International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015
ISSN 2091-2730

Prevention of Attacks In Manet Using Usor Protocol

Karthikeyan.V[1]
Department of Electronics and Communication Engineering.
Angel College of Engineering and Technology,
Tirupur-641 665, INDIA
karthik.v.1987@gmail.com

Abstract—Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wireless networks, providing privacy protection with low power devices and low bandwidth network connection is very challenging task. In this project, solid privacy requirements has been defined regarding privacy-maintain routing in MANET. Then an unobservable secure routing scheme USOR has been proposed to offer complete unlink ability and content un-observability for all types of packets. Privacy-preserving routing is crucial for some Adhoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in Adhoc networks. However, none of these schemes offer complete unlinkability or unobservability property.USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery.USOR has been implemented on ns2, and evaluated its performance by comparing with AODV and MASK. The simulation results show that USOR not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes like MASK.

Keywords-Unobservable Secure On Demand Routing Protocol (USOR), Mining Association with Secrecy Constrains (MASK), Adhoc on Demand Distance Vector Routing Protocol (AODV)

I. INTRODUCTION

Communication is the process by which two or more people exchange ideas, facts, feelings, or impressions in ways that each gains a common understanding of the meaning, intent, and use of messages. Thus, good communication consists of creating understanding of the message. In computerized technology, we need to transfer the data from one another without any problem like security and quality. In wired networks, one has to gain access to wired cables so as to eavesdrop communications. The attacker only needs an appropriate transceiver to receive wireless signal without being detected. In wired networks, devices like desktops are always static and do not move from one place to another. Hence in wired networks there is no need to protect users' mobility behavior or movement pattern, while this sensitive information should be kept private from adversaries in wireless environments.

A. Need of security

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, denial of a computer network and network-accessible resources. Users choose an ID and password or other authenticating information that allows them access to information and programs within their authority [1]. The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers.

They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations[2][3]. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

II. THREATS TO NETWORK SECURITY

A Network attack or security incident is defined as a threat, intrusion, and denial of service or other attack on a network infrastructure that will analyze your network and gain information to eventually cause your network to crash or to become corrupted. In many cases, the attacker might not only be interested in exploiting software applications, but also try to obtain unauthorized access to network devices. Unmonitored network devices are the main source of information leakage in organizations. In most organizations, every email message, every web page request, every user logon, and every transmittable file is handled by a network device. Under some setups, telephone service and voice messaging are also handled by network devices. If the attacker is able to "own" your network devices, then they "own" your entire network.[2][3] Network attacks cut across all categories of software and platform type. There are at least seven types of network attacks.

- Sniffing

- Hijacking
- Trojans
- DoS

A. Sniffing

Packet sniffing is the interception of data packets traversing a network. A sniffer program works at the Ethernet layer in combination with network interface cards (NIC) to capture all traffic travelling to and from internet host site[1][4]. Further, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating by anywhere near the internet host site. A sniffer placed on any backbone device, inter-network link or network aggregation point will therefore be able to monitor a whole lot of traffic. Most of packet sniffers are passive and they listen all data link layer frames passing by the device's network interface [4][5]. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion network host interface to detect sniffing.

The key to detecting packet sniffing is to detect network interfaces that are running in promiscuous mode. Sniffing can be detected two ways:

1. Host-based: Software commands exist that can be run on individual host machines to tell if the NIC is running in promiscuous mode.
2. Network-based: Solutions tend to check for the presence of running processes and log files, which sniffer programs consume a lot of. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files. The best countermeasure against sniffing is end-to-end or user-to-user encryption.

B.Hijacking

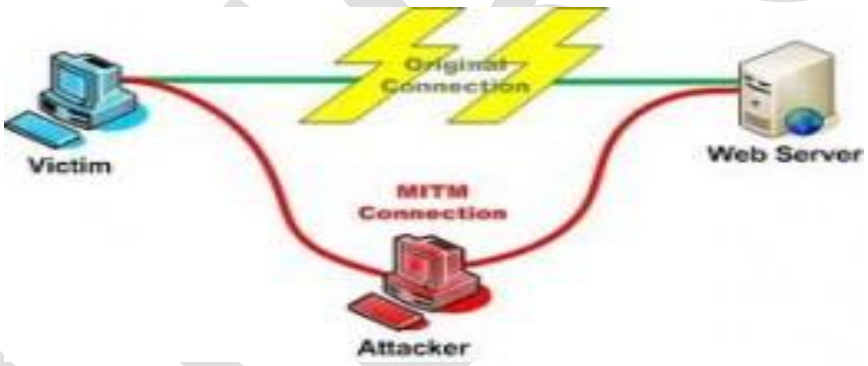

Figure 1. Man-in-the-middle attacks

This is a technique that takes advantage of a weakness in the TCP/IP protocol stack, and the way headers are constructed. Hijacking occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange.[2][7] When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-middle attacks as shown in the Figure1 say that someone assuming your identity in order to read your message. The person on the other end might believe it is you, because the attacker might be actively replying as you, to keep the exchange going and gain more information.

C.Trojans

These are programs that look like ordinary software, but actually perform unintended or malicious actions behind the scenes.[3][5] Most remote control spyware programs are of this type. The number of Trojan techniques is only limited by the

attacker's imagination. A torjanizes file will look, operate, and appear to be the same size as the compromised system file. The only protection is early use of a cryptographic checksum or binary digital signature procedure.

D.Denial-of-Service attack (DoS)

A denial of service attack is a special kind of Internet attack aimed at large websites. It is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic and as shown in Figure 2. Denial of Service can result when a system, such as a Web server, has been flooded with illegitimate requests, thus making it impossible to respond to real requests or tasks. Yahoo! and e-bay were both victims of such attacks in February 2000. A Dos attack can be perpetrated in a number of ways[5].

Figure 2. DOS attack over

III. ATTACKS IN AD-HOC NETWORKS

Classes of attack might include passive monitoring of communication, active network attack, close –in attack, exploitation by insiders and attacks through the service providers. Information system and networks offer attractive targets and should be resistant to attack from full range of threat agents, from hackers to nation states.A system must be able to limit damage and recover rapidly when attacks occur.There are different types of attacks in AD-HOC networks but the following attacks were only considering

1. Black hole attack
2. Wormhole attack

A. Black hole attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes. This is called black hole attack and it is a "passive" and a simple way to perform a Denial of Service. [1][7]The attack can be done selectively (drop routing packets for a specified destination, a packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

A Wireless ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. Mainly, there are two solutions for this attack. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. Computer simulation shows that compared to the original ad hoc on-demand distance vector (AODV) routing scheme; the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.

B.Wormhole attack

The wormhole attack is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission, or an optical link. [2][7]The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved.In wormhole attacks, the attackers tunnel the packets between distant locations in the network through an in-band or out-of-band channel. [4][5]The wormhole tunnel gives two distant nodes the illusion that they are close to each other.

IV. SYSTEM ANALYSIS

A. Existing System

A number of secure routing schemes have been brought forward**.** MASK is based on a special type of public key crypto system, the pairing-based cryptosystem, to achieve anonymous communication in MANET.

B.AODV

It is a routing protocol for MANETs and other wireless Adhoc networks. It establishes a route to a destination only on demand. [2][3]The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination. The connection setup delay is lower.

One disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.

C. MASK

It offers the anonymity of senders, receivers and sender-receiver relationships in addition to node unlocalability and untrackability and end to end flow untraceability. MASK is based on a special type of public key crypto system, the pairing-based cryptosystem, to achieve anonymous communication in MANET. MASK requires a trusted authority to generate sufficient pairs of secret points and corresponding pseudonyms as well as cryptographic parameters. MASK is quite expensive and may be vulnerable to key pair depletion attacks.

D.Proposed System

An efficient privacy maintain routing protocol USOR has been proposed that achieves content unobservability by employing anonymous key establishment based on group signature. The setup of USOR is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server. The unobservable routing scheme USOR aims to offer the following privacy properties.

E.Anonymity

The senders, receivers, and intermediate nodes are not identifiable within the whole network, the largest anonymity set.

F.Unlinkability

The linkage between any two or more IOIs from the senders, the receivers, the intermediate nodes, and the messages is protected from outsiders. Note linkages between any two messages, e.g., whether they are from the same source node, are also protected.

G.Unobservability

Any meaningful packet in the routing scheme is indistinguishable from other packets to an outside attacker. Not only are the content of the packet but also the packet header like packet type protected from eavesdroppers. [6]And any node involved in route discovery or packet forwarding, including the source node, destination node, and any intermediate node, is not aware of the identity of other involved nodes (also including the source node, the destination node, or any other intermediate nodes)[7].

V. SIMULATION RESULT

A. Malicious Mode of Transmission

When the packets were transferring from source node to destination node through the intermediate nodes where malicious node was introduced in the network. This leads to black hole attack and the packets get lost as shown in the Figure 3. The black holes refer to places in the network where the incoming or outgoing packet is silently discarded without informing the source that the data did not reach its intended recipient.

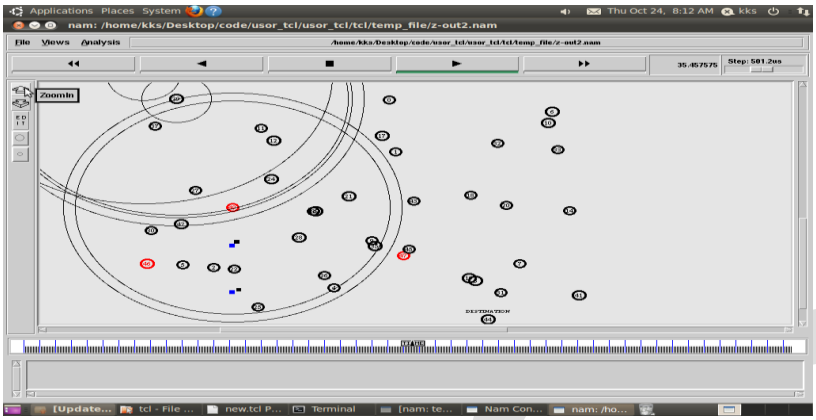

Figure 3.Packet loss in the network

B.USOR Mode of Transmission

Different keys were generated by RSA algorithm for encryption and decryption that are private key, public key and group ID.

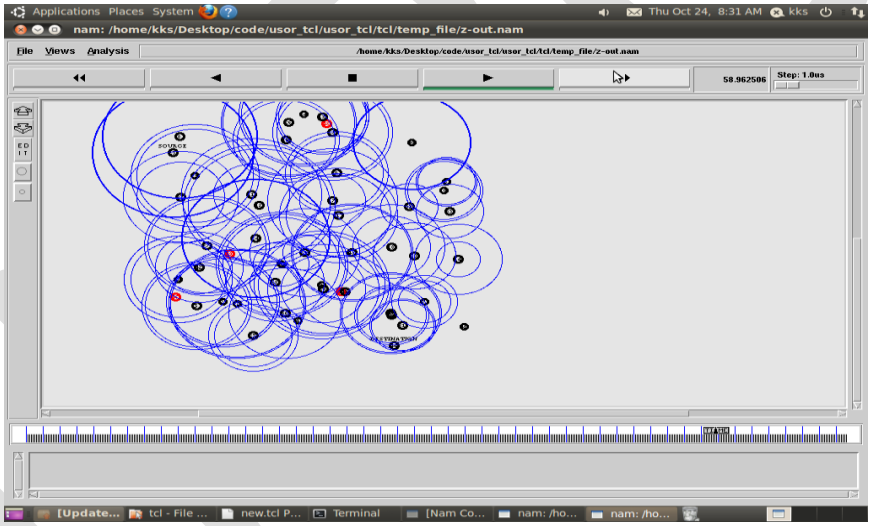

Figure 4. Prevention of attack using USOR.

Initialising the nodes as two types, leader node and normal node. Nodes generate hash code by using sha-1 algorithm and encrypting that code with public key then transmitting it to destination. Destination node can verify that encrypted message by using the private key and as well as group ID.

VI. CONCLUSION

An unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks is proposed. The design of USOR offers strong privacy protection completes unlink ability and content unobservability for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The protocol on ns2 has been implemented and examined performance of USOR, which shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

ACKNOWLEDGMENT

Future work along this direction is to study how to defend against wormhole attacks, which can be prevented with USOR and also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation. In black hole attack prevention, RREQ was only encrypted but in future when avoiding wormhole attack both RREQ and RREP were encrypting.

REFERENCES:

[1].Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba(2005), " SDAR:A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks", Vol.3779,No.3,pp,343-350.

[2].Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons,Abraham Flaxman(2000), "Sybil Guard:defending against sybil attacks viasocial Networks",Vol.33,No.7,pp,320-355

[3].Jiejun Kong, Xiaoyan Hong(2007),"ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks", Vol.41,No.1,pp,888-902.

[4].Karim El Defrawy and Gene Tsudik(2004),"ALARM:Anonymous Location-Aided Routing in Suspicious MANETs",Vol.28,No.3,pp,230-255.

[5].Pfitzmann.A and Hansen.M (July 2000),"Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology draft",Vol.45,No.6,pp,132-149.

[6].Stefaan Seys and Bart Preneel(2003),"ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks". Vol.2482,No.5,pp,54-68.

[7].Yanchao Zhang, Wei Liu and Wenjing Lou(2007),"Anonymous Communications in Mobile Ad Hoc Networks',Vol.13,No.2,pp,569-582.