A BRIEF SURVEY OF VARIOUS SECURITY TECHNIQUES IN MANETS

Prachi Garg*

Abstract: Mobile Ad-hoc Networks (MANET) is an emerging area of research. Most current work is centred on routing issues. A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network .In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in more traditional networks may not directly be suitable for protecting them. A short survey over papers on ad hoc networks shows that many of the new generation security techniques are not yet able to address the security problems. To become commercially successful the technology must allow network to support many users. A complication is that addressing and routing in ad-hoc networks does not scale up easily as in the internet.

*Assistant professor in Computer Science at Geeta Institute of Technology and Management Kanipla, Kurukshetra

INTRODUCTION

In view of the increasing demand for wireless information and data services, providing faster and reliable mobile access is becoming an important concern. Nowadays, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part that is their applications do not interact. Sometimes, however, a group of mobile devices form a spontaneous, temporary network as they approach each other. This allows e.g. participants at a meeting to share documents, presentations and other useful information. This kind of spontaneous, temporary network referred to as mobile ad hoc networks (MANETs) sometimes just called ad hoc networks or multi-hop wireless networks, and are expected to play an important role in our daily lives in near future.

A traditional mobile network consists of a fixed network of servers and clients, with a collection of mobile clients that move throughout the geographic area of the network. Within the mobile network, servers have unlimited power and communicate with mobile hosts over a wireless connection. Mobile clients may only communicate among themselves through a server. Among the issues in this type of network are client power consumption, connectivity of the network, and reachability of mobile clients from a server.

In contrast, a MANET is a collection of mobile servers and clients. All nodes are wireless, mobile and battery powered [9]. The topology can change frequently. The nodes organize themselves automatically, and can be a standalone network or attached to a larger network, including the Internet [2]. All nodes can freely communicate with every other node.

Ad hoc networks may be very different from each other, depending on the area of application. For instance in a computer science classroom an ad hoc network could be formed between students' PDAs and the workstation of the teacher. In another scenario a group of soldiers is operating in a hostile environment, trying to keep their presence and mission totally unknown from the viewpoint of the enemy. The soldiers in the group work carry wearable communication devices that are able to eavesdrop the communication between enemy units, shut down hostile devices, divert the hostile traffic arbitrarily or impersonate themselves as the hostile parties. As can obviously be seen, these two scenarios of adhoc networking are very different from each other in many ways: In the first scenario the mobile devices need to work only in a safe and friendly environment where the networking conditions is predictable. Thus no special security requirements are needed. On the other hand, in the second and rather extreme scenario the devices operate in an extremely hostile and demanding environment, in which the protection of the communication and the mere availability and operation of the network are both very vulnerable without strong protection.

As ad hoc networking somewhat varies from the more traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach somewhat restricts the set of feasible security mechanisms to be used, as the level of security and on the other hand performance are always somewhat related to each other. The performance of nodes in ad hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained, as discussed e.g. in [3]. In addition, the available bandwidth and radio frequencies may be heavily restricted and may vary rapidly. Finally, as the amount of available memory and CPU power is typically small, the implementation of strong protection for ad hoc networks is non-trivial.

The main objective of this paper is to describe how the different security techniques help in various situations in ad-hoc networks. In this firstly the different concepts of manets are discussed related to security then the different techniques for preventing networks are discussed.

VARIOUS ISSUES RELATED TO SECURITY

Physical Security

In ad hoc networks especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However, the significance of the physical security in the overall protection of the network is highly dependent on the ad hoc networking approach and the environment in which the nodes operate. For instance in ad hoc networks that consist of independent nodes and work in a hostile battlefield the physical security of single nodes may be severely threatened. Therefore in such scenarios the protection of nodes cannot rely on physical security. In contrary, in the classroom example scenario the physical security of a node is an important issue to the owner of the node, perhaps for privacy reasons, but the breaking of the physical security does not affect the security of the system as such.

Service Principles

Ad hoc networks may apply either hierarchical or flat infrastructure both in logical and physical layers independently. As in some flat ad hoc networks the connectivity is maintained directly by the nodes themselves, the network cannot rely on any kind of *centralized* services. In such networks the necessary services such as the routing of packets and key management have to be *distributed* so that all nodes have responsibility in providing the service. As there are no dedicated server nodes, any node may be able to provide the necessary service to another. Moreover, if a tolerable amount of nodes in the ad hoc network crash or leave the network, this does not break the availability of the services. Finally, the protection of services against *denial of service* is in theory impossible. In ad hoc networks *redundancies* in the communication channels can increase the possibility that each node can receive proper routing information. Such approaches do, however, produce more overhead both in computation resources and network traffic. The redundancies in the communication paths, however, may reduce the denial of service threat and allow the system to detect malicious nodes from performing malicious actions more easily than in service provisioning approaches that rely on single paths between the source and destination.

Availability is a central issue in ad hoc networks that must operate in dynamic and unpredictable conditions. The network nodes may be idle or even be shut down once for a while. Thus the ad hoc network cannot make any assumptions about availability of specific nodes at any given time. For commercial applications using ad hoc networks availability is often the most important issue from the viewpoint of the clients. The routing protocol must guarantee the *robustness* of the routing fabric so that the connectivity of the network is maintained even when threatened by rapid changes in topology or attackers. Similarly, in the higher layers, the services must be able to rely on that the lower layers maintain the packet-forwarding services at any time. Finally, many ad hoc networking protocols are applied in conditions where the topology must *scale up and down efficiently*, e.g. due to network partitions or merges. The scalability requirements also directly affect the scalability requirements targeted to various security services such as key management. In networks where the area of application restricts the possible size of the network, assumptions can be made about the scalability requirements of the security services as well.

Key Management Security

As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As ad hoc networks significantly vary from each other in many respects, an environment-specific and efficient key management system is needed. To be able to protect nodes e.g. against eavesdropping by using encryption, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. For very rapidly changing ad hoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumptions about a priori negotiated secrets. In less dynamic environments like in the classroom example above, the keys may be mutually agreed proactively or even configured manually (if encryption is even needed).

If public-key cryptography is applied, the whole protection mechanism relies on the security of the private key. Consequently, as the physical security of nodes may be poor, private keys have to be stored in the nodes confidentially, for instance encrypted with a system key. For dynamic ad hoc networks this is not a wanted feature and thus the security of the private key must be guaranteed with proper hardware protection (smart cards) or by distributing the key in parts to several nodes. Hardware protection is, however, never alone an adequate solution for preventing attacks as such. In ad hoc networks a centralized approach in key management may not be an available option, as there may not exist any centralized resources. Moreover, centralized approaches are vulnerable as single point of failures. The mechanical replication of the private keys or other information is an inadequate protection approach, since e.g. the private keys of the nodes simply have then a multiple possibility to be compromised. Thus a *distributed approach* in key management - for any cryptosystem in use - is needed, as proposed e.g. in [10].

Control in Accessing

The access control is an applicable concept also within ad hoc networking, as there usually exist a need for controlling the access to the network and to the services it provides. Moreover, as the networking approach may allow or require the forming of *groups* in for instance network layer, several access control mechanisms working in parallel may be needed. In the network layer the routing protocol must guarantee that no authorized nodes are allowed to join the network or a *packet forwarding group* such as the clusters in the hierarchical routing approach. For example in the battlefield example of the introduction the routing protocol the ad hoc network applies must control so that no hostile node can join and leave the group undetectable from the viewpoint of the other nodes in the group. In application level the access control mechanism must guarantee that unauthorized parties cannot have accesses to services, for instance the vital key management service.

Access control is often related to the *identification* and *authentication*. The main issue in the identification and authentication is that the parties can be confirmed to be authorized to gain the access. In some systems, however, identification or authentication of nodes is not required: nodes may be given e.g. delegate certificates with which the nodes can gain access to services. In this case actual authentication mechanisms are not needed, if the nodes are able to present adequate credentials to the access control system. In some ad hoc networks services may be centralized, while in other networks they are applied in a distributed manner, which may require the use of different access control mechanisms. Moreover, the required security level in access control also affects the way the access control must be implemented. If a centralized ad hoc networking approach with low security requirements is applied - as in the classroom example - the access control can be managed by the server party with simple means such as user id - password scheme. In ad hoc networks that operate in more difficult conditions without any centralized resources as in the battlefield scenario, the implementation of access control is much more difficult. Either the access to the network, its groups and resources must be defined when the network is formed, which is very inflexible. The other possibility is to define and use a very complex, scalable and dynamic access control protocol, which brings flexibility but is prone to various kinds of attacks and it may even be impossible to apply properly and efficiently.

THREATS OF SECURITY

Types of Attacks

Attacks against ad hoc networks can be divided into two groups: *Passive attacks* typically involve only *eavesdropping* of data. *Active attacks* involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. *External attacks* are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely.

External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. *Internal attacks* are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer.

Thus such malicious insiders who may even operate in a group may use the standard security means to actually *protect their attacks*. These kind of malicious parties are called *compromised nodes*, as their actions compromise the security of the whole ad hoc network.

(DoS) Denial of Service

Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks[3]. Distributed Denial of Service (DDoS) attacks has also become a problem for users of computer systems connected to the Internet. A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated.

A denial of service (DoS) attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources [6]. Examples of denial of service attacks include:

- attempts to “flood” a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person

The denial of service attack has many forms: the classical way is to flood any centralized resource so that it no longer operates correctly or crashes, but in ad hoc networks this may not be an applicable approach due to the distribution of responsibility. Distributed denial of service attack is a more severe threat: if the attackers have enough computing power and bandwidth to operate with, smaller ad hoc networks can be crashed or congested rather easily.

Disclosure

Any communication must be protected from eavesdropping, whenever confidential information is exchanged. Also critical data the nodes store must be protected from unauthorized access. In ad hoc networks such information can include almost anything e.g.specific status details of a node, the location of nodes, private or secret keys, passwords and -phrases and so on. Sometimes the control data is more critical information in respect of the security than the actual exchanged data. For instance the routing directives in packet headers such as the identity or location of the nodes can sometimes be more valuable than the application-level messages. This applies especially in critical military applications. For instance in the battlefield scenario the data of a "hello" packet exchanged between nodes may not be as interesting from the viewpoint of the enemy. Instead the identities of the observed nodes - compared to the previous traffic patterns of the same nodes - or the detected radio transmissions the nodes generate may be the information just the enemy needs to launch a well-targeted attack. On the contrary, in the classroom example the disclosure of exchanged or stored information is critical "only" from the viewpoint of a person’s privacy.

TECHNIQUES USED FOR SECURITY

DDM

Dynamic Destination Multicast protocol (*DDM*) is a multicast protocol that is relatively different from many other multicast-based ad hoc protocols. In DDM the group membership is not restricted in a distributed manner, as only the sender of the data is given the authority to control to which the information is really delivered. In this way the DDM nodes are aware of the membership of groups of nodes by inspecting the protocol headers.

The DDM approach also prevents outsider nodes from joining the groups arbitrarily. This is not supported in many other protocols directly; if the group membership and the distribution of source data have to be restricted, external means such as the distribution of keys have to be applied.

DDM has two modes of operation: the *stateless mode* and the *soft-state mode*. In the stateless mode the maintenance of multicast associations and restriction of group membership are handled totally by encoding the forwarding information in a special header of the data packets; the nodes do not have to store state information. This kind of reactive approach thus guarantees that there are no vainless exchange of control data during idle periods. Thus in small ad hoc networks that need not scale up substantially, this kind of ultra-reactive approach can be extremely useful. The soft-state mode, on the other hand, requires that the nodes remember the next hops of every destination and thus need not fill up the protocol headers with every destination. In both modes the nodes must always be able to keep track of the membership of the groups. According to the authors, DDM is best suited for dynamic networks having small multicast groups. Currently the DDM draft ([8]) does not, however, propose any solutions for securing the DDM networks as such. Moreover, it does not provide any suggestions for a concrete protocol that handles the necessary access control needed in the restriction of group membership.

OLSR

Optimized Link State Routing protocol (*OLSR*), as defined in [7], is a proactive and table driven protocol that applies a multi-tiered approach with *multi-point relays* (MPR). MPRs allow the network to apply scoped flooding, instead of full node-to-node flooding, with which the amount of exchanged control data can substantially be minimized. This is achieved by propagating the link state information about only the chosen MPR nodes.

Since the MPR approach is most suitable for large and dense ad hoc networks, in which the traffic is random and sporadic, also the OLSR protocol as such works best in these kind of environments. The MPRs are chosen so that only nodes with one-hop symmetric (bi-directional) link to another node can provide the services. Thus in very dynamic networks where there exists constantly a substantial amount of uni-directional links this approach may not work properly. OLSR works in a totally distributed manner, e.g. the MPR approach does not require the use of centralized resources. The OLSR protocol specification does not include any actual suggestions for the preferred security architecture to be applied with the protocol. The protocol is, however, adaptable to protocols such as the *Internet MANET Encapsulation Protocol* (*IMEP*), as it has been designed to work totally independently of other protocols.

ODMRP

On-Demand Multicast Routing Protocol (*ODMRP*) is a mesh-based multicast routing protocol for ad hoc networks, specified in [10]. It applies the *scoped flooding* approach, in which a subset of nodes - a *forwarding group* - may forward packets. The membership in the forwarding groups are built and maintained dynamically on-demand. The protocol does not apply source routing. ODMRP is best suited for MANETs where the topology of the network changes rapidly and resources are constrained. ODMRP assumes bi-directional links, which somewhat restricts the potential area of application for this proposal; ODMRP may not be suitable for use in dynamic networks in which nodes may move rapidly and unpredictably and have varying radio transmission power. Currently ODMRP does not define or apply any security means as such, "the work is in progress". The forwarding group membership is controlled with the protocol itself, though.

AODV and MAODV

Ad Hoc On-Demand Distance-Vector routing protocol (*AODV*), defined in [5], is an unicast-based reactive routing protocol for mobile nodes in ad hoc networks. It enables multi-hop routing and the nodes in the network maintain the topology dynamically only when there is traffic. Currently AODV does not define any security mechanisms whatsoever.

The authors identify the necessity of having proper confidentiality and authentication services within the routing, but suggest no solutions for them. The IPSec is, however, mentioned as one possible solution. *Multicast Ad Hoc On-Demand Distance-Vector* routing protocol (*MAODV*), specified in [16], extends the AODV protocol with multicast features.

The security aspects currently noted in the design of MAODV are similar to the AODV protocol.

TBRPF

Topology Broadcast based on Reverse-Path Forwarding (*TBRPF*), as defined in [2], is a pure proactive, link-state routing protocol for the ad hoc networks that can also be applied as the proactive part in hybrid solutions. Each of the nodes of the network in TBRPF carry state information of each link of the network, but the information propagation is optimized by applying *reverse-path forwarding* instead of the costly full flooding or broadcast techniques. TBRPF operates over IPv4 in ad hoc networks and can also be applied within hierarchical network architecture. The authors of the proposal, however, do not suggest any specific mechanisms for securing the protocol. Finally, the protocol, just as every other ad hoc network routing protocol, can be protected with IPSec, but this approach is not currently officially in use within TBRPF.

CONCLUSION AND FUTURE SCOPE

Security is an important topic that needs to be addressed when designing networks in MANET environments. This topic involves far more than network routing protocols. In addition, existing security methods are insufficient. They are not geared towards the specialized needs of a MANET. The areas of concern within MANET data communication are raised. Future research will need to begin to resolve DoS attack very carefully because it is one of the most harmful attacks for the network. Along with these issues, standardized benchmarks and criteria for Evaluation must be established so that proposed protocols and methods can be legitimately compared.

REFERENCES

[1] Hao Yang, haiyun luo, Fan Ye, Songwu Lu and Lixia Zhanng, “Security on Mobile Ad Hoc Networks: Challenges and Solutions” 1536-1284/04/IEEE Wireless Communications Feb. 2004

[2] S.Buchegger and J.L. Boudec, “Performance Analysis of the Confident Protocol in dynamic Ad Hoc Networks IEEE/ACM Symp., 2002

[3] S. Corson and J.Macker, “Mobile Ad Hoc Networking routing Protocol Performance Issues and evaluation considerations”, RFC2501, Jan. 1999

[4] Corson, M., Freebergyser, J., and Sastry, A., "Mobile Ad Hoc Networking: Editorial, "Mobile Networks and Applications, 4(3): pp. 137-138, 1999

[5] Singh, S., Woo, M., and Raghavendra, C. Power Aware Routing in Mobile Ad Hoc Networks. In

Proc. 4th International Conf. on Mobile Computing and Networking (MOBICOM '98), pp. 181-190, October, 1998.

[6] Guo, Y., Pinotti, M., and Das, S., "A New Hybrid Broadcast Scheduling Algorithm for Assumetric

Communication Systems," ACM Mobile Computing and Communications Review, 5(4): pp. 39-54, 2001

[7] Claude Castelluccia, Nitesh Saxena, Jeong Hyun Yi, “Robust self-keying mobile adhoc networks” Computer Networks 51 (2007) 1169–1182 1389-1286 2006 Elsevier B.V. doi:10.1016/j.comnet.2006.07.009

[8] C.Zhuand M.Corson, QoS routing for mobile adhoc networks, tech. report, CSHCN Technical Report 2001.

[9] Kärpijoki, V. Signalling and Routing Security in Mobile Ad Hoc Networks. *Proceedings of the Helsinki University of Technology, Seminar on Internetworking - Ad Hoc Networks*, Spring 2000. [referred 25.4.2000]

[10] Lee, S.-J. et al. On-Demand Multicast Routing Protocol (ODMRP). IETF draft, January 2000 (expired). [referred 25.9.2000]