Inter-Ing 2005 UNIVERSITATEA Petru Maior TÂRGU-MUREŞ

„INTERDISCIPLINARITY IN ENGINEERING"
SCIENTIFIC CONFERENCE WITH INTERNATIONAL PARTICIPATION,
TG. MUREŞ – ROMÂNIA, 10 -11 NOVEMBER 2005.

Security Issues in Wireless Distance Vector Routing Protocols

HALLER PIROSKA, GENGE BELA PETRU MAIOR UNIVERSITY

Key words: routing, security, wireless network

Abstract – Most of the ad-hoc wireless network routing protocol assume a trusted environment, mainly because securing communications between routers using conventional authentication methods (asymmetric cryptography, digital signatures, use of symmetric cryptography) are resource consuming. Secure routing protocols become of critical importance and have a lot of proposals to improvement security mechanisms. In this paper we will present the main security issues encountered in these environments and make a comparative study of the proposed mechanisms for securing the communication between wireless router nodes. Different kind of attack have different solution, and we try to select them to be combine in one solution without exceed de routing node capacities.

Introduction

An Ad Hoc Wireless network, opposed to a wireless network, cooperate to form a network without using any infrastructure [1], nodes are free to move, they can appear and disappear. The network is an autonomous system, an association of mobile nodes forward packet for each other [2]. These types of networks can find applicability in emergency rescue situations, military actions, conferences, sensor network, mainly where the setup of a communication infrastructure is not possible, or it would be only temporary and infeasible. They are used in situations where a communication between nodes must be set up quickly using limited or no administration at all. The nodes are terminal and routing node in the same time. The limited processing capacity, the wireless transmission effects, and the specific possibilities of attacks create significant challenges for routing protocols.

Distance Vector Routing assumes that every router holds a routing table of his own, where the best route, together with it's metric, for each known destination is stored. Thus, every node of the network must have an entry in his routing table for every destination in the Autonomous System [3]. Distance Vector protocols find the shortest path between nodes in a network through a „distributed implementation of the classical Bellman-Ford algorithm" [4]. These algorithms are frequently used in wireless networks because they do not require much memory or CPU power. An example of a popular Distance Vector algorithm is RIP [5], or it's follower RIPv2 [6,7].

There has been a large variety of protocols proposed for mobile Ad Hoc Wireless networks, some of them solving the counting to infinity problem (DSDV [8], WRP [9]), others concentrating on the security issues that appear in these environments (duckling [10], SEAD [11]), and some of them solving the slow convergence problem that is so vital in wireless networks ([8], [11]). This paper will only focus on the security issues regarding routing in wireless environments; it will describe the different kind of protocols proposed to prevent attacks in wireless networks.

Possible attacks on distance-vector protocols

Take in consideration the nature of the communication an attacker can infiltrate between two routers, it can record packages, it can easily replay them and can inject bogus information in the received messages, if the communication is not secured [12].

The purpose of creating more secure routing protocols is not to stop anyone from eavesdropping on information being passed from one router to another, but to create a trusting environment, a system where one can say for sure that the information received is from a trusted source.

The main forms of attacks that are found in any wireless environment are the following:

- denial of service
- router impersonation
- ignorance attack
- wormhole attack
- longer or shorter distance fraud („blackhole attack" for advertising distance=0)
- same distance fraud

In the next sections we will describe each of these attacks and overview the possibilities that lay ahead in defending against them.

Preventing attacks in wireless networks

Denial of Service attack

A denial-of-service (DoS) attack is characterised by an explicit attempt by attackers to prevent legitimate users of a service from using that service. The most frequently DoS attach in wireless networks are routing disruption, and resource consumption attacks, caused by injected packets. From a programmer's point of view, the creation of raw sockets [13] allows one to inject a package that may contain any information, it may contain parts of a valid package from the router's communication, it may contain authentication parts, the main idea is that it will keep the router busy.

In these kinds of situations, there are two possible ways to solve the problem:

1). Inform the system administrator that a rather large number of unidentified or invalid packages have been received on an interface

2). Do not apply additional security checks for packages that appear to be „sick".

For example, if a router receives a package with the protocol specifications OK, but the router ID or password are unknown, first, it would be normal to ask for a central authority about this new router, but if there are thousands of packages like this in every second, this would flood the entire network with verification packages, keeping the router busy and the entire wireless bandwidth would be used only for authenticating bad packages.

The previous example assumes that the attacking router does not know any valid router's password or encryption keys. But what happens if a router has been compromised and the attacker now holds all the encryption keys? In this situation, if the malicious router floods a router with valid packages, there is a real problem avoiding the DoS attack, and one could say that this attack is not the main problem. The attacker could inject malicious routes, could manipulate the router's routing table, forcing him to divert traffic.

Router impersonation

This type of attack may appear both in wireless or wired routing environments.

When a router is first started, if it doesn't know anybody (from a router's point of view) it could apply the „resurrecting duckling" [10] principle. This is a metaphor inspired from biology, where a duckling emerging from his egg will recognise the first moving object that he sees or makes a sound. This is called **imprinting**. The same thing will happen to our router R when he first receives a package from C. The principle is called „resurrecting" because the device can be reprogrammed to be imprinted by a different owner's ID, thus resurrecting the body after the previous „soul" has died out.

The duckling principle could be extended so that after R was imprinted, when he comes in the proximity of other routers he will first ask C if it is OK to recognise them as valid. But what happens if R moves around and loses touch with C? Because there is no one to trust, other that C, R could ask C the identity of the next router he will be approaching and thus be imprinted with more owners (or friends).

When moving a router (6), the new router can ask around his neighbours about the authenticity of 6. If has no one to authenticate him, he can ask the central authority. In all of these situations, the necessity of authenticating packages to prevent router impersonation is needed. Having a session password shared by every two routers could do this. Knowing the passwords, the routers could form the HMAC of package and send it. The routers can agree on a common password using the **Diffie Hellman** key exchange protocol [14].

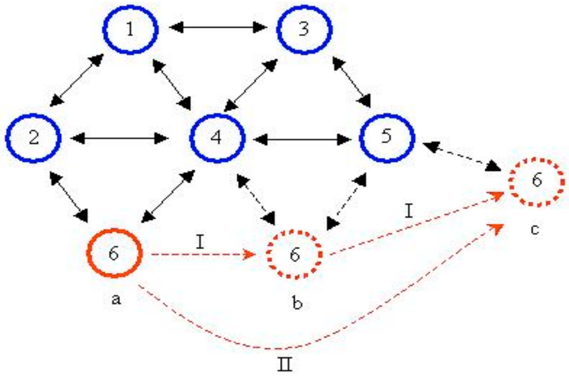

Figure 1. Moving router

After having the session key, routers can authenticate packages using a hash of the package combined with the session key, a MAC: $M = E_k(H(m), k)$, where k is the session key, m is the original message, E is the block encryption elgorithm. MACs are usually constructed out of block ciphers like DES. The simplest way to generate a MAC is to encrypt the hash of the message and the key with a block algorithm like CBC or CFB. Because the hash functions are faster than block ciphers in software implementation [15], today's applications choose to use for E a hash function.

Ignorance attack

This implies that an attacker having corrupted another router starts dropping packages received from adjacent routers. Because no major damage could be done by this form of attack and due to space limitations we will assume that in these situations routers could simply chose another node to deliver their packages, seeing that the other router is unwilling to cooperate. They could also inform other nodes that one of the routers having signature X is miss-behaving, thus activating the „reputation based framework” as described in [16].

Wormhole Attack

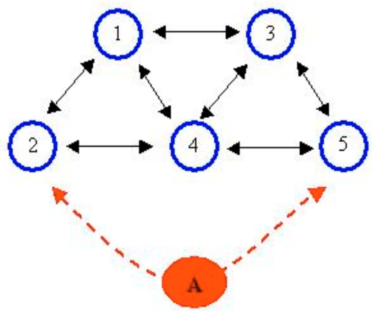

Figure 2. Artificial link

This form of attack is created by a „middle man”, who forwards packages from one router to another which are not in each others proximity, creating the false impression that these routers are neighbours.

In a wireless static network, the best solution to defend against an attack like this would be to have the central authority inform routers about their possible neighbours. In Ad Hoc wireless networks, this is not an easy job to do. Yih Chun Hu et al. in „Packet Leashes” [12] propose and implement a protocol that solve this problem. In this paper the authors propose that each package should be „held in a leash”. The means of doing this is the use of two techniques: **temporal leashes** and **geographical leashes**. In the case of temporal leashes, each package is marked with a timestamp that the receiving router may check and drop if it exceeds the average time that a package can travel from one node to another. This also requires precise clock synchronisation from nodes. In the second case, each package is marked with a geographical signature. Any other router can check it if it was received from a nier-by zone, and detect efficiently the „wormhole attack”.

Shorter distance fraud

Having a router advertise a longer distance than the one in reality is not as bad as one may think. In fact, if a router is compromised and controlled by an attacker, the advertising of longer routes makes other routers chose other nodes.

If a router updates his routing table with a shorter distance received as an advertised route from a malicious router, the attacker could gain control over traffic and all the packages sent to the „spoofed” destination. If a router manages to do this, all packages will be forwarded to him, resulting in an effective „blackhole” attack, placing the attacker in a powerful position.

This type of attack can be preventing using one-way hash chains [4]. Because they do not use symmetric or asymmetric cryptography, they are fast and easy to manipulate. A final random number is chosen, and a repetitive hash function is applied upon it to get the hash chain values [19].

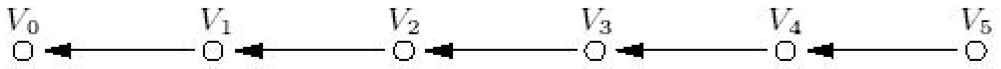

Figure 3. A simple hash chain with Vo as the value made public

The chain values are constructed as follows:

$$V_5 = RAND, V_4 = H(V_5), V_3 = H(V_4), V_2 = H(V_3), V_1 = H(V_2), V_0 = H(V_1)$$

After a node constructs this chain, Vo is made public. A chain is constructed for every destination that the node is directly connected, but for a chain to work there must be a max-hop count established [11]. To authenticate a certain destination with a specific metric, just release a value corresponding to the metric of that route.

For example, let’s consider a chain of m hash values, where V_0 is the last value and V_{m-1} is the first value (the random seed). Consider also maximal hop-count $k, k \leq m-1$. If A is directly connected to a network then he broadcasts the value V_0 using a certified authority. When a refresh period arrives (to advertise known routes), A sends out V_{k-1} for metric 0, to authenticate the known route. A receiving node would then authenticate V_{k-1} using V_0. It would then compute $V_{k-2} = H(V_{k-1})$ and send out to his neighbour the value V_{k-2} and metric 1. The next node would then compute V_{k-3}, and so on. Using this technique, a node can not force a lower metric, it can only send an advertisement with the same or larger metric.

Same distance fraud

This type of attack presumes that an attacker can receive and send valid packages, it can authenticate himself, modify packages and advertise copied routes as he wishes. So the „package leash" technique would be inefficient because the attacker can modify the package itself. The problem is that the attacker holds all the keys, they are valid and can use them on his own will, thus he can modify received metrics in a package, he can send out the same metric with the same hash value V as received, thus creating a „same distance fraud".

A highly efficient mechanism to prevent this kind of fraud was proposed by Yih-Chun Hu et al in [4]. This technique is based on one-way hash chains and hash trees, called one-way hash tree. The hash chain is used to prevent lower metric insertion and the hash tree is used to authenticate nodes, obliging them to increment the metric if they want to encode their own id.

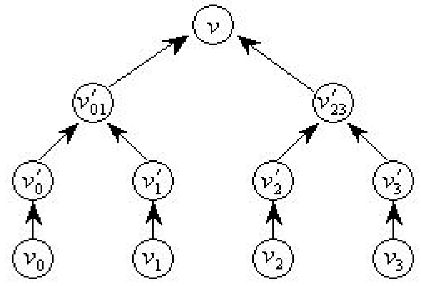

Figure 4. Hash tree

The initially generated seed numbers $v_i, 0 \le i \le 3$, are hidden by the $v'_i = H(v_i), 0 \le i \le 3$. Also, as we go up towards the root, values $v'_{01} = H(v'_0 \,\|\, v'_1), v'_{23} = H(v'_2 \,\|\, v'_3), v = H(v'_{01} \,\|\, v'_{23})$ can be computed out of the previous values. If a node wants to authenticate value v'_1, it sends out v'_0 and v'_{23} from which a node, having the final value v can verify if: $v = H(H(v'_1 \,\|\, v'_0) \,\|\, v'_{23})$

Conclusion

In this paper we briefly described the inherent vulnerabilities of mobile devices in ad-hoc network. In an ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only intermittently, further complicating their detection.

We present a variety of different proposals of secure routing protocols, but every security mechanism comes with a cost. It is always expensive to additionally test the authenticity of a package, it takes precious computational time, and therefore it is advisable to carefully select which protocol is more suited for an environment.

The solution should be to combine more secured routing algorithm. Different applications will have different security requirements, and will be best to adopt network performance-centric security solutions that effectively balance security strength and network performance in practice. The solutions presented in this article only cover a subset of all threats and are far from providing a comprehensive answer to the security problem in ad hoc networks.

References

[1] Bala Suryan, „Ad hoc mobile wireless network protocols: A comparative study of four distinct types", Available at: http://www.cs.clemson.edu/~srimani/CpSc824-S05/Termpapers/2.pdf
[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, Piet Demeester, „Mobile ad hoc networks: network layer issues", in 9th European Conferrence on Network & Optical Communications, NOC2004, Eindhoven, The Netherlands, Jun 29 – Jul 01 2004, pp. 253-260
[3] Andrew S. Tannenbaum, „Computer networks, Fourth Edition", 2003, Byblos
[4] Yih Chun Hu, Adrian Perring, David B. Johnson, „Efficient Security Mechanisms for Routing Protocols," from „Network and Distributed System Security Symposium", NDSS '03, pages 57-73, February 2003
[5] C. Hedrick, „Routing Information Protocol," Rutgers University, RFC 1058, July 1988
[6] G. Malkin, „Routing Information Protocol Version 2," SRI Network Information Center, RFC 2453, November 1998
[7] Balwant Rathore, „Router and Routing Protocol Attacks," FIST Conference 2003 – September Edition
[8] Charles E. Perkins, „Highly Dinamic Destination-Sequenced Distance VectorRouting (DSDV) for Mobile Computers", In Proceedings of the ACM SIGCOMM Conference (SIGCOMM '94), available at:http://citeseer.ist.psu.edu/perkins94highly.html
[9] Shree Murthy and J.J. Garcia-Luna-Aceves „An efficient routing protocol for wireless networks", Mobile Networks And Applications October 1996
[10] Frank Stajano and Ross Anderson, „The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", In proc. Of the 7th International Workshop on Security Protocols, Lecture notes in Computer Science, Berlin, Germany 1999
[11] Yih-Chun Hu, Adrian Perring, David B. Johnson, „SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications, Calicoon, NY, June 2002
[12] Yih-Chun Hu, Adrian Perring, David B. Johnson, „Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks", INFOCOM 2003
[13] Mixter for the BlackCode Magazine – A brief programming tutorial in C for raw sockets, Available at: http://mixter.void.ru/rawip.html
[14] Bruce Schneier, „Applied Cryptography, Second Edition", 1996
[15] Mihir Bellare, „Keying Hash Functions For Message Authentication", Advances In Cryptology – Crypto 96, June 1996
[16] Tao Wan, Evangelos Krankis, P.C. van Oorschot, „S-RIP: A Secure Distance Vector Routing Protocol," Applied Cryptography and Network Security, Second International Conference, Yellow Mountain, China, June 2004
[17] Dan Pei, Dam Massey, Lixia Zhang, „Detection of Invalid Routing Announcements in RIP Protocol", Global Communications Conferrence (Globecom), December 2003
[18] J. Postel, „Internet Control Message Protocol", RFC 792, September 1981
[19] Yih-Chun Hu, Markus Jakobsson, Adrian Perring, „Efficient Constructions for One-way Hash Chains", Proceedings of Applied Cryptography and Network Security 2005, New York, July 2005, to appear.