Security and Service Discovery Issues in Mobile Ad-hoc Networks

[1]Rutvij Jhaveri, [1]Kruti Dangarwala and [2]Neha Bhanot
[1]*Department of Computer Engineering and Information Technology, SVMIT, Bharuch, India*
[2]*Department of Information Technology, SVMIT, Bharuch, India*

Abstract—The world is going wireless and the user-services are being mobile. With the characteristics like self-creation, self-organization and self-administration, Mobile Ad-hoc Networks (MANETs) have become a great asset to this wireless world. MANETs are infrastructure-less and autonomous. This paper touches some major technical issues like security and service discovery, and their possible solutions for MANETs.

Keywords: MANET, Protocols, Security, Service Discovery, Solutions

I. INTRODUCTION

A MANET is a self configuring network formed by mobile hosts having wireless communication devices (Figure-1). Main features of MANET are multihop and mobility. It can be standalone or can be connected to Internet. As communicating nodes might be out of range, the nodes must be able to relay traffic. All the nodes in MANET use same frequency spectrum or physical channel. Therefore, MAC plays an imperative part in synchronizing channel access among the nodes. They are used in sensor networks, military operations, disaster recovery, medical support, e-commerce, vehicular traffic and accident guidance, ad-hoc communication, conferences, multi-user games, robotic pets, biological detection, mobile workspace, rescue operations, cellular network and in other vital applications.

II. MANET PROTOCOLS

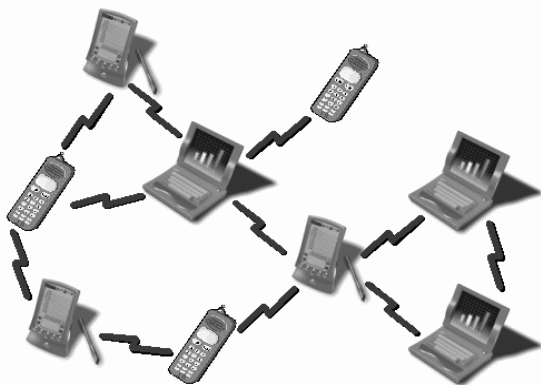The protocols are generally classified as Reactive, Proactive and Hybrid.

Fig. 1: Mobile Ad-hoc Network

A. Reactive Protocol

This type of protocol reacts on demand by flooding a query. It determines route if and when needed. The source, here, initiates the process of finding of the route. Therefore, the routing overhead is less, but the delay for discovering the route is more. Also, excessive flooding may cause network clogging; although this has been shown to be efficient, at least for some MANETs. Example of one such protocol is Ad hoc On-Demand Distance Vector Routing (AODV).

B. Proactive Protocol

This type of protocol is also called table-driven keeps route constantly updated. It frequently maintains lists of destinations and routes by distributing routing tables all over the network. The routes are established based on continuous control traffic and they are always available. The main flaws are slow reaction on restructuring and malfunctioning, and overhead created by control traffic. Examples of such protocol are OLSR and DSDV.

C. Hybrid Protocol

It is the combination of some selected features of reactive and proactive protocol. Example of such protocol is Zone Routing Protocol (ZRP).

III. CRITICAL ISSUES AND POSSIBLE SOLUTIONS

In MANET, there is no need for an adversary to get the physical access to visit the network. Once the adversary is in the radio range of any other nodes, it can communicate with those nodes in its radio range and thus connect to the network automatically. Therefore, Wireless channels are not as trustworthy as wired one. Also, they experience interference, limited security, fading and path loss. The wireless links between mobile nodes in MANET are not consistent as energy supply for the wireless nodes is limited and the mobility of the nodes. Though MANET offers some inimitable benefits compared with WLANs and cellular network, there are also some and challenges in this field.

A. Security

MANET pretense a number of challenges to security solutions due to their diverse resources, severe resource constraints, unclear line of defense, shared wireless

medium, dynamic network topology and wireless shared medium. Compromised nodes behave very well until they are compromised. Threats from compromised nodes inside the network are far dodgier than the attacks from outside the network as these attacks are much tougher to spot because they come from the compromised nodes. Problem detection becomes even more difficult as MANET doesn't have any centralized administration facility, such as server. Trust management is also a severe issue because of lack of centralization. MANET security possesses some challenges like privacy, authenticity, availability and integrity.

1. Attacks on mobile Ad-hoc network

MANET is prone to two types of attacks: Internal and external. Internal attacks in which the adversary wants to get access of the network by taking part in the network activities. It uses the current node as a basis to conduct its malicious behaviors. Therefore, internal attacks are more harmful than external attacks. In external attacks, the attacker causes traffic congestion or disturbs nodes by denying services:

- By altering the sequence number in the control message field, malicious nodes may cause Denial of Service (DoS) attacks or redirection of traffic.
- DoS attack can also be launched by altering the source routes in the packet headers.
- Routing information propagation can be blocked by attack on routing protocols.
- To disturb the packet transmission along the predefined path, attacker attacks on packet forwarding.
- To disturb a working route, attacker may generate a bogus route error or to create the wrong impression on others, it may suppress the error.
- A node may represent its wrong identity and attacks by spoofing which is called impersonation.
- Eavesdropping attack obtains some confidential information like public key, private key or passwords.
- Some other attacks intend to get the control over the nodes themselves by some unrighteous way and then utilize the compromised nodes to perform further wicked actions.

2. Possible solutions to security issues

To achieve security in MANET stability against attacks should be the top priority. There must be a guarantee for discovery of correct route. The network topology

should be kept confidential. Also, ability to detect a malicious node is an utmost requirement.

- Use of symmetric and asymmetric key algorithm as well as secret public key.
- Key management by threshold cryptography, password-based group system and self-organized public key management.
- Protecting privacy by framework based on constantly changing pseudonyms.
- Trusting device instead of owner called Key Pre-Distribution Infrastructure (KPI).
- Secure packet forwarding in which every node has the role to keep an eye on its neighbors.
- Determining the spot of a breakdown in a network by algorithms called fault localization technique.
- By collecting end-to-end measurements for longer paths, analyzing loss and delay measurements.
- Token Based Cooperation Enforcement in which tokens required to participate in the network.

B. Service Discovery

Service discovery deals with how network devices find out what sort of services exist in the network. Service discovery permits devices to automatically trace network services. It also allows devices to publicize their own capabilities to the rest of the network. Due to the resource constraints of nodes and dynamic characteristics of network, timely service discovery has been a great challenge for MANET. The challenges are to find services dynamically for wireless devices, to enable service discovery in a huge MANET.
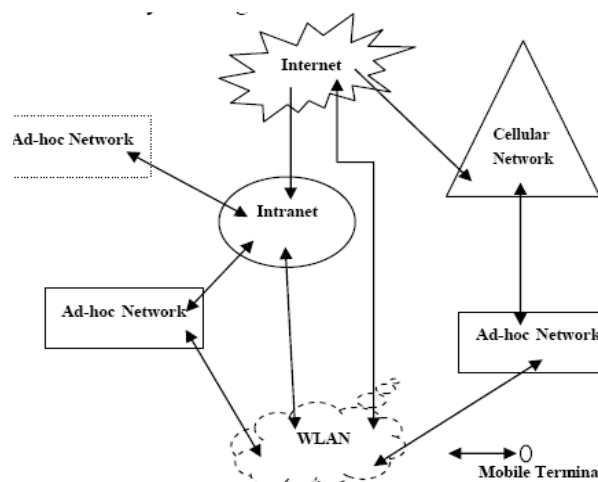

Fig. 2: Architecture of MANET

As Intranet and Internet connectivity is the main source of service (Figure-2), the main challenge is to bridge MANETs with infrastructure-based networks.

1. Possible service discovery solutions

Due to ubiquitous networking, MANETs are in the center of pervasive computing. But most of the existing solutions mainly suited for small-scale MANETs. Some proposals to the service discovery are:

- On-Demand Multicast Routing Protocol (ODMRP) is very effective and efficient in most simulation scenarios.
- Decentralized discovery solutions like push-based discovery and pull-based discovery are pretty effective though they have drawback of network flooding.
- To make the discovery protocol more scalable, a distributed set of directories are set up over gateways which are responsible for a spatial area for a cell.
- For large MANET and reducing utilization of resources and traffic, directories should be further distributed dynamically on a centralized architecture as a virtual network.
- In the hybrid network, a gateway directory holding description of services existing in all the networks and publicizes itself to the networks it links to.

IV. CONCLUSION

As mobile devices and users are increasing day by day, there are lots of challenges still left in designing best solution for MANETs. In this paper, we have examined some basics of MANET and we have explored two of the hottest issues in the MANET like security and service discovery. This paper also overviews some possible solutions to the attacks as well as schemes for making efficient discovery of services in different kind of MANETs.

REFERENCES

[1] Nishu Garg and R.P.Mahapatra: MANET Security Issues. In *International Journal of Computer Science and Network Security*, Pages 241-246, August 2009.

[2] Gene Tsudik1: Some Issues in WSN, MANET and Cellular Security http://moss.csc.ncsu.edu/~mueller/esns07/tsudik.pdf

[3] Wenjia Li and Anupam Joshi: Security Issues in Mobile Ad Hoc Networks- A Survey http://www.cs.umbc.edu/~wenjia1/699_report.pdf

[4] Refik Molva and Pietro Michiardi: Security in Ad hoc Networks http://citeseerx.comp.nus.edu.sg/viewdoc/summary?doi=10.1.1.14.4597

[5] Aqeel-ur-Rehman: Management of MANET Security Issues http://cruc.khi.nu.edu.pk/Presentations/Management_of_MANET_Security_Issues.pps

[6] Cristian Tuduce and Thomas Gross: Resource Monitoring Issues in Ad Hoc Networks http://citeseerx.comp.nus.edu.sg/viewdoc/summary?doi=10.1.1.5.5540

[7] B Sathish Babu: Security Issues in MANETS http://pet.ece.iisc.ernet.in/sathish/SecurityinAdhocNetworks.pdf

[8] Hongqiang Zhai, Jianfeng Wang, Xiang Chen and Yuguang Fang: Medium access control in mobile ad hoc networks: challenges and solutions http://citeseerx.comp.nus.edu.sg/viewdoc/summary?doi=10.1.1.60.9799

[9] Chunglae Cho and Duckki Lee: Survey of Service Discovery Architectures for Mobile Ad hoc Networks http://folk.uio.no/paalee/referencing_publications/ref-sd-cho-cice05.pdf

[10] Franc̨oise Sailhan, Val´erie Issarny: Scalable Service Discovery for MANET http://www-rocq.inria.fr/arles/doc/percom05.pdf