International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 10, October-2014, pp: (1-5), Impact Factor: 1.296, Available online at: www.erpublications.com

Various Solutions for Security in MANET A Review

Sumeer Kumar, Sumit Kumar

Abstract: In this manuscript, the authors have described the various possible solutions for Security in MANET Systems. Mobile Ad-hoc Networks are unplanned, self-organizing networks composed of mobile nodes that utilize mesh networking principles for interconnectivity. Routing in ad hoc networks is a very challenging issue due to nodes mobility, dynamic topology, frequent link breakage, limitation of nodes memory, battery, bandwidth, and processing power and lack of central point like base stations or servers. Mobile ad hoc network (MANET) is an autonomous system of mobile nodes. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These cause extra challenges on security. In this paper, evaluation of prominent on-demand routing protocol i.e. AODV, MAODV, RAODV has been done by varying the network size. An effort has been carried out to do the performance evaluation of these protocols using random way point model. The authors have introduced the security issues specific to MANETs and present a detailed classification of the attacks/attackers against these complex distributed systems. Then we discuss various proactive and reactive solutions proposed for MANETs. We outline secure routing solutions to avoid some attacks against the routing protocols based on cooperation between nodes. We also give an overview of intrusion detection in MANETs and indicate the nature of IDSs that have been proposed for MANETs in the past decade.

Keywords: MANET, security, solution, network.

Introduction

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table). MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

Multi-hop relays date back to at least 500 BC. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. Much research has been done to counter and detect attacks against existing MANET routing protocols, including work on secure routing protocols and intrusion detection systems. However, for practical reasons the proposed solutions typically focus on

a few particular security vulnerabilities since providing a comprehensive solution is non-trivial. If we are to develop more general solutions we must first have a comprehensive understanding of possible vulnerabilities and security risks against MANETs. This is the main goal of this chapter. Section 2 presents the specific vulnerabilities of MANETs and the fundamentals of an exemplar routing protocol (AODV) to help understanding of the attacks given in Section 3. An overview of security solutions proposed to prevent and detect attacks on MANETs is presented in Section 4. Finally, ideas for future research are given.

Security Threats in MANET

The wireless Channel is accessible to both legitimate network users and malicious attackers. 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

Charter for Working Group

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion or other factors.

Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features.

Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol (RMP)

- Proactive MANET Protocol (PMP)

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed.

The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues.

The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

Importance of Network Security Goals

In providing a secure networking environment some or all of the following services may be required:

Confidentiality:

Ensures that the intended receivers can only access transmitted data. This is generally provided by encryption. Two types of encryption are commonly used (a detailed description of these is outside the scope of this report).Symmetric Encryption, where 2 nodes share a key (e.g. - DES, AES). Any data transmitted between the nodes is encrypted using this key. This key must be provided to the nodes over a secure channel. Symmetric encryption generally requires less computational resources than public key encryption. Public Key Encryption, where all nodes participating generate a public\private key pair pubKn/privKn. The node makes its public key pubKn available to all nodes. If other nodes wish to send data to node n, they encrypt their data using pubKn, safe in the knowledge that it can only be decrypted by n's private key privKn, which only node n knows.

Non-repudiation:

Ensures that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. Non-repudiation requires the use of public key cryptography to provide digital signatures. A trusted third party is required to provide a digital signature.

Availability:

Ensures that the intended network security services listed above are available to the intended parties when required. The availability is typically ensured by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocols.

Integrity:

Ensures that the data has not been altered during transmission. The integrity service can be provided using cryptographic hash functions along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

Authentication:

Both sender and receiver of data need to be sure of each other's identity. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates. Details of the construction and operation of digital signatures can be found in RFC2560.

MANETs Security Problem and Proposed Solution

As we are aware of that MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets or impersonate a node. This violets the network's goal of availability, integrity, authentication and nonrepudiation. Compromised nodes can also launch attacks from within a network. Most proposed routing algorithms today do not specify schemes to protect against such attacks. We give below methods that are pertinent for authentication, key distribution, intrusion detection and rerouting in case of Byzantine failures in MANETs.

Cryptography

Often, the sender/receiver is an organization. The goal of cryptography is to split a cryptographic operation among multiple users so that some predetermined number of users so that some predetermined number of users can perform desired operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and / or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key. The power to sign should then be shared, to avoid abuse and to guarantee reliability.

Decentralized authentication of new modes

Two nodes authenticate each other using signed unforgeable certificates issued by virtual trusted CA. Multiple nodes will function collectively as a CA. Authority and functionality of an authentication server is distributed across k nodes that collaboratively serve and provide authentication services.

Intrusion detection in manets

An effective IDS is a key component in securing MANETs. Two different methodologies of intrusion detection are commonly used: anomaly intrusion detection and misuse intrusion detection. Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misused detection systems can not detect new types of attack. Hybrid systems using both techniques are often deployed in order to minimize these shortcomings.

Per-packet and per-hop authentication

A new node has to be initially authenticated by each of its neighbors to join the network. Once that has been accomplished, each packet sent by the node to its one-hop neighbor is authenticated by the neighbor using a packet authentication tag. The one-hop neighbor then replaces the tag with its own authentication tag and forwards the packet to its neighbor. This next neighbor verifies the new authentication tag as coming from its immediate neighbor and the process is repeated iteratively until the packet reaches its destination. Therefore, each packet is authenticated at every hop.this scheme has the advantage that is resistant to denial of service (DoS) attacks and sessions hijacking attacks such as man-in-the-middle attack.

Conclusions

The authors try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. MANETs consists of mobile nodes interconnected by multi hop communications paths or radio links. A MANETs consists of mobile platforms known as nodes, which are free to move at any speed in any direction and organize themselves randomly. The nodes in the network function as routers, clients and servers. These nodes are constrained in power consumption, bandwidth and computational power. Because of this unique characteristics and constraints traditional approaches to security are inadequate in MANETs. Traditional authentication, key distribution and intrusion detection methods are often too inefficient to be used in resource constrained devices in MANETs. In this paper we propose to combine efficient cryptographic techniques and a distributed intrusion-detection system. We also propose to use distributed Certifying Authority (CA) along with per-packet and per-hop authentication for addressing the related security issues.

References

[1]. G.V.S. Raju and Rehan Akbani " Some security Issues in Mobile Ad- hoc Networks" in proceedings of the cutting Edge Wireless and IT Technologies Conference, Nov. 2004.
[2]. D. Remondo " Tutorial on Wireless Ad-hoc Networks" HET-NETs '04: Second International Working Conference in Performance Modelling and Evaluation of Heterogeneous Networks.
[3]. David Blount, "A study of Mobile Ad-Hoc Network Architectures and Technologies" National University of Ireland, Cork, April 2004.-
[4]. H Yang, H.Y.Luo and F.Ye, "Security in Mobile ad hoc Networks: challenges and Solutions" University of California, 2004. IEEE Wireless communications.11 (1), pp 38-47.
[5]. C.E.Perkins and P. Bhagwat (Oct 1994) ―Highly dynamic destination-sequenced distance vector routing for mobile computers, Comp, Comm. Rev., pp 234-44.
[6]. Belding-Royer, E.M. and C.K. Toh, (1999). A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communication magazine pp:46-55.
[7]. M. Frodigh, P. Johansson, and P. Larsson(2000)―Wireless ad hoc networking: the art of networking without a network, Ericsson Review,No.4, pp. 248-263.
[8]. Hu Y.-C., Perrig A., Johnson D.B., "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", In Proc. of the ACM Workshop on Wireless Security, 2003.
[9]. Karlof C., Wagner D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, pp. 293-315, 2003.
[10]. Hu Y.-C., Perrig A., Johnson D.B., "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", In Proc. of INFOCOM, 2003.