from one node to another.

VIII. RELATED WORK

There are lots of work has been proposed in order to detect the wormhole in the mobile ad-hoc network.

Here we have discussed some of them. In paper [8] author has proposed the wormhole detection technique which is worked on the properties of signal processing and improves and extends the frequency-based wormhole attack detection mechanism. The proposed Technique detects wormhole attacks through analysing the FFT magnitude spectrum patterns of the timing data collected in the MAC layer at the destination node.

This paper [9] gives the introduction the wormhole attack and an approach to stop and detect this attack.

The author suggested some changes in AODV protocol to avoid the malicious activity. By changingin AODV protocol it is possible to disable the malicious node. It will reduce the cost also. In this method [10] author proposed new approach using digital signature for detecting the wormhole. Author said that if sending node's digital signature verified at receiving node than it will help to detect the wormhole. Here first of all we need to create a secure path between sender and receiver with the help of verification of digital signature by which malicious node will unable to attack in the network.

VII. CONCLUSION

- After this study it seems to be that there are so many attacks are available in order to do the malicious activity in the mobile ad-hoc network. Some of these problems has sort out by many researchers. This paper throws some light on the various attacks in MANET and some methodology in order to prevent these attacks from spoiling the integrity of data

REFERENCES

[1].Khalil, S. Bagchi, N.B. shroft "Lite Worp: Detection and isolation of the wormhole in static mulihop wireless network. Journal," Acm: The international Journal of Computer and Telecommunications Networking Archive, Vol. 51, Issue 13, September 2007.

[2].H. Vu, A. Kulkarni, N. Mittal, "WOMEROS: A new framework for defending against wormhole attacks on wireless ad hoc networks," in W ASA 2008, LNCS 5258,pp. 491-502, 2008.

[3].Y. C. Hu, A. Perrig, and D. B. Johnson," Wormhole Attack in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp.370-380, 2006.

[4].Manikandan K.P.; Satya prasad R.; Rajasekhararao. Analysis and Diminution of Security Attacks on Mobile Ad hoc Network. IJCA Special Issue on MANETs, 2010.

[5].N. Song, L. Qian, and X. Li. "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach", ipdps, p. 289a, 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17, 2005.

[6].W. Wang, B. Bhargava, Y. Lu, and X. Wu, Defending against Wormhole Attacks in Mobile Ad Hoc Networks, Journal of Wireless Communication and Mobile Computing (WCMC), vol.6, no.4, pp.483-503, Wiley Inter Science, June, 2006

[7].Sebastian Terence J, "Secure Route Discovery against Wormhole Attacks in Sensor Networks using Mobile Agents", IEEE 2011, pp 110-115.

[8].Ronggong, Song Peter and C. Mason Ming Li "Enhancement of Frequency-based Wormhole Attack Detection", IEEE 2011, pp 1139-1145.

[9].Mariannne. A. Azer, "Wormhole Attacks Mitigation", IEEE 2011, pp 561-568.

[10].Pallavi Sharma and Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", IEEE 2011, pp

[11].A Review of 'MANET's Security Aspects and Challenges, Pradeep Rai Shubha singh, *IJCA Special Issue on "Mobile Ad-hoc Networks "MANETs, 2010*

Effective Regression Testing Technique is use to Reducing the Residual Defects

Mohd. Muneer Siddiqui
M. Tech scholar, Computer Science and Engineering
Al-Falah School of Engineering and Technology. Dhouj, Faridabad, Haryana

ABSTRACT

The principle of regression testing is to make sure that changes made to software, such as adding new features or modifying existing features, have not adversely affected features of the software that should not change. Many techniques have been reported on how to select regression tests so that the number of test cases does not grow too large as the software evolves. Our technique combines modification, minimization and prioritization-based selection using a list of source code changes and the execution traces from test cases run on previous versions. One important issue associated with a system lifetime view that we have overlooked in past years is the effects of residual defects (persist undetected) across several releases of a system. Depending on an organization's business goals and the type of system being built, residual defects might affect the level of success of the software products. In this paper, we conducted an empirical study to investigate whether Regression Testing Technique are effective in reducing the persistence of residual defects across a system's lifetime considering test case prioritization techniques.

Regression testing is a testing activity that is performed to provide that changes do not harm the existing behavior of the software. A number of deferent approaches have been studied to maximize the value of the accrued test suite: minimization, selection and prioritization. Test suite minimization seeks to eliminate redundant test cases in order to reduce the number of tests to run. Test case selection seeks to identify the test cases that are relevant to some set of recent changes. Test case prioritization seeks to order test cases in such a way that early fault detection is maximized. This paper surveys each area of minimization, selection and prioritization technique and discusses open problems and potential directions for future research.

Keywords: Regression Testing, Modification-Based Test Selection, Test Set Minimization, test case prioritization, residual defects.

1. INTRODUCTION

Regression Testing is a well recognized practice in the software industry. Many techniques have been proposed to perform cost-effective regression testing. However, one type of defect was not being studied experts in this field. That defect type is residual defects - those that have existed through several releases undetected. This paper looks to study the effectiveness of using regression testing to find this type of defect.

The paper states that residual defects could make about 22% of the total defects within a piece of software. The cost of fixing residual defects grows with program complexity.

It is a complex procedure that is all the more challenging because of some of the recent trends in software development paradigms.

For example, the component-based software development method tends to result in use of many black-box components, often adopted from a third-party. Any change in the third-party components may interfere with the rest of the software system, yet it is hard to perform regression testing because the internals of the third-party components are not known to their users.

The shorter life-cycle of software development, such as the one suggested by the agile programming discipline, also imposes restrictions and constraints on how regression testing can be performed within limited resources.

Naturally, the most straightforward approach to this problem is to simply execute all the existing test cases in the test suite; this is called a retest-all approach. However, as software evolves, the test suite tends to grow, which means it may be prohibitively expensive to execute the entire test suite.

Testers might rerun all test cases generated at earlier stages to ensure that the program behaves as expected. However, as a program evolves the regression test set grows larger, old tests are rarely discarded, and the expense of regression testing grows. Repeating all previous test cases in regression testing after each minor software revision or patch is often impossible due to the pressure of time and budget constraints. On the other hand, for software revalidation, arbitrarily omitting test cases used in r egression testing is risky. In this paper, we investigate methods to select small subsets of effective fault-revealing regression test cases to revalidate software.

In this paper, we first select tests from the regression testing that execute any of the modifications in the old program. Third section includes case studies.

2. REGRESSION TESTING

Regression testing is performed between two deferent versions of software in order to provide confidence that the newly introduced features of the System under Test (SUT) do not interfere with the existing features. While the exact details of the modifications made to SUT will often be available, they may not be easily available in some cases. For example, when the new version is written in a different programming language or when the source code is unavailable, modification data will be unavailable.

The following notations are used to describe concepts in the context of regression testing. Let P be the current version of the program under test, and P0 be the next version of P. Let S be the current set of specifications for P, and S0 be the set of specifications for P0. T is the existing test suite. Individual test cases will be denoted by lower case: t. P(t) stands for the execution of P using t as input.

2.1. Test Case Prioritization

Test case prioritization approaches that are used to execute the regression testing in a cost-effective manner were investigated. We discussed the critical issues and best practices that a software company should focus on before and after the implementation of test case prioritization techniques inside the company. Due to the increasing complexity of today's software intensive systems, the number of test cases in a software development project increases for an effective validation & verification process and the time allocated to execute the regression tests decreases because of the marketing pressures. For this reason, it is very crucial to plan and setup test case prioritization infrastructures properly in software companies to improve the software testing process. Ten best practices for a successful test case prioritization are introduced and explained in this study.

2.2. Regression Test Suite

A regression test suite of 1000 distinct tests was created based on the operational profile of how the space program was used. An operational profile, as formalized by Musa and used in our experiment, is a set of the occurrence probabilities of various software functions. To obtain an operational profile for space we identified the possible functions of the program and generated a graph capturing the connectivity of these functions. Each node in the graph represented a function. Two nodes, A and B, were connected if control could flow from function A to function

2.3. Economic model for Regression Testing

Software engineering methodologies are subject to complex cost-benefit tradeoffs. Economic models can help practitioners and researchers assess methodologies relative to these tradeoffs. Effective economic models, however, can be established only through an iterative process of refinement involving analytical and empirical methods. Sensitivity analysis provides one such method. By identifying the factors that are most important to models, sensitivity analysis can help simplify those models; it can also identify factors that must be measured with care, leading to guidelines for better test strategy definition and application. In prior work we presented the first comprehensive economic model for the regression testing process, that captures both cost and benefit factors relevant to that process while supporting evaluation of these processes across entire system lifetimes. In this work we use sensitivity analysis to examine our model analytically and assess the factors that are most important to the model. Based on the results of that analysis, we propose two new models of increasing simplicity. We assess these models empirically on data obtained by using regression testing techniques on several non-trivial software systems. Our results show that one of the simplified models assesses the relationships between techniques in the same way as the full model.

3.A CASE STUDY

A case study was conducted on a space program developed for the European Space Agency.4 A modification based selection technique and the subsequent test set minimization and prioritization techniques were used to select regression tests for re execution. Three metrics, size reduction, recall and precision, were computed to measure the cost-effectiveness of these techniques. Our experiment is explained below in detail.

3.1. The Space Program

The space program provides a language-oriented user interface that allows the user to describe the configuration of an array of antennas using a high level language. Its purpose is to prepare a data file in accordance with a predefined format and characteristics from a user, given the array antenna configuration described in a language-like form.

An appropriate Array Definition Language was defined and used within the program. This language allows the user to describe a certain antenna array by a few statements instead of having to write the complete list of elements, positions and excitations. The program consists of about 10,000 lines of code divided into three subsystems, parser, computation, and formatting. Details of these subsystems can be found in their design documents.

The fault set for the space program used in this study was obtained from the error-log maintained during its testing and integration phase (see Appendix). For convenience, each fault has been numbered as Fk where the integer k denotes the fault number. This number does not indicate the order in which faults were detected.

3.2. Regression Test Suite

A regression test suite of 1000 distinct tests was created based on the operational profile of how the space program was used. An operational profile, as formalized by Musa and used in our experiment, is a set of the occurrence probabilities of various software functions. To obtain an operational profile for space we identified the possible functions of the program and generated a graph capturing the connectivity of these functions. Each node in the graph represented a function. Two nodes, A and B, were connected if control could flow from function A to function B.

There was a unique start and end node representing functions at which execution began and terminated, respectively.

A path through the graph from the start node to the end node represents one possible program execution. To estimate the occurrence probability of the software functions, each arc was assigned a transition probability, i.e., the probability of control flowing between the nodes connected by the arc.

4.TEST CASE PRIORITIZATION

Test case prioritization seeks to find the ideal ordering of test cases for testing, so that the tester obtains maximum benefit, even if the testing is prematurely halted at some arbitrary point. The approach was first mentioned by Wong et al.

However, in that work it was only applied to test cases that were already selected by a test case selection technique. Harrold and Rothermel proposed and evaluated the approach in a more general context.

4.1. Coverage-based Prioritization

Structural coverage is a metric that is often used as the prioritization criterion. The intuition behind the idea is that early maximization of structural coverage will also increase the chance of early maximization of fault detection. Therefore, while the goal of test case prioritization remains that of achieving a higher fault detection rate, prioritization techniques actually aim to maximize early coverage.

Rothermel et al. reported empirical studies of several prioritization techniques [144,145]. They applied the same algorithm with different fault detection rate surrogates. The considered surrogates were: branch-total, branch-additional, statement total, statement-additional, Fault Exposing Potential (FEP)-total, and FEP-additional.

The branch-total approach prioritizes test cases according to the number of branches covered by individual test cases, while branch-additional prioritizes test cases according to the additional number of branches covered by individual test cases.

The statement-total and statement-additional approaches apply the same idea to program statements, rather than branches.

Algorithmically, `total' approaches are essentially instances of greedy algorithms whereas `additional' approaches are essentially instances of additional greedy algorithms.

The FEP of a test case is measured using program mutation. Program mutation introduces a simple syntactic modification to the program source, producing a mutant version of the program [23]. This mutant is said to be killed by a test case if the test case reveals the deference between the original program and the mutant. Given a set of mutants, the mutation score of a test case is the ratio of mutants that are killed by the test case to the total kill-able mutants. The FEP-total approach prioritizes test cases according to the mutation score of individual test cases, while the FEP-additional approach prioritizes test cases according to the additional increase in mutation score provided by individual test cases. Note that FEP criterion can be constructed to be at least as strong as structural coverage; to kill a mutant, a test case not only needs to achieve the coverage of the location of mutation but also to execute the mutated part with a set of test inputs that can kill the mutant.

Elbaum et al. extended the empirical study of Rothermel et al. by including more programs and prioritisation surrogates.

Among the newly introduced prioritization surrogates, function-coverage and function-level FEP enabled Elbaum et al. to study the effects of granularity on prioritization. Function-coverage of a test case is calculated by counting the number of functions that the test case executes. Function-level FEP is calculated, for each function f and each test case t, by summing the ratio of mutants in f killed by t. Elbaum et al. hypothesized that approaches with coarser granularity would produce lower APFD values, which was confirmed statistically.

Jones and Harrold applied the greedy-based prioritization approach to Modified Condition / Decision Coverage (MC/DC) criterion [82]. MC/DC is a `stricter form' of branch coverage; it requires execution coverage at condition level. A condition is a Boolean expression that cannot be factored into simpler Boolean expressions. By checking each condition in decision predicates, MC/DC examines whether each condition independently affects the outcome of the decision [28]. They presented an empirical study that contained only an execution time analysis of the prioritization technique and not an evaluation based on fault detection rate.

4.2. Interaction Testing

Interaction testing is required when the SUT involves multiple combinations of different components. A common example would be configuration testing, which is required to ensure that the SUT executes correctly on different combinations of environment, such as different operating systems or hardware options. Each component that can be changed is called a factor; the number of choices for each factor is called the level of the corresponding factor. As the number of factors and levels of each factor increase, exhaustive testing of all possible combinations of factors becomes infeasible as it requires an exponentially large test suite.

Instead of testing exhaustively, pair-wise interaction testing requires only that every individual pair of interactions between different factors are included at least once in the testing process. The reduction grows larger as more factors and levels are involved. More formally, the problem of obtaining interaction testing combinations can be expressed as the problem of obtaining a covering array, CA (N; t; k; v), which is an array with N rows and k columns; v is the number of levels associated with each factor, and t is the strength of the interaction coverage (2 in the case of pair-wise interaction testing).

Bryce and Memon also applied the principles of interaction coverage to the test case prioritization of Event-Driven Software

(EDS). EDS takes sequences of events as input, changes state and outputs new event sequences. A common example would be GUI-based programs. Bryce and Memon interpreted t-way interaction coverage as sequences that contain different combinations of events over t unique GUI windows. Interaction coverage based prioritization of test suites was compared to deferent prioritization techniques such as unique event coverage (the aim is to cover as many unique events as possible, as early as possible), longest to shortest (execute the test case with the longest event sequence _rst) and shortest to longest (execute the test case with the shortest event sequence first). The empirical evaluation showed that interaction coverage based testing of EDS can be more efficient than the other techniques, provided that the original test suite contains higher interaction coverage. Note that Bryce and Memon did not try to generate additional test cases to improve interaction coverage; they only considered permutations of existing test cases.

5. CONCLUSION

Effective regression testing is a trade-off between the number of regression tests needed and the cost. In this paper, we propose a modification-based technique followed by test set minimization or prioritization to determine which regression tests should be rerun.

Three metrics, size reduction, precision, and recall, are used to examine the goodness of using (I) and (II). These metric values depend not only on the nature of the regression test suite but also the extent and the locations of the modifications.

Unlike many other proposed test selection techniques, ours is supported by a tool called ATAC.

If for reasons of safety or performance an application is not tolerant of a great deal of intrusive instrumentation, our modification-based test selection can be conducted at a higher level of granularity such as at the function or subsystem level.

On the other hand, if a high percentage of precision and recall is required, one can apply more complicated, and more expensive, techniques such as relevant slicing to construct a smaller super set, 0, of those regression tests which need to be re executed.

We can then apply test set minimization and prioritization to 0 to identify a representative subset of tests which have a higher priority to be rerun.

The bottom-line for making a decision on whether any of these alternatives should be adopted goes back to the original trade-off problem: What we should do in regression testing versus what we can afford to do. Experiments are underway to compare the cost-effectiveness of these alternatives.

The results of these studies will provide more information to help us determine how to conduct efficient and effective regression testing in practice.

REFERENCES

[1] IEEE Standard Glossary of Software Engineering Terminology. IEEE Press, 10 Dec 1990.

[2] H. Agrawal, J. R. Horgan, E. W. Krauser, and S. A. London. Incremental regression testing. In Proceedings of the International Conference on Software Maintenance (ICSM 1993), pages 348{357. IEEE Computer Society, September 1993.

[3] N. Alshahwan and M. Harman. Automated session data repair for web application regression testing. In Proceedings of 2008 International Conference on Software Testing, Veri_cation, and Validation, pages 298{307, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[4] J. H. Andrews, L. C. Briand, and Y. Labiche. Is mutation an appropriate tool for testing experiments? In Proceedings of the 27th International Conference on Software Engineering (ICSE 2005), pages 402{411. ACM Press, May 2005.

[5] R. Anido, A. R. Cavalli, L. P. Lima Jr, and N. Yevtushenko. Test suite minimization for testing in context. Software Testing, Veri_cation and Reliability, 13(3):141{155, 2003.

[6] T. Apiwattanapong, R. Santelices, P. K. Chittimalli, A. Orso, and M. J. Harrold. Matrix: Maintenance-oriented testing requirements identi_er and examiner. In Proceedings of Testing: Academic & Industrial Conference on Practice And Research Techniques, pages 137{146, Los Alamitos, CA, USA, 2006. IEEE Computer Society.

[7] T. Ball. On the limit of control ow analysis for regression test selection. In Proceedings of the International Symposium on Software Testing and Analysis (ISSTA 1998), pages 134{142. ACM Press, March 1998.

[8] S. Bates and S. Horwitz. Incremental program testing using program dependence graphs. In Proceedings of the 20th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, pages 384{396. ACM Press, January 1993.

[9] Y. Chen, D. Rosenblum, and K. Vo, "TestTube: A system for selective regression testing," in Int'l. Conf. Softw. Eng., May 1994, pp. 211-220.

[10] J. Offutt, J. Pan, and J. M. Voas, "Procedures for reducing the size of coverage-based test sets," in Proc. Int'l. Conf. Testing Comp. Softw., Jun. 1995, pp. 111-123.

[11] G. Rothermel and M. J. Harrold, "A safe, efficient regression test selection technique," ACM Trans. Softw. Eng. Meth., vol. 6, no. 2, pp. 173-210, Apr. 1997. (Pubitemid 127684922)

[12] G. Rothermel, R. Untch, C. Chu, and M. J. Harrold, "Test case prioritization," IEEE Trans. Softw. Eng., vol. 27, no. 10, pp. 929-948, Oct. 2001.

[13] A. Walcott, M. L. Soffa, G. M. Kapfhammer, and R. Roos, "Time-aware test suite prioritization," in Int'l. Symp. Softw. Test. Anal, Jul. 2006, pp. 1-12.

[14] H. Do, S. Mirarab, L. Tahvildari, and G. Rothermel, "An empirical study of the effect of time constraints on the cost-benefits of regression testing," in Proceedings of the ACM SICSOFT Symposium on Foundations of Software Engineering, Nov. 2008, pp. 71-82.

[15] S. Elbaum, A. G. Malishevsky, and G. Rothermel, "Test case prioritization: A family of empirical studies," IEEE Trans. Softw. Eng., vol. 28, no. 2, pp. 159-182, Feb. 2002.

[16] J. Kim and A. Porter, "A history-based test prioritization technique for regression testing in resource constrained environments," in Int'l. Conf. Softw. Eng., May 2002, pp. 119-129.

[17] A. Orso, N. Shi, and M. J. Harrold, "Scaling regression testing to large software systems," in Proceedings of the International Symposium on Foundations of Software Engineering, Nov. 2004.

[18] N. Fenton and S. Pfleeger, "Science and substance: A challenge to software engineers," IEEE Software, pp. 86-95, Jul. 1994.

Embedding Different XML Transformation Techniques for Developing Dynamic XSLT Document

Dr. Jitender Rai,
Associate Professor, Tecnia Institute of Advanced studies, Delhi,
Email: jitender12rai@gmail.com

ABSTRACT

In this paper we develop Extensible Style sheet Language Transformations (XSLT) architecture which can be used for many purposes to change the styles of different websites. The area of XML is very large but we optimize some problems of XML transformation using different web based programming technologies like java, HTML, C#.net, JavaScript, etc, to generate formatted HTML output, or to create an alternative XML representation of the data or develop dynamic XSLT documents. XSLT is a language used to specify the transformation of XML documents. It takes an XML document and transforms it into another XML document. The HTML conversion is simply a special case of XML transformation. And because the styling is applied automatically, it's easy to change the layout of my Web site. All that's required is a change to the style sheet. In a world of changing Web fashions, this is a major advantage.

Keywords: XML, XSLT, C#, .Net Technology, Java Technology.

1. INTRODUCTION

XML is a markup language much like HTML, a meta-language that describes the content of the document. XML was designed to describe data. XML is not a replacement for HTML [5].XML tags are not predefined. You must define your own tags. XML was designed to carry data, not to display data. XML is designed to be self-descriptive. Extensible Markup Language (XML) is a set of rules for encoding documents in machine- XSLT describes rules for transforming a source tree into a result tree. The transformation is achieved by associating patterns with templates. A pattern is matched against elements in the source tree. A template is instantiated to create part of the result tree. The result tree is separate from the source tree. The structure of the result tree can be completely different from the structure of the source tree readable form. It is defined in the XML 1.0 Specification produced by the W3C, and several other related specifications, all gratis open standards [1]. A transformation expressed in constructing the result tree, elements from the source tree can be filtered and reordered, and arbitrary structure can be added. A transformation expressed in XSLT is called a style sheet [2]. This is because, in the case when XSLT is transforming into the XSL formatting vocabulary, the transformation functions as a style sheet. This specification defines the syntax and semantics of XSLT, which is a language for transforming XML documents into other XML documents. XSLT is designed for use as part of XSL, which is a style sheet language for XML. XML and XSL help because they enable me to write the document in one format (XML) and automatically create distribution copies in text and HTML. And because the styling is applied automatically, it's easy to change the layout of my Web site. All that's required is a change to the style sheet. In a world of changing Web fashions, this is a major advantage.

1.1. RELATED WORK

The following work has done by previous author:
XSLT is influenced by functional languages, [10] and by text-based pattern matching languages like SNOBOL and awk. Its most direct predecessor is DSSSL, which did for SGML what XSLT does for XML [11].

XSLT 1.0: XSLT was part of the World Wide Web Consortium (W3C)'s Extensible Stylesheet Language (XSL) development effort of 1998–1999, a project that also produced XSL-FO and XPath. Some members of the standards committee that developed XSLT, including James Clark, the editor, had previously worked on DSSSL. XSLT 1.0 was published as a W3C recommendation in November 1999.[3]

XSLT 2.0: after an abortive attempt to create a version 1.1 in 2001,[9] the XSL working group joined forces with the XQuery working group to create XPath 2.0,[10] with a richer data model and type system based on XML Schema. The most recent version is XSLT 2.0,[11] developed under the editorship of Michael Kay. It reached recommendation status in January 2007.[13] As of 2010, however, XSLT 1.0[13] is still widely used, since 2.0 is not supported natively in web browsers or for environments like LAMP[4].

1.2. PROBLEM STATEMENTS

XML web designers organize a document by structure, so that changing a document's appearance is a simple matter of changing the definition of an element once, and letting the changes ripple through an entire file - or a huge Web site. In the future, more people will turn to specialized devices to view the Web. Already WebTV has achieved some success. Mobile phones and PDAs, such as the popular Palm Pilot, will be increasingly used for Web browsing. The way pages are displayed has to be changed for these smaller devices. One solution may be to use XHTML, an XML simplified version of HTML. XSL will make it easy to manage the diversity of browsers and platforms by maintaining the document source in XML and converting to the appropriate XHTML subset with XSLT [5].

2. PURPOSED WORK

2.1 Overview of XSLT

There are some important cases where XSLT can be a good choice ETL software can use in some cases XSLT. For example, it can be a good choice when both extracted data and data to load are in an XML format, and where transform may be changed without the need to recompile the application. Some applications which store data in XML use XSLT to present this data in a human-readable format[1]. For example, Windows Live Messenger stores the trace of messages as XML, but when you open the history in WLM itself, it shows you a pretty table which in fact is HTML built through XSLT. (3)Some developer-oriented or data-oriented websites may want to give an access to XML if the intent is to use the pages of the website programmatically[2]. It is somehow nicer than to use HTML parsers, especially since HTML code can be changed at any moment. (4)XSLT, when used in websites, allow strict separation between HTML and code-behind, which enables to hire a developer for code-behind and another developer for HTML/CSS stuff.

Will XSLT be a significant choice in future?
Well, this is not a significant choice today, and I doubt the usage of XSLT will increase over time. I ignore the reason of that, but many developers don't like XML and hate XSLT. Can you recommend new programmers to study XSLT? Sure! Not only XSLT can be used in some circumstances when other approaches would be more difficult, but also XSLT has a very specific approach that other languages don't have.

2.2 XSLT Transformation Architecture

In addition to XSLT, XSL includes an XML vocabulary for specifying formatting. XSL specifies the styling of an XML document by using XSLT to describe how the document is transformed into another XML document[6].That uses the formatting vocabulary. XSLT is also designed to be used independently of XSL The detail description of XSLT Transformation explain with step wise.

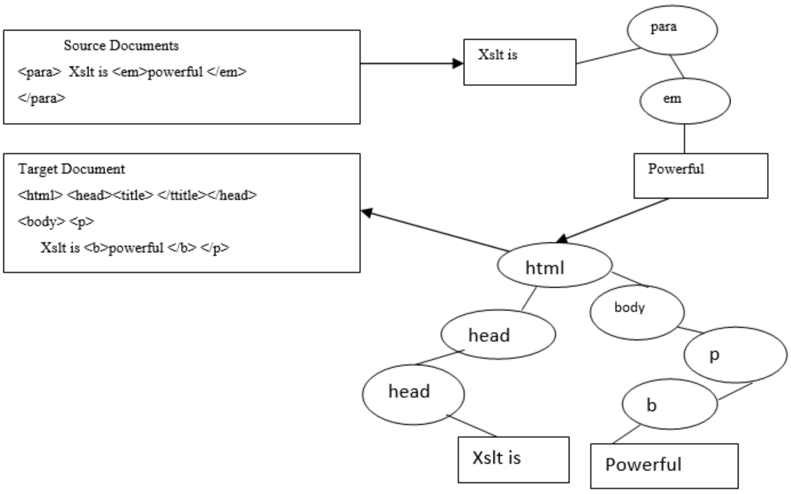


Figure 1.1 XSLT Transformation coding

However, XSLT is not intended as a completely general-purpose XML transformation language. Rather it is designed primarily for the kinds of transformations that are needed when XSLT is used as part of XSL.

2.3 Document Transformation via XSLT Processor

At this point, let's provide a quick introduction to XSLT. The W3C has already standardized a specification for transforming XML data to HTML format for display. The section covering XML structure 1999 as the "XSLT (XSL Transformations)" specification. "XSL-FO (Formatting Object)," a section related to XML format transformation, was recommended in October 2001 in the "XSL (Extensible Style sheet Language)" specification. Under XSLT, a XSLT style sheet is used to describe transformation rules in XML format. This is read by an application called an "XSLT Processor," transforming a designated XML document. The transformation results are Output in XML, HTML or text format.

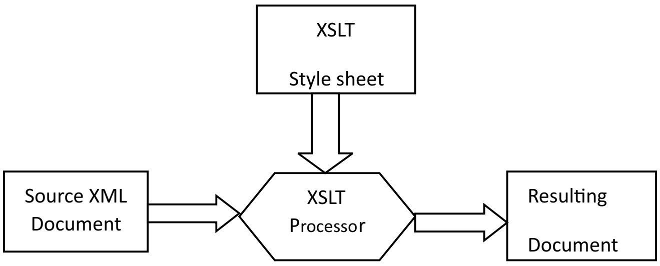


Figure1.2: Document Transformation via XSLT Processor

With XSL, document information is described in XML format (normally, an XML document is transformed via XSLT, and document information is added). This can then be loaded into an application called an "XSL Formatter" that provides an end-product (display, printed page) in a uniformly formatted layout.

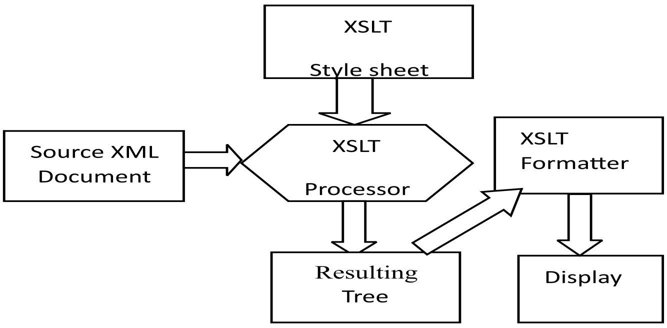


Figure1.3.XML Source Document Transformation Using XSLT

2.4 Data Transformation using XSLT Style sheets

(Converting xml documents to html documents using XSLT)
Use an XSLT style sheet to transform XML data into HTML data. Here, we will take a look at an example that uses an XSLT style sheet (LIST2) to transform an XML Document (LIST1) representing user information. LIST3 shows the actual data transformed into an HTML format. The second line of LIST1 is where the designated XSLT style sheet (list2.xsl) is applied.

LIST1: Source XML Document list1.xml

```
<?xml version="1.0"?>
<?xml style sheet type="text/xsl"href="list2.x">
<UserList>
 <User>
 <Name>John Smith</Name>
 <Account>John</Account>
 </User>
</UserList>
```

LIST2: XSLT Stylesheet list2.xsl

```
<?xml version="1.0" ?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform
">
<xsl:template match="/">
 <html> <body>
<h1>Welcome</h1>  Mr. <xsl:value-of
select="UserList/User/Name" /><br/>
</body></html></xsl:template> </xsl:stylesheet>
```

LIST3:Transformation Result list3.html

```
<html> <body> <h1>Welcome</h1>
Mr. John Smith<br> </body> </html>
```

Opening the XML doc

3. ROLE OF XSLT IN DOCUMENTS PUBLISHING

An XSLT file transforms an xml file into another xml file. An xslt processor generates a documents tree form a source xml documents and convert this to a result tree by executing the instruction specified in the xslt file .the resultant xml file may be an xhtml file which a browser can understand or a WML(wireless markup language file, which is cellular phone can display[8]. In general the following task can be performed using xslt (1) constant text generation (2) reformatting of information (3) sensitive information suppression (4) adding new information (4)sorting documents with respect to a criteria.

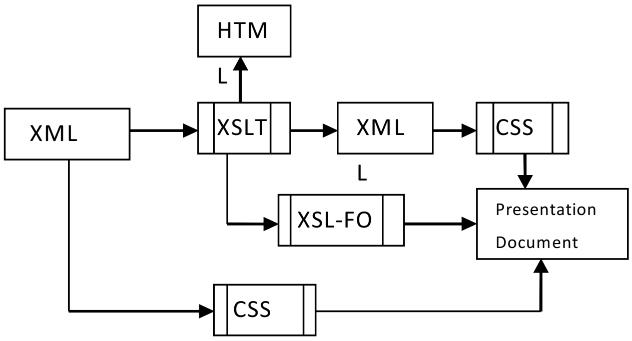


Figure1.4: Role of xslt in documents publishing

4. ROLE OF XSLT USING WEB PROGRAMMING TECHNOLOGIES

4.1 Transform XSLT Documents Using C# Technologies

Transformation (XSLT) to an Extensible Markup Language (XML) document by using the XSL Transform class to create a new XML document. XSL is an XML-based language that is designed to transform one XML document into another XML document or an XML document into any other structured document. Requirements the recommended hardware, software, network infrastructure, and service packs that you need(1)Microsoft Visual Studio 2008(2) Microsoft .NET SDK Quick Starts [10].This example uses two files that are named Books.xml and Books.xsl. I can create own Books.xml and Books.xsl files or use the sample files that are included with the .NET Software Development Kit (SDK).

Example code:

```
using System;
using System.Xml;
using System.Xml.Xsl;
namespace XSLTransformation
  { /// Summary description for Class1.
   class Class1 {
     static void Main(string[] args) {
        XslTransform myXslTransform;
             myXslTransform = new XslTransform();
myXslTransform.Load("books.xsl");
myXslTransform.Transform("books.xml",
"ISBNBookList.xml");
   }}}
```

4.2 Transform XSLT documents using Java Technologies

XSLT (Extensible Stylesheet Language Transformations) is a language for transforming XML documents into HTML, XML, or other types of documents. Formatting rules to transform the input XML data is specified in a XML stylesheet (XSL). Inside the XSL typically XML Path language (XPath) is used to identify different parts of the XML document. Xalan-Java (http://xml.apache.org/xalan-j/) is an XSLT processor for transforming XML documents. Xalan-Java fully implements W3C specification of XSLT version 1.0 and XPath version 1.0.Simple Java program to transform XML into HTML In this example we are interested to transform an XML document into a HTML table for presentation.

This is input XML data file.

```
<?xml version="1.0"?>
<catalog> <book id="bk101">
<author>Gambardella, Matthew</author>
<title>XML Developer's Guide</title>
<genre>Computer</genre>
<price>44.95</price>
  <publish_date>2000-10-01</publish_date>
<description>An in-depth look at creating
applications with XML.</description> </book>
<book id="bk102">
      <author>Ralls,Kim</author>
<title>MidnightRain</title>
<genre>Fantasy</genre>
<price>5.95</price><publish_date>2000-12-
16</publish_date>
 <description>A former architect battles corporate
zombies,  an evil sorceress, and her own childhood to
become queen  of the world.</description> </book>
 <book id="bk103">
 <author>Corets, Eva</author>
 <title>Maeve Ascendant</title>
 <genre>Fantasy</genre> <price>5.95</price>
 <publish_date>2000-11-17</publish_date>
<description>After the collapse of a nanotechnology
society in England, the young survivors lay the
foundation for a new society.</description>  </book>
</catalog>
```

This is input XSL file.

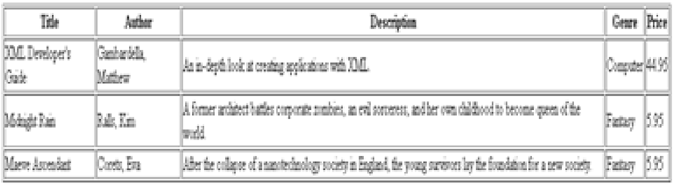
```
<? xml version="1.0" encoding="UTF-8"?>
<htmlxsl:version="1.0"xmlns:xsl="http://www.w3.or
g/1999/XSL/Transform">
 <body> <table border="1">
<tr><th>Title</th><th>Author</th>
<th>Description</th>
<th>Genre</th> <th>Price</th></tr>
<xsl:for-each select="catalog/book">
  <tr> <td><xsl:value-of select="title"/></td>
<td><xsl:value-of select="author"/></td>
   <td><xsl:value-of select="description"/></td>
<td><xsl:value-of select="genre"/></td>
  <td><xsl:value-of select="price"/></td></tr>
</xsl:for-each> </table> </body> </html>
```

Transform to Java program to perform the transformation(we use a system property to specify that we are interested in using Xalan XSLT processor).

Program code:

```
package com.sourcetricks.transform;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import javax.xml.transform.Transformer;
importjavax.xml.transform.TransformerFactory;
importjavax.xml.transform.stream.StreamResult;
importjavax.xml.transform.stream.StreamSourc;publ
ic class TransformXml
     {
public static void main(String[] args){// Input xml
data file
String xmlInput="resources/input.xml"; // Input xsl
(stylesheet) file
String xslInput="resources/input.xsl"; // Output html
file
String htmlOutput="/tmp/output.html";// Set the
property to use xalan processor System.
SetProperty("javax.xml.transform.TransformerFacto
ry","org.apache.xalan.processor.TransformerFactory
Impl");  // try with resources
try(FileOutputStream os=new
FileOutputStream(htmlOutput) ) {
FileInputStream xml=new
FileInputStream(xmlInput);
FileInputStream xsl=new
FileInputStream(xslInput);//Instantiate a transformer
factory
TransformerFactory tFactory =
TransformerFactory.newInstance(); // Use the
TransformerFactory to process the stylesheet source
and produce a Transformer
StreamSource styleSource=new StreamSource(xsl);
Transformer  transformer=tFactory.newTransformer
(styleSource); // Use the transformer and perform the
transformation
StreamSource xmlSource = new StreamSource(xml);
  StreamResult result = new StreamResult(os);
  transformer.transform(xmlSource, result); }
 catch (Exception e) {
  e.printStackTrace();}} }
```

Table 1.1 Output of the XML program using Java (screen-shot)



Title	Author	Description	Genre	Price
XML Developer's Guide	Gambardella, Matthew	An in-depth look at creating applications with XML.	Computer	44.95
Midnight Rain	Ralls, Kim	A former architect battles corporate zombies, an evil sorceress, and her own childhood to become queen of the world.	Fantasy	5.95
Maeve Ascendant	Corets, Eva	After the collapse of a nanotechnology society in England, the young survivors lay the foundation for a new society.	Fantasy	5.95

5. Conclusions:

We develop Extensible Style sheet Language Transformations (XSLT) architecture which can be used for many purposes to change the styles of different websites. In this paper we used different programming technology to develop web pages like transformation of XSLT using java technology. XSLT is a language used to specify the transformation of XML documents. It takes an XML document and transforms it into another XML document. The HTML conversion is simply a special case of XML transformation. And because the styling is applied automatically, it's easy to change the layout of my Web site. In coming future in the use of this technology we provide styles and designs code of different using websites.

6. References:

[1]Transforming XML with XSLT O'Reilly,oreilly.com /catalog/orxmlapp/chapter/h07.pdf.

[2]http://www.xmlmaster.org/en/article/d01/c07/.

[3]http://www.w3schools.com/xsl/xsl_transformation.asp.

[4] http://support.microsoft.com/kb/307322.

[5]http://www.daniweb.com/softwaredevelm nt/xml-xslt-and-xpath/threads/370593/xmlto xml-using-xslt-through-c.

[6]http://new.renderx.com/files/demos/xmlspec/xslt/REC-xslt-19991116.pdf.

[7]http://www.sourcetricks.com/2014/01/transform-xml-using-xslt-in-java.html.

[8]http://docs.oracle.com/javaee/1.4/tutorial/doc/JAXPXSLT6.html

[9]XML Encryption Syntax and Processing, W3C Recommendation (2002).http://www.w3.org/TR/xmlenc-core/.

[10].Dimitre Novatchev."Higher-Order Functional Programming with XSLT 2.0 and FXSL".ExtremeMarkupLanguages.Retrieved August 8, 2009.

[11]."A Proposal for XSL". W3C. Retrieved November 7, 2012.

[12]"XML and Semantic Web W3C Standards Timeline".

[13] http://www.w3.org/TR/xslt20/.

Fusion In Biometrics

Shruti Chanana
Department of computer science
Alfalah University, Dhauj Faridabad
Email: Shruti.chanana22@gmail.com

ABSTRACT

User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom, non-universality of the biometric trait and unacceptable error rates. Attempting to improve the performance of individual matchers in such situations may not prove to be effective because of these inherent problems. Multibiometric systems seek to alleviate some of these drawbacks by providing multiple evidences of the same identity. These systems help achieve an increase in performance that may not be possible using a single biometric indicator. Further, multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. However, an effective fusion scheme is necessary to combine the information presented by multiple domain experts.

Keywords: Multibiometric, fusion, identity, traits.

I. INTRODUCTION

A wide variety of applications require reliable verification schemes to confirm the identity of an individual requesting their service. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust verification schemes, these systems are vulnerable to the wiles of an impostor. Credit card fraud for example, costs the industry millions of dollars annually, primarily due to the lack of effective customer verification techniques [1].

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to applications. However, security can be easily breached in these applications when a password is divulged to an unauthorized user or a badge is stolen by an impostor. The emergence of biometrics has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person . Biometric systems make use of fingerprints,hand geometry, iris, retina, face, hand vein, facial thermo grams, signature or voice print to verify a person's identity [2]. They have an edge over traditional security methods in that they cannot be easily stolen or shared.

A simple biometric system has a sensor module, a feature extraction module and a matching module. The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Further, if the biometric trait being sensed or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant matching score computed by the matching module may not be reliable. Simply put, the matching score generated by a noisy input has a large variance. This problem can be addressed by installing multiple sensors that capture different biometric traits. Such systems, known as multi modal biometric systems [3], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications [4].

Multimodal systems address the problem of non-universality: it is possible for a subset of users to not possess a particular biometric. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. By asking the user to present a random subset of biometric traits, the system ensures that a `live' user is indeed present at the point of acquisition. However, an integration scheme is required to fuse the information presented by the individual modalities.

II. Fusion in Biometrics

The layout of a bimodal system is shown in Figure 2. The purpose of this diagram is to illustrate the various levels of fusion for combining two (or more) biometric systems. The three possible levels of fusion are: (a) fusion at the feature extraction level, (b) fusion at the matching score level, (c) fusion at the decision level.

(1) Fusion at the feature extraction level: The data obtained from each sensor is used to compute a feature vector. As the features extracted from one biometric trait are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector. The new feature vector now has a higher dimensionality and represents a person's identity in a different (and hopefully more discriminating) hyperspace. Feature reduction techniques may be employed to extract useful features from the larger set of features.

(2) Fusion at the matching score level: Each system provides a matching score indicating the proximity of the feature vector with the template vector.

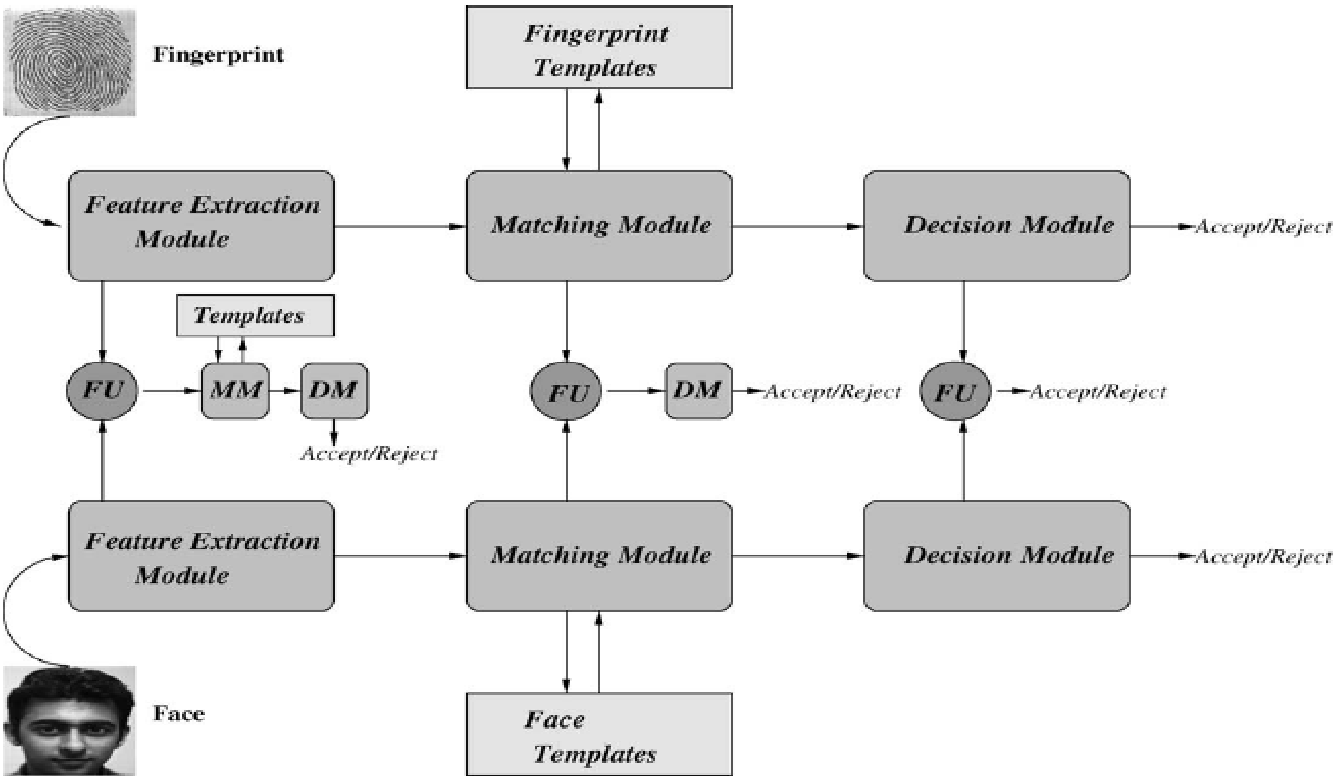


Fig. 2. A bimodal biometric system showing the three levels of fusion; FU: Fusion Module, MM: Matching Module, DM: Decision Module.

These scores can be combined to assert the veracity of the claimed identity. Techniques such as logistic regression may be used to combine the scores reported by the two sensors. These techniques attempt to minimize the FRR for a given FAR[5].

(3) Fusion at the decision level: Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes – accept or reject. A majority vote scheme, such as that employed in [6] can be used to make the final decision.

Fusion in the context of biometrics can take the following forms:
(1) Single biometric multiple representation.
(2) Single biometric multiple matchers.
(3) Multiple biometric fusion.

1 Single Biometric Multiple Representation

This type of fusion involves using multiple representations on a single biometric indicator. Typically, each representation has its own classifier. The similarity scores reported by these classifiers are then consolidated. Cappelli et al. [7] describe a fingerprint classification system that combines a structural classifier with a KL transform-based classifier by integrating the scores generated by the two classifiers. This is done by first mapping the scores (which are distance measures) into a common domain via a double sigmoid function and then taking a weighted average in the new domain. Jain et al. [8] also use multiple classifiers for fingerprint indexing. Their technique uses a K nearest neighbor classifier and a set of 10 neural network classifiers to classify fingerprints. General strategies for combining multiple classifiers have been suggested in [9]. All the approaches presented there (the highest rank method, the Borda count method and logistic regression) attempt to reduce or rerank a given set of classes. These techniques are thus relevant to the identification problem in which a large number of classes (identities) are present.
The fusion in this approach takes place at the matching stage, after the classifiers report a similarity score for each class. Prabhakar and Jain [10] show that selecting classifiers based on some “goodness" statistic may be necessary to avoid performance degradation when using classifier combination techniques. It should also be possible to combine (concatenate) the feature vectors extracted by the individual classifiers.

2 Single Biometric Multiple Matchers

It is also possible to incorporate multiple matching strategies in the matching module of a biometric system and combine the scores generated by these strategies. Jain et al. [5] use the logistic function to map the matching scores obtained from two different fingerprint matching algorithms into a single score. The authors demonstrate that such an integration strategy improves the over-all performance of a fingerprint verification system. This type of fusion also takes place at the matching stage of a biometric system. Although there are multiple matchers in this case, all matchers operate on the same representation of the biometric data.

3 Multiple Biometric Fusion

Multibiometric fusion refers to the fusion of multiple biometric indicators. Such systems seek to improve the speed and reliability (accuracy) of a biometric system[4] by integrating matching scores obtained from multiple biometric sources. A variety of fusion schemes have been described in the literature to combine these various scores. These include majority voting, sum and product rules, k-NN classifiers, SVMs, decision trees, Bayesian methods, etc. (see for example [11-16]).
An important aspect that has to be addressed in fusion at the matching score level is the normalization of the scores obtained from the different domain experts [17]. Normalization typically involves mapping the scores obtained from multiple domains into a common domain before combining them. This could be viewed as a two-step process in which the distributions of scores for each domain is first estimated using robust statistical techniques [18] and these distributions are then scaled or translated into a common domain.

Besides the techniques described above, other types of fusion are also possible in biometrics.

(i) A fingerprint biometric system may store multiple templates of a user's fingerprint (same finger) in its database. When a fingerprint impression is presented to the system for verification, it is compared against each of the templates, and the matching score generated by these multiple matchings are integrated.
(ii) A system may store a single template of a user's finger, but acquire multiple impressions of the finger during verification.
(iii) Another possibility would be to acquire and use impressions of multiple fingers for every user. These possibilities have been discussed in [19].

I. Conclusion and Future Work

The benefits of multi-biometrics may become even more evident in the case of a larger database of users. Future experiments include developing user specific weights for the individual modalities. Different users tend to adopt differently to individual biometric indicators. For example, some users may find it easier to interact with a fingerprint sensor than with a hand image sensor. Consequently, their chances of being rejected by a stand-alone hand geometry biometric system may be high. Therefore, it would be appropriate to associate different weights to the individual modalities based on the user's preference or the system's performance for that user. These weights can be learnt over time by examining the stored template of the user, the query set provided by the user, and the matching scores for each of the individual modalities. By doing so, each user is tightly coupled with that subset of biometric traits that distinguishes her very well from the rest of the users. User specific weights also help address the problem of non-universality of biometric traits by giving less weightage to those traits that are not easily extracted.

References

[1] P. Wallich, How to steal millions in chump change, Scientific American (Aug
1999).

[2] A. K. Jain, R. Bolle, S. Pankanti (Eds.), Biometrics: Personal Identification in
Networked Society, Kluwer Academic Publishers, 1999.

[3] L. Hong, A. K. Jain, S. Pankanti, Can multi biometrics improve performance?, in: Proceedings AutoID'99, Summit(NJ), USA, 1999, pp. 59{64.

[4] L. Hong, A. K. Jain, Integrating faces and fingerprints for personal identification, IEEE Transactions on PAMI 20 (12) (1998) 1295{1307.16

[5] A. K. Jain, S. Prabhakar, S. Chen, Combining multiple matchers for a high security fingerprint verification system, Pattern Recognition Letters 20 (1999)1371{1379.

[6] Y. Zuev, S. Ivanon, The voting as a way to increase the decision reliability, in:
Foundations of Information/Decision Fusion with Applications to Engineering
Problems, Washington D.C., USA, 1996, pp. 206{210.

[7] R. Cappelli, D. Maio, D. Maltoni, Combining fingerprint classifiers, in: First
International Workshop on Multiple Classifier Systems, 2000, pp. 351{361.

[8] A. K. Jain, S. Prabhakar, L. Hong, A multichannel approach to fingerprint classification, IEEE Transactions on PAMI 21 (4) (1999) 348{359.

[9] T. K. Ho, J. J. Hull, S. N. Srihari, Decision combination in multiple classifier systems, IEEE Transactions on PAMI 16 (1) (1994) 66{75.

[10] S. Prabhakar, A. K. Jain, Decision-level fusion in fingerprint verification, Pattern Recognition 35 (4) (2002) 861{874.

[11] U. Dieckmann, P. Plankensteiner, T. Wagner, Sesam: A biometric person identification system using sensor fusion, Pattern Recognition Letters 18 (9) (1997) 827{833.

[12] J. Kittler, M. Hatef, R. P. Duin, J. G. Matas, On combining classifiers, IEEE
Transactions on PAMI 20 (3) (1998) 226{239.

[13] E. Bigun, J. Bigun, B. Duc, S. Fischer, Expert conciliation for multimodal person authentication systems using Bayesian Statistics, in: First International Conference on AVBPA, Crans-Montana, Switzerland, 1997, pp. 291{300.

[14] A. K. Jain, L. Hong, Y. Kulkarni, A multimodal biometric system using fingerprint, face and speech, in: Second International Conference on AVBPA,
Washington D.C., USA, 1999, pp. 182{187.

[15] P. Verlinde, G. Cholet, Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application, in: Second International Conference on AVBPA, Washington D.C., USA, 1999, pp. 188{193.

[16] S. Ben-Yacoub, Y. Abdeljaoued, E. Mayoraz, Fusion of face and speech data for person identity veri_cation, Research Paper IDIAP-RR 99-03, IDIAP, CP 592, 1920 Martigny, Switzerland (Jan 1999).

[17] R. Brunelli, D. Falavigna, Person identi_cation using multiple cues, IEEE Transactions on PAMI 12 (10) (1995) 955{966.

[18] F. Hampel, P. Rousseeuw, E. Ronchetti, W. Stahel, Robust Statistics: The Approach Based on Inuence Functions, John Wiley & Sons, 1986.

[19] A. K. Jain, S. Prabhakar, A. Ross, Fingerprint matching: Data acquisition and performance evaluation, Technical Report MSU-TR:99-14, Michigan State University (1999). 17

[20] H. Rowley, S. Baluja, T. Kanade, Neural network-based face detection, IEEE
Transactions on PAMI 20 (1) (1998) 23{38.

[21] G. Burel, C. Carel, Detection and localization of faces on digital images, Pattern
Recognition Letters 15 (1994) 963{967.

[22] G. Yang, T. Huang, Human face detection in a complex background, Pattern
Recognition 27 (1) (1994) 53{63.

[23] M. Kirby, L. Sirovich, Application of the Karhunen-Loeve procedure for the characterization of human faces, IEEE Transactions on PAMI 12 (1) (1990) 103{108.

[24] M. Turk, A. Pentland, Eigenfaces for recognition, Journal of Cognitive Neuroscience 3 (1) (1991) 71{86.

[25] A. K. Jain, L. Hong, S. Pankanti, R. Bolle, An identity authentication system using fingerprints, Proceedings of the IEEE 85 (9) (1997) 1365{1388.

[26] A. K. Jain, A. Ross, S. Pankanti, A prototype hand geometry-based verification system, in: Second International Conference on Audio and Video-based Biometric Person Authentication (AVBPA), Washington, D.C., USA, 1999, pp.166{171.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005