Security in Ad hoc Network

Pin Nie
Telecommunications Software and Multimedia Laboratory
Helsinki University of Technology
niepin@cc.hut.fi

Abstract

Due to the superior advantages, ad hoc networking technology is becoming a hotspot in both research and application areas. However, its inherent features also make it be more vulnerable to a wide range of attacks, since many traditional security mechanisms cannot be simply moved to ad hoc networks. In this paper, we presents possible attacks to ad hoc networks and defense solutions to handle them.

Keywords: security, ad hoc network, attacks, secure routing

1 Introduction

Ad hoc networks are a promising paradigm for easy communication, especially the wireless ad hoc network for mobile hosts (e.g. MANET [8]). Ad hoc networks requires no fixed infrastructure or any kind of central servers. All nodes in ad hoc manner usually have equivalent status in the services. Nodes are connected either directly if within the radio range or via the intermediary nodes, which relay messages as routers, for remote destinations. Frequent changes such as positions and available status of the nodes can be accepted without severely influence on the quality of services. The ad hoc networks can adjust its topology dynamically.

The pleasing characteristics above bring good benefits, for example, fast deployment, self-organize and great flexibility, surpassing other traditional networks. However, on the other side, these apple features raise big challenges to the security issue of the platform and service creation. For the five key attributes of security, i.e. availability, confidentiality, integrity, authentication and non-repudiation, each item must be carefully considered in ad hoc networks. The reduce of the threshold in building ad hoc networks removes the central control, maintaining and monitoring units, as well as the infrastructure. How to distribute these necessary functionalities to the improvising networks, without adding too much complexity to the structure and nodes is a difficulty question. Furthermore, the heterogenous environment in ad hoc applications can provide very limited reliable information to assess the situation and surrounding nodes.

Attacks from both external and internal nodes can easily affect the stability of the ad hoc networks. The degree of the influence depends largely on the active level of the malicious nodes. The time to recover the services relies on the detection of the mistakes or errors and responding policy. For example, an active bad relay node can cause a lot of packets loss and may disable the remote connections. If this relay node can be identified quickly and select other relay nodes, the attack would not be effective long.

Security discussion in this paper targets at the attacks, based on the ranking of the five attributes in the practical applications of ad hoc networks. In Section 2, I survey the possible attacks launched on the networks. Oriented from the attacks, the defense solutions and countermeasures are described

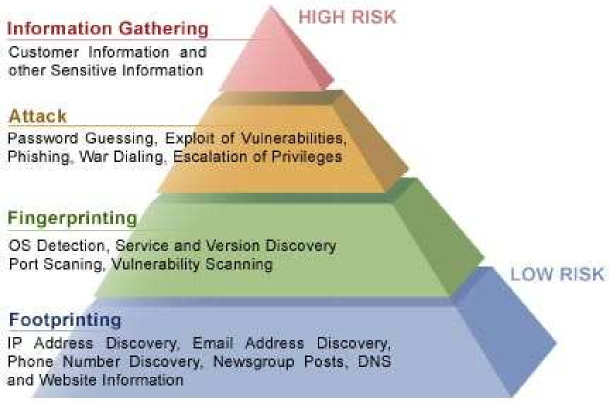
HIGH RISK
Information Gathering
Customer Information and other Sensitive Information
Attack
Password Guessing, Exploit of Vulnerabilities, Phishing, War Dialing, Escalation of Privileges
Fingerprinting
OS Detection, Service and Version Discovery Port Scaning, Vulnerability Scanning
LOW RISK
Footprinting
IP Address Discovery, Email Address Discovery, Phone Number Discovery, Newsgroup Posts, DNS and Website Information

Figure 1: Security assessment and testing provided by TrustCC

in Section 3. In Section 4, some new and novel ideas and suggestions concerning security in ad hoc applications are introduced. Finally, the conclusion is reached in Section 5.

2 Network Attacks

Network attacking is similar to playing chess. It is an intelligent game between hackers and warriors in the cyberspace. On the dark side in this game, people try their best to find other's vulnerabilities, plant the handy tools, wait for the chance and take the action for what they are seeking for. On the bright side, people keep looking after the existing systems, administrating the legal use, monitoring and detecting any misuse or misbehavior. In this section, security is discussed from the viewpoint of the attackers.

2.1 Objectives and targets selection

The attacks can be roughly divided into three categories, according to purposes. The first one is the illegal/invalid access to the resources for personal benefit, such as impersonating and masquerading. This does not lead to any serious consequence to the system usually, but increasing its workload. The second one is stealing. The private or confidential content is revealed to irrelevant parties or persons. Attacks include eavesdropping, snooping and interception. This still does not affect the running of the system much. But it causes a big trouble to the users and degrades the system to an *Untrusted Domain*, which spoils the service. The third case is the worst. The attackers target at either the content or the resources and make active operations. For the content, attacks include virus, fabricating/forging, replay stale messages and black hole. For the resources of the system, it could be DoS, worm and overflow. The system and service are definitely influenced and may be dropped or taken over by attackers. These attacks are often taken step by step. It is hard to detect any trace at the beginning when the risk is not high enough to alert people. The figure 1 gives an attacking risk pyramid to illustrate the situation. As we can see from the picture, attackers often start from gathering information of the target. After making analysis of the collected information, more active operations would be taken and more useful information can be obtained for further actions. The whole procedure is carried out step by step.

Many attacks involve combinations of vulnerabilities. Here is a list of the top 10 vulnerabilities, as of June 2000 [2]. We can see 4 of them are on the application programs, 3 on the communications protocol and mechanism, and 2 on the operating systems. It proves the strong security impact of the networking protocols.

- *A stack overflow attack on the BIND program,* used by many Unix and Linux hosts for DNS, giving immediate account access.
- *Vulnerable CGI programs on Web servers,* often supplied by the vendor as sample programs and not removed. CGI program flaws are the common means of taking over and defacing Web servers.
- *A stack overflow attack on the remote procedure call (RPC) mechanism,* used by many Unix and Linux hosts to support local networking, and which allows intruders immediate account access (e.g. DDoS).
- *A bug in Microsoft's Internet Information Server (IIS) Web server software,* which allowed immediate access to an administrator account on the server.
- *A bug in sendmail, the most common mail program on Unix and Linux computers.* Many bugs have been found in sendmail over the years.
- *A stack overflow attack on Sun's Solaris operating system,* which allows intruders immediate root access.
- *Attacks on NFS and their equivalents on Windows NT and Macintosh operating system.* These mechanisms are used to share files on a local network.
- *Guesses of usernames and passwords,* especially where the root or administrator password is weak, or where a system is shipped with default passwords that people don't bother to change.
- *The IMAP and POP protocols,* which allow remote access to email but are often misconfigured to allow intruder access.
- *Weak authentication in the SNMP protocol,* used by network administrators to manage all types of network-connected devices. SNMP uses a default password of ”public”.

Figure 2 shows us a general distribution. It tells that tentative scanning, failed login or frequent invalid operations, which can be found in the log files, could be a sign of attacks. Usually, central servers is more likely to be targeted due to the important functionalities and information convergence, such as mail server, web server, database, DNS server and so on.

2.2 Classifications of attacks

In the book [4], attacks on ad hoc wireless networks fall into a category tree grouped by different features, as shown in Fig. 3. Firstly, by operations, they are separated into **passive** and **active**. The first type may be the prestage of the later attacks. According to the carrier and underlying services, the active attacks are categorized to four layers and one general type. On the network layer model, every specific layer has its own features and primary services, which attract certain part of attacks. The more profound layer, the more important it means to the network. For example, attacks launched on the application layer may affect several applications. But it would tear down the whole network if the attack takes place in the network layer on routing service. No upper layer services can be built up at that moment. The paper [5] presents the misbehavior in ad hoc networks at MAC layer. Attacks in the general box are not associated with any specific layer, but services and applications. For example, DoS attack can be fired in application layer, transport layer and network layer, based on the target service.

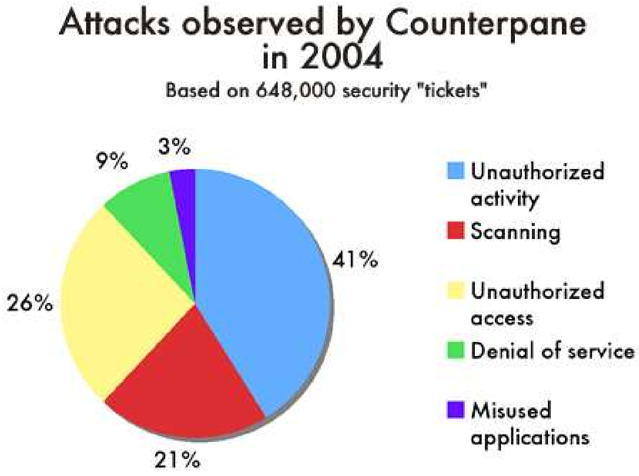

Figure 2: Attacks distribution (provided by Bruce Schneier)

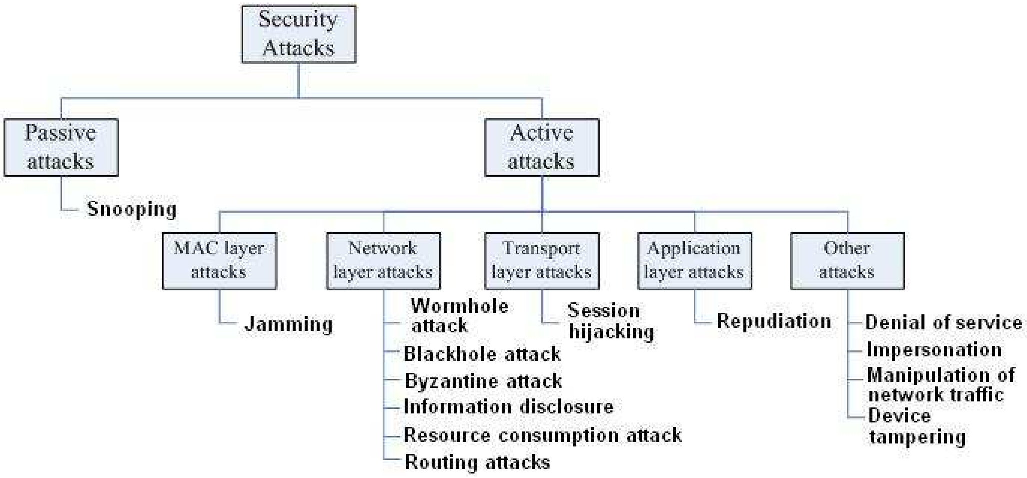

Figure 3: Classifications of attacks

However, the attack classification tree can be produced in another way by intentions, regarding to the objectives, such as invalid access, limited disturb and disable functions. This taxonomy makes it easier to capture the attacker's intention and track his/her actions. It is helpful in the defense, which I will talk in the next section.

2.3 Vulnerable Services

It is hard to give a ranking list of most vulnerable services, because of the fast pace of services creation and new bugs release. But by following the features of ad hoc network, we can still foresee a few easy security troubles. The first problem is the routing. Moreover, the topology changes frequently. Tampering with routing information can compromise the whole network. A secure routing solution is one of the major challenges within ad hoc network. The second is the link level security, the wireless ad hoc network uses radio to connect nodes. Radio transmission is susceptible to the interference and passive attacks. The first three security aspects availability, confidentiality and integrity are easily violated here. The third service is the key management and trust establishment. In the ad hoc networks, there is no trusted third party (e.g. CA) and central distributed credential. The cryptography and authentication required in other services are based on the key distribution protocol. So far to my best knowledge, a scalable and comprehensive key management mechanism has not yet been developed in ad hoc networks. The fourth issue concerns the privacy. Privacy may not be a service, but it is often required in many services. Spoofing of identity leads to privacy threats and may cause the chain reaction. In the ad hoc network, we lack other ways to identify the remote, due to the limited services available. The paper [7] gives a guidance view of the security within ad hoc networks.

3 Defense and Countermeasures

Based on the attacks analysis above, defense mechanisms and solutions are presented in this section. It covers three fundamental issues. The rest problems are left to the discussion part.

3.1 Secure routing

As I mentioned before, routing is an essential service in ad hoc network. It is critical to form and organize the topology and determine the connectivity of the network. There are a few types attacks mounted on the routing protocols [4].

- **Routing table overflow:** The adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network. The objective is to cause an overflow of the routing table and prevent the creation of entries to authorized nodes.
- **Routing table poisoning:** The compromised nodes send fictitious updates or modify genuine route update packets to other nodes. It may result in congestion or even inaccessible of the network.
- **Packet replication:** The malicious node replicates stale packets to consume resources, e.g. bandwidth and battery power (sleep deprivation attack) of other nodes.
- **Route cache poisoning:** Similar to routing table poisoning, an adversary can also poison the route cache to achieve objectives. It happens to on-demand routing protocol.
- **Rushing attack:** An adversary floods the received RouteRequest packet to the network, in order to take position in other nodes' routing table. It can take the man-in-the-middle attacks later on.

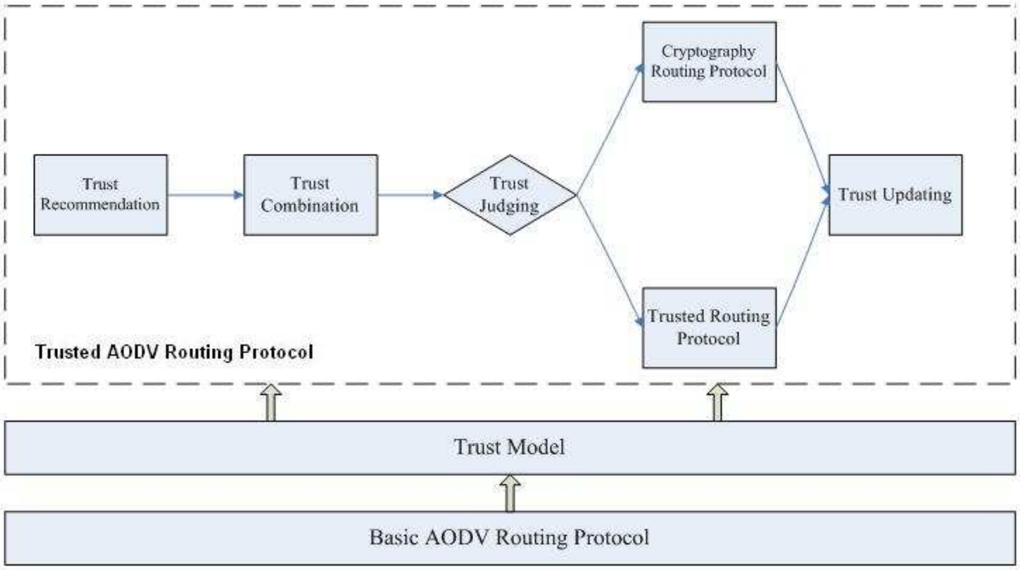

Figure 4: Framework of the Trusted AODV (TAODV)

In the paper [12], it suggests to use the redundancy property of ad hoc network to cope with the routing failures and attacks. *Diversity coding* takes advantage of multiple paths in an efficient way without message retransmission. The idea is to use more channels for error detection and correction. But it consumes more resources (e.g. memory) at the same time.

Paper [3] reviews the relationship between security and mobility, and make use of the mobility to set up security associations in mobile ad hoc networks. In the solution, each node maintain a local database of physical encounters with other node and trusted friends list. Note that the trust is assumed to be non-transitive, which means only one-hop direct connection is allowed. This policy takes advantage of proximity of mobile nodes. However, for the remote nodes, it still assumes a authority controlling network membership.

A trust model based routing protocol (TAODV) proposed in paper [9] explores the problem in another way. It constructs a framework of the trust AODV, as shown in Fig. 4. Simply speaking, this routing protocol is a knowledge-based edition of the original AODV. It records what the node experienced in the previous processes. The improvement is obvious, especially for *stable* ad hoc networks. But meanwhile, two negative effects are explicit as well. Firstly, it does not fit a frequent changing ad hoc network, due to the intensive computation. Too sensitive trust model makes it more vulnerable to DoS attack and fluctuation. Secondly, from its updating policy, it ignores a fact in social network that trust is built up slowly and dropped quickly. In other words, the mechanism is rather slow to detect sudden compromise of internal nodes in ad hoc network, which may be an important assumption in some use cases (e.g. battlefield).

3.2 Attacks detection

An Internet expert said: "The best way to cope with the failure of transmission is to accept it." It is the same when dealing with attacks. In practical applications, the availability is usually the most important. Too strict security solution would break this condition. Thus, the attacks detection should be always considered in ad hoc networks. The faster the attack can be detected, the sooner the system can be recovered, the less loss it may cost.

Intrusion Detection System (IDS) has been studied for many years, but only recently on the ad hoc networks. It is because the strict requirements posed on ad hoc IDS. First of all, the IDS should not

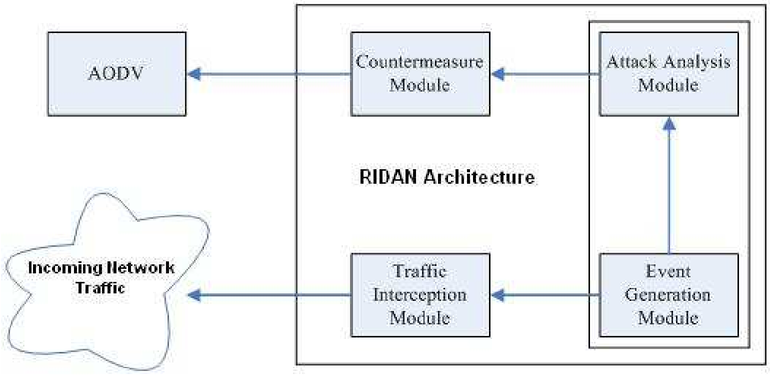

Figure 5: High-level architecture of RIDAN components [6]

make big changes on routing protocols to keep the performance and scalability. Second, it must be sensitive to the recognized attack patterns and able to accommodate the frequent changing environment in ad hoc networks. On the basis of the prerequisites, the paper [6] proposed a Real-time IDS for ad hoc networks. It applies the knowledge-based methodology to recognize the attack patterns and detect intrusion. Meanwhile, it utilizes timed finite state machines (TFSMs) to analyze network traffic. Every TFSM corresponds to an attack pattern. They are triggered by specific incoming packets and generate attack alarms, once a state transition sequence satisfying the predefined attack patterns is captured. Figure 5 shows the internal structure of this intrusion detection system.

In ad hoc networks, it is possible to distribute the attack detection functionality to all peers, which share the responsibility and cooperate with each other to achieve a secure system. The paper [1] presents such a cooperative intrusion detection system for ad hoc networks. In order to balance workload and reduce the resource consumption, it applies the cluster-based detection model, where a cluster of neighboring nodes can periodically, randomly and fairly elect a monitoring node for the entire neighborhood. For the attacks identification, the solution needs fine-grained statistics to produce certain rules. Though it overcomes the low efficiency at the initial stage in knowledge-based mechanisms, the rules have to be updated for different situations.

A few more advanced ideas are brought out recently to give a new direction of IDS. For example, peer-to-peer (P2P) mechanism can spread the suspect attacker nodes quickly and provide early warning for others. The main idea of P2P IDS is to build up cross fire for the full-directions covering. Theocratically, a fact is more communication helps to reveal conflicts, which are often a part of attacks or intrusions. Another idea orient from the attack taxonomy based on the intention, as I mentioned in the last section 2.2. In this way, the attacks can be predicted before the actual actions. However, this solution requires a detailed traffic log and precise attacks pattern descriptions. Otherwise, the false alarm would be a big problem. From these solutions, we can see a trend of IDS development, i.e. moving towards the early warning system (EWS).

3.3 Security standardization

In order to formalize the security establishment and relevant issues, security standardizations in ad hoc network is highly required. Paper [11] addresses several standardization areas for securing ad hoc networks. The areas include node configuration, key management, routing protocol security and intrusion detection. The standardization of these areas can minimize the misuse of the system and leave limited space for attackers. Furthermore, with the formal security document, problems can be easier identified. Currently, a few industrial standardization working groups (e.g. IETF MANET WG) are focusing on these areas.

4 Discussion

Security for ad hoc networks is still under active research. More improvements and solutions are being constructed and tested. Due to the volatile physical environment and dynamically changing topology, a strong voice suggests to build specific security suite according to different applications, such as device-to-device, device-to-people and people-to-people. The flexible security deployment can leverage the advantages and fit the situation better. For example, the paper [10] proposed a promising paradigm to establish secure association between digital elements. It would be very useful to build up sensor networks. One more argument is the choice between security-aware and attack-aware, either of which owns a strong ground to support. The first one stands for the secure platform, while the latter one put more emphasis on services. Still, it should be considered with the practical situations in my opinion.

Another useful concept is the *Roof Limits*, which means the node in the ad hoc network accepts only certain number of packets or information from any other nodes. For example, the node can accept 10 routing response at the most. In this case, the poisoning attacks on the routing table and flooding routing packets can be prevented efficiently. At worst situation, only 10 routing records in the table are bad ones. Furthermore, this strategy can avoid the overuse the high performance nodes in the ad hoc network, due to its fair load limits.

5 Conclusions

In this paper, possible attacks on ad hoc networks are introduced and analyzed in both ways from the attacker side and defender side. Based on the classification and description of attacks, defense and countermeasure are presented to handle the problems. Some typical solutions are provided as examples and novel ideas are identified. The advantages and disadvantages of these solutions are addressed for a clear view. The study of attacks can help us to find the direction of security, which would be useless if it is talked without any reason.

References

[1] Y. an Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147, Fairfax, Virginia, 2003. ACM Press.

[2] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley & Sons Inc, 2001.

[3] S. Capkun, J.-P. Hubaux, and L. Buttyan. Mobility helps security in ad hoc networks. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 46–56, Annapolis, Maryland, USA, 2003. ACM Press.

[4] C.Siva Ram Murthy and B.S.Manoj. *Ad Hoc Wireless Network: Architectures and Protocols.* Prentice Hall Ptr, 2004.

[5] L. Guang and C. Assi. Mac layer misbehavior in ad hoc networks. In *Proceedings of Canadian Conference on Electrical and Computer Engineering, 2005.*, pages 1103–1106, Montreal, Que., Canada, 2005. IEEE computer society.

[6] P. G. A. Ioanna Stamouli and H. Tewari. Real-time intrusion detection for ad hoc networks. In *Proceedings of World of Wireless Mobile and Multimedia Networks, 2005.*, pages 374–380, Montreal, Que., Canada, 2005. IEEE computer society.

[7] P. V. Jani. Security within ad hoc networks. At http://www.pampas.eu.org/Position_Papers/Nokia.pdf, 2002.

[8] D. K. Kim. A new mobile environment: Mobile ad hoc networks (manet), 2003.

[9] X. Li, M. R. Lyu, and J. Liu. A trust model based routing protocol for secure ad hoc networks. In *Proceedings of Aerospace Conference, 2004.*, pages 1286–1295, Hong Kong, China, 2004. IEEE computer society.

[10] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. At http://www.cl.cam.ac.uk/~rja14/duckling.pdf, 1999.

[11] R. Talpade and A. McAuley. Standardization areas for securing ad hoc networks. In *Proceedings of The 2002 45th Midwest Symposium on Circuits and Systems, 2002.*, pages 619–622, USA, Aug. 2002.

[12] L. Zhou and Z. J. Haas. Secure ad hoc networking. *IEEE Network*, 13:24–30, Nov. 1999.