Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Surveys of Attacks in MANET

Manjeet Singh[1]
Research Scholar (Deptt. of CSE)
SGGSW University , Fatehgarh Sahib
Punjab, India

Gaganpreet Kaur [2]
Assistant Professor (Deptt. of CSE)
SGGSW University , Fatehgarh Sahib
Punjab, India

Abstract--- A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces In order to make communication among nodes, the nodes dynamically establish paths among one another. The nature and structure of such networks makes it attractive to various types of attackers. Security is a major concern for protected communication between mobile nodes. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. MANET can operate in isolation or in coordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. This flexibility, along with their self-organizing capabilities, are some of MANET's biggest strengths, as well as their biggest security weaknesses.

Keywords-MANET, mobile-node, malicious-attacker, gateway.

I. Introduction

A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. Nodes in MANETs can join and leave the network dynamically [1]. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment. As the transmission takes place in open medium makes the MANETs more vulnerable to security attacks. In the presence of security protocol effect of various attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes.

II. MANET VULNERABILITIES:

A vulnerability is a weakness in security system [2]. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

A. *Lack of centralized management*

MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

A. Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

B. Scalability

Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

C. Cooperativeness

Routing algorithm for MANETs usually assume that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

D. Dynamic topology

Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

E. Limited power supply

The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is find that there is only limited power supply.

There are different types of attacker present in MANETs, which tries to reduce the performance of network. In this paper we study about various attackers, which are classified in the figure 1.

Fig 1: Classification of Attackers

III. Attacks On Manet

An integrated Internet and mobile ad hoc network can be subject to many types of attacks [3]. These attacks can be classified into two categories, attacks on Internet connectivity and attacks on mobile ad hoc networks.

A. Attacks on Internet Connectivity

Attacks on Internet connectivity can be classified into following categories:

*1) Bogus Registration***:** A bogus registration is an active attack in which an attacker does a registration with a bogus care-of address by masquerading itself as someone else. By advertising fraudulent beacons, an attacker might be able to attract a MN (mobile node) to register with the attacker as if MN has reached HA (home agent) or FA (foreign agent). Now, the attacker can capture sensitive personal or network data for the purpose of accessing network and may disrupt the proper functioning of network. It is difficult for an attacker to implement such type of attack because the attacker must have detailed information about the agent.

2) Replay Attack: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

Suppose any mobile node A wants to prove its identity to B. B requests his password as proof of identity, which A dutifully provides (possibly after some transformation like a hash function); at the same time, C is eavesdropping the conversation and keeps the password. After the interchange is over, C connects to B presenting itself as A; when asked for a proof of identity, C sends A's password read from the last session, which B accepts. Now, it may ruin the proper operation of the network.

3) Forged FA: It is a form of network attack in which a node advertises itself as a fraudulent FA then MN's under the coverage of the forged FA may register with it. Now, forged FA can capture the sensitive network data and may disrupt the proper functioning of the network.

B. Attacks on Mobile Ad hoc Networks

Attacks on mobile ad hoc networks can be classified into following two categories:

1) Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information [5]. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

2) 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 [2].

3) Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries [1]. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

4) Snooping: Snooping is unauthorized access to another person's data [3]. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function. For

example, a snoop server is used to capture network traffic for analysis, and the snooping protocol monitors information on a computer bus to ensure efficient processing.

5) Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed

6*) Flooding attack:* In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [6]. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

7) *Black hole Attack:* Route discovery process in AODV is vulnerable to the black hole attack [8]. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough route, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

8) Rushing Attack: Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [1]. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react. For example, in figure the node "4" represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than do those from other nodes. This result in when neighboring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attacker.

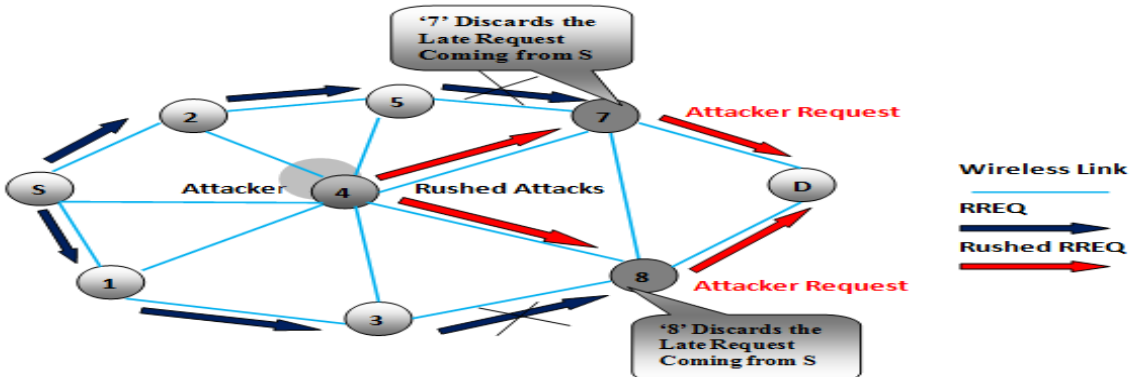

Fig 2: Rushing Attack

9) Colluding misrerlay attack: In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET [6]. This attack is difficult to detect by using the conventional methods such as *watchdog* and *path rater*. Consider the case where node A1 forwards routing packets for node T. the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In [6] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

10) Link spoofing attack: In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

11) Selective Forwarding Attack: The selective forwarding Attack was first described by Karlof and Wagner [7]. This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them.

There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behavior causes a DoS attack for that particular node or a group of node.

They also behave like a Black-hole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network. Another form of selective forwarding attack is called Neglect and Greed. In this form, the subverted node arbitrarily neglecting to route some messages. It can

still participate in lower level protocols and may even acknowledge reception of data to the sender but it drops messages randomly. Such a node is neglectful. When it also gives excessive priority to its own messages it is also greedy. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between sensor nodes.

12) Sleep Deprivation: In sleep deprivation attack, the resources of the specific node/nodes of the network are consumed by constantly keeping them engaged in routing decisions [9]. The attacker node continually requests for either existing or non-existing destinations, forcing the neighboring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.

13) Node Isolation Attack: The authors in this work have introduced an attack against the OLSR protocol . As implied by the name, the goal of this attack is to isolate a given node from communicating with other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

14) *Routing Table Poisoning Attack:* Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number. This causes all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.

15) Blackmail: The attack incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network [9].

16) Snare Attack: Lin et al. have proposed the snare attack, which relates to military specific applications. In a battlefield, a node could be physically compromised (say when the corresponding soldier is caught by the enemy). Afterwards, the compromised node could be used to lure a Very Important Node, (say the commander), into communicating with it. Since the adversary can easily intercept any transmission in the network through the compromised node, the adversary can identify the physical location of the VIN by tracing and analyzing some routes. After locating the VINs, the adversary will be able to launch a Decapitation Strike on those VINs as a short cut to win the battle.

17) The Invisible Node Attack: Andel et al. have defined the invisible node attack and proved it to be different from the existing attacks (man in the middle, masquerading, and wormhole) and established its uniqueness. They have defined it as in any protocol that depends on identification for any functionality, any node that effectively participates in that protocol without revealing its identity is an invisible node and the action and protocol impact is termed an INA. Discussing the effects of INA on different routing protocols, they have shown it to be an unsolvable attack so far.

18) *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 [2]. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole .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.

19) *Cloning Attack:* Clone attack or node replication attack is a severe attack in WSNs [10]\. In this attack, an adversary captures only a few of nodes, replicates them and then deploys arbitrary number of replicas throughout the network. It is very hard to distinguish between non compromised nodes a clone node since a clone has the same security and code information of original node. Hence cloned nodes can launch a variety of other attacks. The detection of cloning attacks in a wireless sensor network is therefore a fundamental problem. Many existing protocols expose the following limitations: high performance overheads, unreasonable assumptions, necessity of central control, lack of smart attack detection etc. Few existing approaches like solved these problems. But here we present a security model to detect two more attacks along with cloning attack detection with the same communication cost and performance overhead. We used the benefit of mobile agent to reduce the communication cost. Also the proposed protocol considers Mobile Wireless Sensor Network environment.

20) Jamming: Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication [1]. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

21) Active Interference: An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information.

22) *Selfish Misbehavior of Nodes:* Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network. It may include two important factors.

Conservation of battery power

Gaining unfair share of bandwidth

The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads to congestion in network. However most of routing protocols have no mechanism to detect whether the packets being forwarded or not except DSR (dynamic source routing).

23) Replay Attacks: In MANETs, the topology is not fixed; it changes frequently due to mobility of nodes. In replay attack, a malicious node record control messages of other nodes and resends them later. This results in other nodes to record their routing table with stale routes. These replay attacks are later misused to disturb the routing operation in a MANETs.

24) Link Withholding & Link Spoofing Attacks: In link withholding attack, the malicious node does not broadcast any information about the links to specific nodes [1]. It results in losing the links between nodes. In Link spoofing attacks, a malicious node broadcasts or advertises the fake route information to disrupt the routing operation. It results in, malicious node manipulate the data or routing traffic.

25) Session Hijacking: Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc.) and other information from nodes. Session hijacking attacks are also known as address attack which make effect on OLSR protocol. The TCP-ACK storm problem may occur when malicious node launches a TCP session hijacking attack.

26) SYN Flooding Attack: The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node . These half opened connection are never completes the handshake to fully open the connection.

27) Malicious code attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

28) Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

29) 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 [2].

30) 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.

31) 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

32) 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.

33) 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.

34) Eavesdropping: The intruder silently listens to the communication by tapping the wireless link.

35) 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 reciever or impersonate the receiver to reply to the sender.

36) 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 neighbor can no longer be contacted.

37) 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.

IV. Conclusion

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with

certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many both known and unknown security threats.

References

[1] Gagandeep, Aashima, Pawan Kumar, *Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review* ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[2] Priyanka Goyal,Sahil Batra , Ajit Singh, *A Literature Review of Security Attack in Mobile Ad-hoc Networks*, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[3] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, *Different Types of Attacks on Integrated MANET- Internet Communication* , International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).

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

[5] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, *Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm*, International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[6] Rishabh Jain, Charul Dewan, Meenakshi, *A Survey on Protocols & Attacks in MANET Routing*, IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 2231 –5268

[7] Wazir Zada Khana, Yang Xiangb, Mohammed Y Aalsalema, Quratulain Arshada *The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures*, I.J. Wireless and Microwave Technologies, 2012, 2, 33-44 Published Online April 2012 in MECS.

[8] Pramod Kumar Singh, Govind Sharma, *An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[9] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, *A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks*, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617.

[10] *D Sheela , G. Mahadevan, Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations, International Journal of Computer Applications (0975 – 8887) Volume 55– No.9, October 2012.*

