Available online at http://acfa.apeejay.edu

APEEJAY JOURNAL OF COMPUTER SCIENCE AND APPLICATIONS

ISSN:0974-5742(P)
Vol. 2, January 2014

A Survey on Routing Protocols and Vulnerabilities in Mobile Ad-hoc Network (MANETS)

Gagandeep Singh *
Assistant Professor, Department of CSE,
Sri Sai Institute of Engineering & Technology, Manawala, Amritsar

Abstract

Mobile ad hoc network (MANET) is composed of a collection of mobile nodes which are movable. Therefore, dynamic topology, unstable links, limited energy capacity and absence of fixed infrastructure are special features for MANET when compared to wired networks. MANET does not have centralized controllers, which makes it different from traditional wireless networks (cellular networks and wireless LAN). Due to these special features, the design of routing protocols for MANET becomes a challenge One of the main issues in MANET routing protocols is development of energy efficient protocols due to limited bandwidth and battery life. In this paper we will discuss about few energy-efficient routing protocols which will help in reducing power consumption as MANET is typically based on battery power Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it then address the possible solution to protect the security mechanism, which involve Availability, integrity, authentication and non repudiation. Finally we survey the current security solutions for the mobile ad hoc network.

Index Terms- MANET, Power utilization , routing, attacks.

1. Introduction

In circumstances where mobile telephony as we know it is not possible or difficult, perhaps internet technology can be of help. The dependency on a costly telecom infrastructure could thereby be decreased, which would be quite welcome considering the current situation in the telecom world. The technology that is to make this possible is MANET, or Mobile Adhoc Networking. The solution lies in the mobile device itself.

One important aspect of ad-hoc networks is power efficiency since only a simple battery provides nodes independence. Thus, minimizing power consumption is a major challenge in these networks. Wireless Ad-hoc Networks operates without a fixed infrastructure. Mobility, multihop, large network size combined with device heterogeneity bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge [1]. Power consumption is also one of the most important performance metrics for wireless ad hoc networks, it directly relates to the operational lifetime of the networks.[2] Mobile elements have to rely on finite source of power while battery technology is improving over time, the need for power consumption will not reduce. This point will have a harmful effect on the operation time as it will have on the connection quality and bandwidth In MANETs, every node has to perform the functions of a router. So if some nodes die early due to lack of power so that the network becomes disjointed, then it may not be possible for other nodes in the network to communicate with each other. In the Wireless Ad-hoc Networks, battery replacement may not be possible. So as far as power consumption concerned, we should try to save power while maintaining high connectivity. Overall performance becomes highly dependent on the energy efficiency of the algorithm. Energy consumption is one of the most important performance metrics for wireless ad hoc networks because it directly relates to the operational lifetime of the network. [3].

Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network acts both as host and a router and must therefore is willing to forward to packets for other nodes. Application such as military exercises, disaster relief, and mine site operation may benefit from adhoc networking, but secure and reliable communication is a necessary pre- requisite for such applications.

MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered.[4]. The main factors of routing protocols consume maximum power are as following: [5]

2. Mobile Adhoc Networks

2.1. Introduction

Mobile Adhoc Network (MANET) is a collection of in- dependent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. These networks are fully distribute, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust.
The characteristics of these networks are summarized as follows:

- Communication via wireless means.
- Nodes can perform the roles of both host and router
- No centralized controller and infrastructure.
- Intrinsic mutual trust.
- Dynamic network topology.
- Frequent routing updates.

2.2 Advantages and Applications

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

Some of the applications of MANETs are

- Military or police exercises.
- Disaster relief operations.
- Mine cite operations.
- Urgent Business meetings.

3.1 Description

There are some ultimate goals regarding security solutions with respect to Mobile ad hoc networks or we can say there are some security services which should be fulfill in order to enforce security like authentication, confidentiality, integrity to mobile users, we also use another term for them CIA which should be fulfill. In order to achieve goal in security, Table 2.1 shows the security issues with respect to each layer. In this thesis we will consider a fundamental security problem in MANET[6].

Multihop connection established between two nodes in mobile ad hoc network through two steps:
1. It ensuring one-hop connection through link-layer protocols like wireless medium access control (MAC).
2. Through network layer it will extend connection between multiple hops and provide routing and data forwarding protocols.

3.2 Challenges

One of the fundamental vulnerability of MANETs comes from open peer-to-peer Architecture. In case of wired networks there are dedicated routers but in case of mobile ad hoc network each mobile node acts as a router in order to forward packets for one node to other node. In mobile ad hoc networks there are no boundaries of wireless channel; it is accessible to both network users as well as to malicious attackers. According to security information with respect to MANET network are vulnerable compromises or physical capture, especially at the end of low-end devices due to weak protection. Intruders enter into the network and poses weakest link and incur a domino effect of security in the network. According to wireless channel is concerned bandwidth is one of constrained and use to share among multiple different network nodes. There is also one more restriction that is computation capability; like low-end devices for e.g. PDAs, can hardly perform low computation due to this way they usually use asymmetric cryptographic computation which is bit low complex, because mobile devices have very limited energy resources due to this way mostly mobile devices powered by batteries.

3.3 Routing protocol description

There are basically there kind of routing protocols which are:

- Table driven routing protocols

In these routing protocols each node in the network maintains the complete routing information of the network by occasionally updating the routing table, so when a node needs to send some data or information, so there is no any kind of delay for discovering the route in the whole network. This type of routing protocols approximately works the same way as the wired network routing protocol works. The able driven protocols are DSDV and WR

- On-Demand routing protocols

While in this kind of routing protocols, a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used. These routing protocols are AODV, DSR and TORA.

- Hybrid routing protocols (ZRP)

In this type of routing protocol is the combination of the above two categories. In which nodes belonging to a particular geographical area or within a certain detachment from an anxious node are said to be in routing area and uses table driven routing protocol. Communication between nodes in different areas will rely on the source initiated or on-demand routing protocols. This routing protocol Include ZRP.

3.3.1 AODV

AODV using a classical distance vector routing algorithm. It is also shares DSR's on-demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes. One of the best features of AODV is to provide broadcast, unicast, and multicast communication. During route discovery algorithm AODV uses a broadcast and for reply it uses unicast.

3.3.2 DSR

The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages like AODV, and due to this way it reduces network bandwidth overhead, and also avoids large routing updates as well as it also reduces conserves battery power. In order to identify link layer failure DSR needs support from the MAC layer. It is consist of the two network processes, Route Discovery and Route Maintenance. Both of neither AODV nor DSR guarantees shortest path.

3.3.3. TORA

The TORA is an adaptive, scalable and efficient distributed routing algorithm. It is mainly designed for multi-hop wireless networks as well as highly dynamic mobile environment. It is also called source-initiated on-demand routing protocol. It is also use to find multiple routes from source to destination node. One of the main features is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. It has three basic functions: Route maintenance, Route erasure and Route creation.

4. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

4.2. Threats from Compromised nodes Inside the Network

In the previous subsection, we mainly discuss the vulnerability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network.

4.3. Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner. First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network . It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently. Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time.

4.4. Restricted Power Supply

While nodes in the wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems[10].

The first problem that may be caused by the restricted power supply is denial-of-service attacks. Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power.

4.5. Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network [8]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future.

5. Security Solutions to the Mobile Ad Hoc Networks

5.1. Security Criteria

We have discussed several routing techniques that potentially make the mobile ad hoc networks in secure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

5.1.1 Availability

It 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.

5.1.2 Integrity

It 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.

5.1.3 Confidentiality

Ensures that the intended receivers can only access transmitted data. This is generally provided by encryption.

5.1.4. Authenticity

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.

5.1.5. 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.

5.1.6. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

5.1.7. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should

Try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

5.2. Attack Types in Mobile Ad Hoc Networks

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types [9]

- External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

- Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

5.2.1. Denial of Service (DoS)

This active attack aims at obstructing or limiting access to a certain resource. This resource could be a specific node or service or the whole network. This will affect the availability security service mentioned above. The nature of ad-hoc networks where several routes exist between nodes and routes are very dynamic gives ad-hoc a built-in resistance to DoS attacks, compared to fixed networks. Security mechanisms for wireless ad-hoc networks should aim to provide all the security services listed above and prevent any of the attacks mentioned. However, due to the lack of infrastructure in an ad-hoc wireless network, typical wired-network implementations of the methods mentioned above may not be possible. Along with the general issues listed above, there are also other specific key issues and challenges for providing security in ad-hoc.

5.2.2. Impersonation

Here the attacker uses the identity of another node to gain unauthorized access to a resource or data. This attack is often used as a prerequisite to eavesdropping. By impersonating a legitimate node the attacker can try to gain access to the encryption key used to protect the transmitted data. Once the attacker knows this key, she can successfully perform the eavesdropping attack.

5.2.3. Eavesdropping

This attack is used to gain knowledge of the transmitted data. This is a passive attack, which is easily performed, in many networking environments. However using an encryption scheme to protect the transmitted data can prevent this attack.

5.2.4 Modification

This attack modifies data during the transmission between the communicating nodes, implying that the communicating nodes do not share the same view of the transmitted data. An example could be when the transmitted data represents a financial transaction where the attacker has modified the transactions value.

5.2.5. Attacks against Routing

The routing within ad hoc networks is more vulnerable to attack as each device itself acts as a router. An attacker can pose as a member node and incorrectly route packets to achieve an attack. Denials of service attacks are particularly easy doing this. Thus implementation of secure routing protocol is one of the challenges within ad hoc network. The use of IPSec to provide authentication, confidentiality and integrity is discussed in this report. By securing all IP traffic (or whatever network layer protocol is used), you are also securing outing.

5.2.7 Link Level Security

In wireless environment the links are susceptible to attacks where eavesdropper can intercept data packets. Physical barriers such as walls\rooms\&c. provide no barrier to wireless radio packets.

6. Conclusion

In this survey paper, we 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. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.

First we introduce the basics of the mobile ad hoc network. We then discuss some typical and dangerous vulnerabilities in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these vulnerabilities has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks.

References:

[1] Juan Carlos Cano and Pietro Manzoni., “A Performance Comparison of Energy Consumption for Mobile Ad Hoc Network Routing Protocols”, Proceeding of 8th International Symposium on Modeling, Analysis and Simulation of Computer & Telecommunication System 2000.

[2] Dhiraj Nitnaware and Ajay Verma, “Performance Evaluation of Energy Consumption of Reactive Protocols under Self-Similar Traffic”, International Journal of Computer Science & Communication, Vol. 1, pp. 67-71, 2010.

[3] H. Ehsan and Z.A. Uzmi (2004), “Performance Comparison of AdHocWireless Network Routing Protocols”, IEEE INMIC 2004. [4] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, “Security in mobile ad hoc networks: Challenges and solutions” (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[4] Yih-Chun Hu , Adrian Perrig, “A Survey of Secure Wireless Ad Hoc Routing”, IEEE Security and Privacy, v.2 n.3, p.28-39, May 2004

[5] D. Djenouri, L. Khelladi and A.N. Badache. “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, Communications Surveys & Tutorials, IEEE, Vol. 7, Issue 4, pp. 2--28, Fourth Quarter 2005.

[6] B. Schneier, *Secret and Lies, Digital Security in a Networked World,* Wiley, 2000.

[7] N.Vetrivelan and A.V.Reddy, 2008. “Performance Analysis of Three routing Protocols for Varying MANET Size”,Proceedings of the International Multi-Conference of Engineers and Computer Scientists.

[8] E.M.Royer and C.K.Toh, 1999. “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”,IEEE Personal Communications Magazine, 46-55.

[9] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *AdHoc Networks Technologies and Protocols (Chapter 9),* Springer, 2005.

[10] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30),* CRC Press LLC, 2003.

[11] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31),* CRC Press LLC, 2003.

[12] Gupta, Munish, Paramjeet Singh, and Shveta Rani. "Cross Layer Energy Efficient Protocols For Wireless Sensor Networks: A Survey.*",Apeejay Journal of Computer Science and Applications”,* Vol. 1, 2013, pp 27-32.