International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 1-10

http://www. irphouse.com /ijict.htm

A Study on Different Security Threats in Mobile Ad-hoc Network

A. Chirag Tehlanl and Divya Sharma

CSE/IT Department, ITM University, Sector-23A Gurgaon, INDIA.

Abstract

As the mobile network is a public access network, so that the major challenge in this network is the security threats. These threats exist in different network layers to reveal the information or damage the communicating data. In this paper, different kinds of attacks are discussed along with their impact analysis and the damage control mechanism. The exploration of some common mobile network attack is also present in this paper.

Keywords: Security Threats, Attacks, DOS, Active, Passive.

1. Introduction

A Mobile network is one of the most available decentralized system in which nodes are generally in moving position. Because of these moving capabilities, the nodes enter and exit from one network to other. When a new node enters to some network, it cannot be treated as the suspicious node because of open nature of the network. This dynamic nature of mobile network is itself a challenge in terms of security. Each node in mobile network itself acts as a host or the router. To perform the communication with any node, each node depends only on his current neighbors and these neighbor nodes are not fixed. It means the communication in mobile network cannot be fully reliable at any time.

Security is always the major concern in mobile network. It is defined under different vectors of confidentiality, reliability, integrity of the data as well as nodes. There are number of security issues faced by a mobile network because of different reasons, shown in Fig.1. The open medium here defines the different kind of communication medium available for communication at the same time and during communication it can switch to these communication medium because of open nature. The dynamic topology formation defines the inclusion and exclusion of any node dynamically to the network so that the security threats get increased.

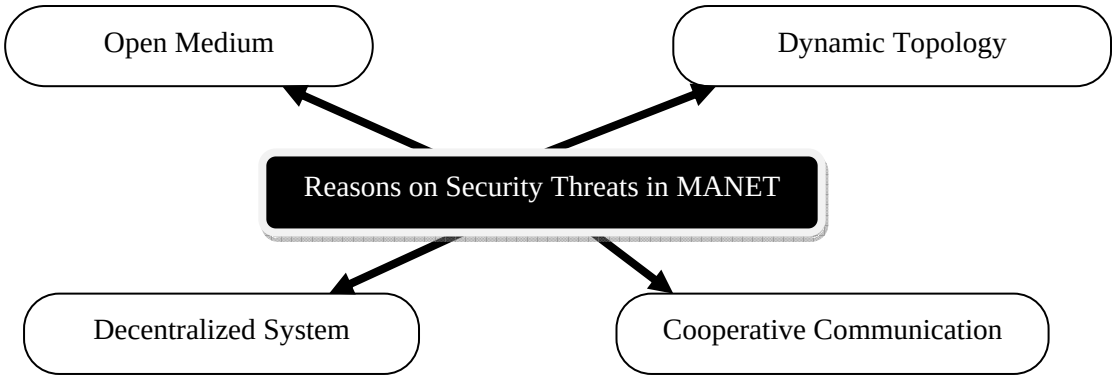

Fig. 1: Reasons of Security Threats in MANET.

The decentralized system here means there the lack on central control or the management to the mobile network. Each node itself behaves independently without the control of any central entity. Each node itself behaves as the node as well as the router. The cooperative communication is another reason of increasing security threats in mobile network. This kind of communication is performed with the help of neighboring nodes rather than dedicated path. The attacks or the threats associated with a mobile network exist at different layers of mobile network. Some of such attacks, their associated layers and the effective solution is shown in table 1.

Table 1: Layer based Attack Distribution.

Layer	Attacks	Solution
Application Layer	Repudiation, data corruption	Detecting and preventing virus, worms, malicious codes and application abuses by use of Firewalls.
Transport Layer	Session hijacking, SYN Flooding	Authentication and securing end-to-end or point-to-point communication use of public cryptography
Network Layer	Routing protocol attacks (e.g. DSR, AODV), Wormhole, blackhole, Byzantine, looding	Protecting the ad hoc routing and forwarding protocols
Data Link Layer	Traffic analysis, monitoring, disruption MAC(802.11), WEP weakness etc.	Protecting the wireless MAC protocol and providing link layer security support.
Physical Layer	Eavesdropping, Jamming, Interceptions.	Preventing signal jamming denial-of-service attacks by using Spread Spectrum Mechanism.

There are different kind of attacks that are divided under different categories based on different parameters. These attack categories are discussed here under.

1.1 External and Internal Attack

As the name suggest, the external attacks are performed by the node that is not part of the network itself. In this attack, attacker generally disturbs the communication by sending the fake packets, and increases the network congestion so that the performance of the network degrades. But in case of internal node attack, the attacker node behaves like a normal node but sometimes not participate in some communication event. The internal node can present its identify as some other node so that it can avail the information that is communicating to some other node. These kind of attacks includes the man-in-middle attack that basically reveals the information of some other active node of the network.

1.2 Active and Passive Attack

In this type of attack classification, the impact of the attack is considered as the attack categorization parameter. The active attack can be an internal or external attack. These attacks basically destroy the communicating information and degrade the network performance. As they are the active part of the network they can inject the attack easily over the attack to affect the particular service or node. This kind of attack is capable to reveal the information or represent itself as the fake entity so that the network communication can be captured. Attacker can modify and fabricate the information in communicating packets easily. In case of passive attack, the attacker is capable to identify the network communication and disturb the network communication. This attack can easily hijack the network information or delay the network communication.

In this paper, the exploration to the security threats in the mobile network is defined. In this section, the introduction to the network security and security threats is defined. The section also includes the classification of different kind of attacks as well as their distribution among different network layers is defined. In section II, the earlier work in the direction of security threats is discussed. In section III, the exploration of some of the most common security threats is defined. In section IV, the conclusion derived from the work is presented.

2. Existing Work

As the network security is one of the most critical issue for mobile networks, because of this, lot of concern is given to the security threats in mobile networks. Some of the work defined by earlier researchers is discussed in this section. In year 2010, Axel Kring has presented a neighborhood monitoring mechanism for adhoc network. Author presented a k-hop analysis based mechanism under defined constraints so that the network limitations will be handled. Author has defined the work on the malicious node detection by performing the dynamic analysis on neighboring nodes[1]. Another work on the the malicious node detection was proposed by Ying Li in year 2011. Author defined the work on tracking based scenario. Author defined the mathematical and probabilistic framework for the detection of attacks and the exceptions[2]. Another work on the malicious node detection and a secure routing was presented by Bogdan Carbunar in year 2004. Author investigate the security threats in mobile networks so

that the reliable communication will be drawn from the communication. Author has defined a secure infrastructure oriented communication in misbehaving mobile networks[3].

A work on the exploration of hijacking attack and the preventive mechanism was presented by Johann Schlamp in year 2012. Author has defined a security based work to identify the spam packets during the communication process as well as provided an effective approach to detect the victim and analysis is done through the IP prefix analysis so that the long term benefits will be obtained from the work. Author has defined the incidental communication and control mechanism in mobile network[4]. A control mechanism to restrict the outgoing spam communication was handled by Joshum Goodman in year 2004. Author has defined the conventional technique to analyze the message packets under different techniques so that the life time of the network communication will be increased. Author has defined the work to obtain the maximum profit from the communication so that reliable communication effect will be drawn[5]. Danny Dhillon has defined the work to improve the communication integrity in case of intrusion mobile network. Author defined the safeguard based approach to increase the detection rate so that effective communication schedule will be obtained[6].

Ahmed Khurshid has presented a work on the real time analysis on different network invariants that affects the network flow. Author presented a controller device based approach to control the forwarding communication as well as the reliable communication will be drawn from the network[7]. Another work on the blackhole detection was presented by Evan Cooke in year 2004. Author defined the exploration of work under the traffic analysis so that reliable packet communication will be performed. Author defined the work based on Internet Motion sensor so that the infrastructure based effective communication will be drawn from the network[8]. A work on the effective routing in opportunistic network was presented by Umair Sadiq in year 2012. Author presented the forwarding rate analysis along with packet loss analysis to identify the communication incentive. Author presented the work to analyze the control in non linear communication network. Author defined the work in the optimal conditions so that the flow maximization will be performed[9]. The exploration of the node replication attack was presented by Mauro Conti. Author presented a energy and memory effective solution in a constrained network so that reliable communication path will be obtained[10].Garima Gupta defined the characteristic analysis based algorithm which generate an effective route under the malicious node attack. Author defined the probabilistic behaviors analysis scheme to provide the solution against blackhole attack[11]. A work on the topology aware analysis approach to reveal the security scheme in mobile networks. Author presented an isolated mechanism to handle the attacks and to reduce the false detection rate. Author presented a overhead analysis approach to improve the network reliability and to minimize the attack impact in mobile network[12]. A two dimensional analysis approach to improve the network QoS under different adversarial environments was presented by Peter J.J. McNeney. Author discussed two main issues to improve the

QoS and to improve the network reliability. Author defined a single path adaptation and multipath adaptation mechanism to improve the network bandwidth and to increase the network reliability[13].

3. Security Threats

In this section, some of the most promising security attacks are defined along with their processing as well as the impact on the mobile network. The impact of different kind of attacks is performed in terms of malicious activities. Some of such activities are shown here in table 2

Table 2: Malicious Activities Performed by Different Attacks.

Activity	Attack	Relative Checking Action
Delay	DOS Attack (Flooding, Jamming)	The packet delivery time will be increased than normal
Packet Drop	AODV, Wormhole, DOS	The packet does not arrive to the destination node so that throughput is decreased
Modify	Phinising	The information of a packet is modified, the outgoing packet is not same to the actual packet sent
Fabricate	counterfeiting	Information exists with the packet, the sending packet and the outcome packet is not same.
Misrouting	AODV, Wormhole	Modify the route of the packet

3.1 Denial of Service (DoS)

DoS attack is one of the most common attack that actually disturb the service distribution over the network. There are different forms of DoS attacks. In the traditional form of DoS attack, it floods the network by broadcasting the fake packets over the network. Because of this, the congestion over the network is increased and the efficiency of the network degrades. This kind of attack is performed from any centralized location so all nodes so that the resources to the other nodes not get available for the longer time and the complete network communication delays. This kind of attack having its impact in long term over the communication network when the communication over the network becomes heavy and slowly it start losing the packets over the network. DoS attack can be injected by the attacker on any network layer so that the overall network communication get disturb. This kind of attack actually exploits the network communication and disrupts the communication functionality. This disturb the routing process as well as block the resource access so that the normal functioning associated with the particular resource will also disturb. This attack can also be applied to any protocol and implied the affect in terms of

network delay, low response time and packet loss. The basic model of DoS attack is shown in Fig.2.

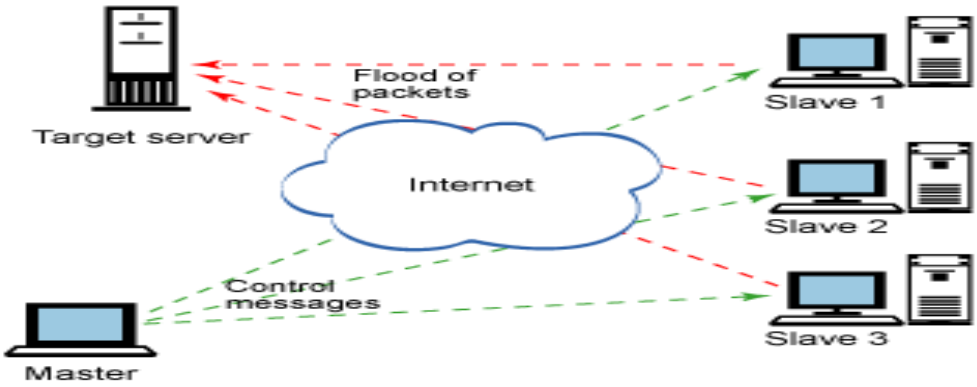

Fig. 2: DoS Attack.

Different type of Dos Attacks are also listed in this section.

A) Jamming

In this kind of DoS attack, the concentration of the attacker is to some centralized resource or the node that attacker wants to block. Attacker keep monitoring the communication on that node and identify the communication frequency over that node or the resource. Author has defined the error free signal reception and communication under different communication spectrums. Jamming basically, block the communication over that node and get the full access to the particular resource.

B) SYN Flooding

It is the another form of DoS attack in which, the attacker node performs the bulk communication so that the spoofing of the SYN packets is performed. As a node receive the SYN packets, it sends the SYN-ACK packets to the attacker node. The victim node waits for the ACK packets so that the network get open for getting the response packet. The network is half open to the vitim so that the connection is defined for the fixed size table so that the size table of the communication also get large set of entries. This overall disturbs the network communication and the communication gets delayed. It also overflow the buffer of the victim and it results the packet loss over the communication. The normal nodes over the network does not get the sufficient bandwidth to perform the reliable communication. In case of 3-way acknowledgement process, the situation becomes more critical where the ACK packets over the network get increased.

C) Distributed DoS Attack:

Distributed DoS attack is more critical than normal Dos attack because it affect the throughput of overall distributed network. This kind of attack includes the several adversaries so that the network throughput is colluded and the preventive

communication access is performed over the network. The distributed DoS attack is shown in Fig.3.

D) Blackhole Attack

It is one of the critical mobile network attack in which attacker node direct the communication to some victim node towards the attacker node. Attacker node accepts the data packets but not forward to the neighboring nodes. The processing of the blackhole attack is shown in Fig.4. In this attack form, the attacker node represent itself as the normal node and consume the network packets. As shown in the figure, the attacker node 3 behaves abnormally that accepts the packet from the source node but does not forward it to the neighboring nodes. Because of this, the throughput on the receiver node is decreased and the packet drop ratio over the network gets increased.

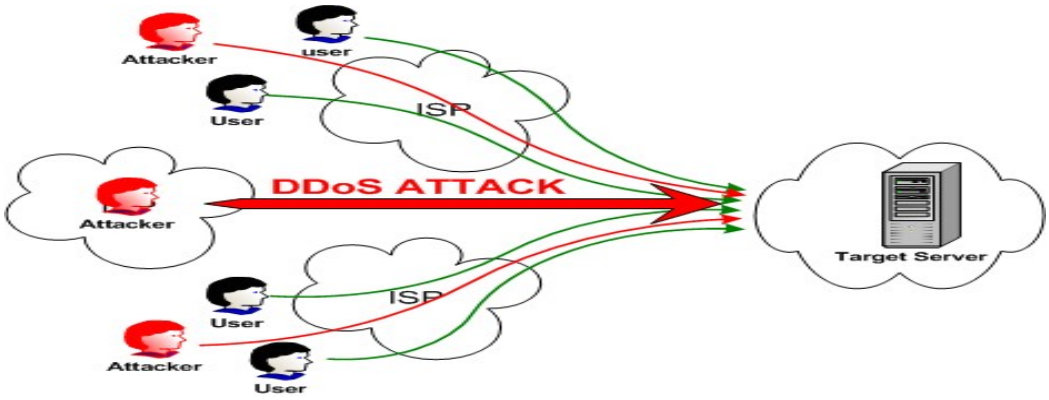

Fig. 3: Distributed DoS Attack.

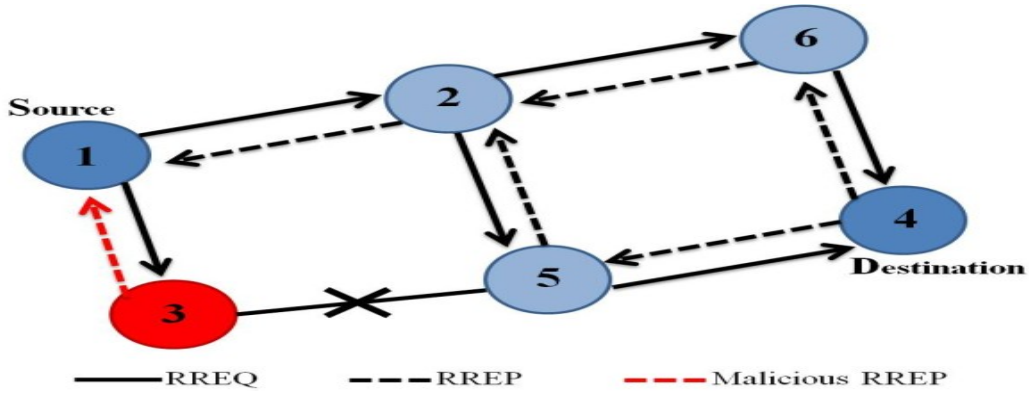

Fig. 4: Blackhole Attack.

E) Wormhole attack

It is a tunnel based attack in which two or more network nodes forms a tunnel and if the communication diverts to this tunnel, the communication will not be forwarded to any other node over the network. This kind of attack is applied over the network

because the attacker nodes exist in a pair. The attacker nodes make a private communicating path so that the bandwidth of the network is also consumed. The process of worm hole attack is shown in Fig.5.

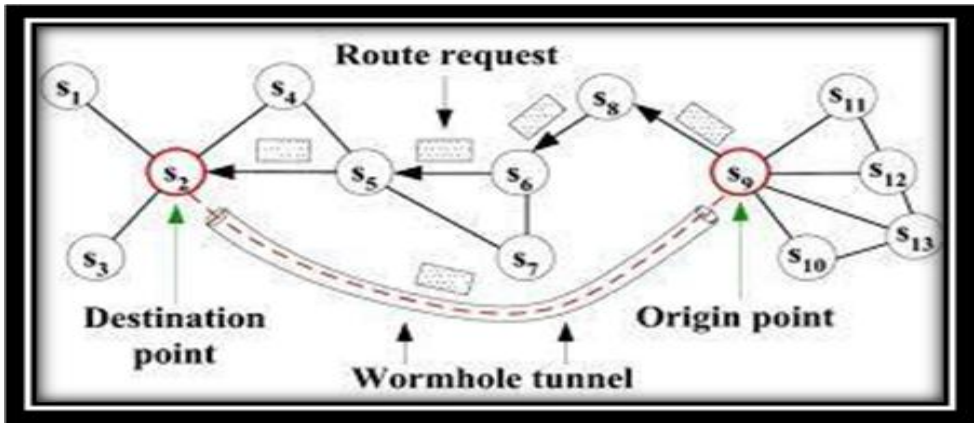

Fig. 5: Worm Hole Attack.

4. Conclusion

In this paper, an exploration to the security threats associated with mobile networks is defined. The paper has defined the work on classification and exploration of different kind of attacks in the mobile network. The attack impact and the basic functioning is also described in this paper.

Table III: Defense against DoS attacks at specific layer, requirements and drawbacks.

Attack Type	Targeted Layer	Requirement	Drawbacks
Flooding	Network layer	Neighbor suppression and path cutoff	No implementation details
Collision, packet drop	MAC and network layer	RTS/CTS and watch-dog monitoring	Higher computational overhead
Black hole/Gray hole	Network and transport layer	Least-alike re-routing (LARR) algorithm	Experimented in identical network condition
Jamming	MAC Layer	Correlation, CTS, RTS, DCF and CSMA/CA	Only very few nodes used for simulation
Jamming and collision	MAC and network layer	IDS, k-means, information gain ratio, neural networks	Higher computational overhead

Flooding resource consumption	Network layer	Apriori algorithm, clustering and association algorithm	Node complexity is high
Packet drop, reorder delay	Network layer	Disjoint outgoing paths, semi-markov process, node isolation	Impact of node behaviours on network performance is still problem

References

[1] Axel Krings," Neighborhood Monitoring in Ad Hoc Networks", CSIIRW ’10, April 21-23, 2010, Oak Ridge, Tennessee, USA ACM 978-1-4503-0017-9

[2] Ying Li," Component-Based Track Inspection Using Machine-Vision Technology", ICMR’11, April 17-20, 2011, Trento, Italy ACM 978-1-4503-0336-1/11/04

[3] Bogdan Carbunar," JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks", WiSe’04, October 1, 2004, Philadelphia, Pennsylvania, USA. ACM 1-58113-925-X/04/0010

[4] Johann Schlamp," How to Prevent AS Hijacking Attacks", CoNEXT Student’12, December 10, 2012, Nice, France. ACM 978-1-4503-1779-5/12/12

[5] Joshua Goodman," Stopping Outgoing Spam", EC’04, May 17–20, 2004, New York, New York, USA. ACM 1-58113-711-0/04/0005

[6] Danny Dhillon," Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", IWCMC’06, July 3–6, 2006, Vancouver, British Columbia, Canada. ACM 1-59593-306-9/06/0007

[7] Ahmed Khurshid," VeriFlow: Verifying Network-Wide Invariants in Real Time", HotSDN’12, August 13, 2012, Helsinki, Finland. ACM 978-1-4503-1477-0/12/08

[8] Evan Cooke," Toward Understanding Distributed Blackhole Placement", WORM’04, October 29, 2004, Washington, DC, USA. ACM 1-58113-970-5/04/0010

[9] Umair Sadiq," CRISP: Collusion–Resistant Incentive–Compatible Routing and Forwarding in Opportunistic Networks", MSWiM’12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10

[10] Mauro Conti," A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks", MobiHoc’07, September 9-14, 2007, Montréal, Québec, Canada. ACM 978-1-59593-684-4/07/0009

[11] Garima Gupta," Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks", Q2SWinet’12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10

[12] Abhijit Das," Energy Aware Topology Security Scheme for Mobile Ad Hoc Network", ICCCS’11, February 12–14, 2011, Rourkela, Odisha, India. ACM 978-1-4503-0464-1/11/02

[13] Peter J. J. McNerney," A 2-Dimensional Approach to QoS Provisioning in Adversarial Mobile Ad Hoc Network Environments", MSWiM’12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10