A SERVICE DISCOVERY THREAT MODEL FOR AD HOC NETWORKS

Adrian Leung and Chris Mitchell
Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX, UK

Keywords: Security, Secure Service Discovery, Threat Model, Mobile Ad Hoc Networks, MANETs.

Abstract: The dynamic yet vulnerable nature of an hoc network presents many new security and privacy challenges. Securing the process of service discovery is one of them. Novel solutions are therefore required. However, in order for appropriate security measures to be devised, all possible security threats must first be identified and thoroughly analysed. In this paper, we present a threat model for service discovery in ad hoc networks. Based on these threats, we proceed to derive the security services required to achieve secure service discovery.

1 INTRODUCTION

An ad hoc network is formed spontaneously by a collection of two or more mobile devices. These devices, also referred to as *Nodes*, may communicate directly if they are within radio range of each other, or rely on intermediate nodes to route their messages if they are not. Nodes may join, leave or change their existing locations, and this results in a constantly changing network topology. The dynamic and infrastructureless nature of the ad hoc network poses many interesting problems and challenges. Service Discovery is one of them.

One of the primary objectives of forming an ad hoc network is for nodes to share and utilise each others' resources. Before a resource can be used, it needs to be located. The process of finding available resources in an ad hoc network is known as *service discovery* and research in this important area is slowly gathering momentum. A variety of ad hoc network service discovery schemes (Garcia-Macias and Torres, 2005; Mohan et al., 2004) have recently been proposed, with each scheme focusing on different aspects of service discovery, such as architectural choice (Lim et al., 2005), service description syntax (Tyan and Mahmoud, 2005) and other performance metrics (Gao et al., 2006). However, none addresses the issue of security from the outset, despite its fundamental importance.

Before any novel security solutions are devised to secure service discovery, a thorough analysis of all possible security threats that could arise must be conducted. Effective solutions can then be developed with these threats in mind. In this paper, we focus on the threats that arise during service discovery, and we also analyse the threats according to the type of misbehaviour that the nodes exhibit.

The remainder of this paper is organised as follows. In section 2, we define the terminology used, and section 3 describes the different service discovery architectures. In section 4, we present the threat model. In the penultimate section, the security requirements are identified, and conclusions are drawn in section 6.

2 TERMINOLOGY

We begin with the definition of a service. O'Sullivan (O'Sullivan et al., 2002) has defined a *Service* as: "An action performed by an entity on behalf of another and this action involves the transfer of value". In the context of an ad hoc network, examples of service may include printing of documents, performing computations, data storage, image capture, etc. Against this backdrop, *Service Discovery* can thus be defined as: "The act or process of finding and locating a service on a network". The overall performance of a service discovery scheme can be measured with a metric known as *Service Availability*. This metric is the ratio of the number of service requests made against the number of requests that were actually fulfilled.

The entities participating in the service discovery process are now introduced: A *Service User* (SU) node is a node that seeks a particular service offered by other nodes in the network. A *Service Provider*

Leung A. and Mitchell C. (2006).
A SERVICE DISCOVERY THREAT MODEL FOR AD HOC NETWORKS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 167-174
DOI: 10.5220/0002097301670174

(SP) node has one or more services to offer other nodes. Depending on the service discovery architecture employed, a *Directory* (SD) node may also be involved in the service discovery process. An SD node acts as a broker between the SU and SP nodes. It maintains a list of the available services in the network. Some nodes may not participate directly in the service discovery process, but may be called upon to forward or route the service messages between the principal participants. We call these nodes *Forwarding* (FW) nodes. It is also possible for a node to take on more than one role. For instance, a node may offer a particular service (SP node) and also be a consumer of another service (SU node).

A variety of different service messages are exchanged and sent between the entities during service discovery. A *Service Request* (SrvReq) is a message sent by an SU node to search for a particular service. A *Service Reply* (SrvRep) is a message sent to an SU node if the requested service is available. It can be sent by either an SP or an SD node. A *Service Advertisement* (SrvAdv) is a message sent (via broadcast) by an SP node to announce its service offering. An SU node sends an *Acknowledgement* (SrvAck) message to the SP node if it is interested in the advertised service. *Service Register/Deregister* (SrvReg/SrvDReg) messages are sent by an SP node to an SD node to register or deregister a service. In response, an *Acknowledgement* (SrvAck) message is sent back to the SP node. An SD node will broadcast a *Directory Advertisement* (DirAdv) message to announce its presence to other nodes. A *Service List* (SrvList) is a file maintained by an SD node that contains a listing of the available services.

Two other important terms, used to denote the distance (in terms of radio ranges) between two nodes, are *hop* and *hop count*. Nodes within radio range of each other are said to be one hop apart. Two nodes are X hops away from each other if a minimum of $X-1$ intermediate nodes are required to route a message between them. Hop count is defined as the maximum number of times that a particular message will be forwarded by an intermediate node. The set of nodes which are at most X hops away from a node is also referred to as the *scope* of a node.

3 AD HOC NETWORK SERVICE DISCOVERY ARCHITECTURES

In an ad hoc network, services may be discovered in a number of different ways. This has an effect on how the entities interact with each other, which in turn affects the type of threats that arise during service discovery. Hence, it is imperative to have a good understanding of the various discovery methods in order to produce an accurate threat model.

As depicted in Figure 1, techniques for service discovery in ad hoc networks can generally be classified into three main types (Rao, 2004). They are the *mediated*, *immediate* and *hybrid* architectures.

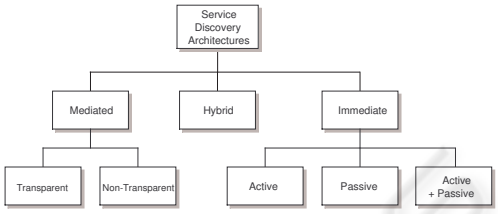

Figure 1: Classification of Service Discovery Architectures.

We now examine the workings of the three architectures, based on the assumption that all the nodes are non-malicious, co-operative and trustworthy.

3.1 Mediated Architecture

This architecture is also known as the *Service Co-Ordinator Based* architecture (Toh, 2002). In this architecture, SU and SP nodes rely on a service coordinator or an SD node to facilitate service discovery. As an ad hoc network is usually composed of heterogenous devices, the role of an SD node is usually taken on by the more powerful devices (the method used to select an SD node is beyond the scope of this paper).

Assuming that an SU and an SP node are both within the scope of an SD node, service discovery takes place as follows:

1. The SD node periodically announces its presence by broadcasting a DirAdv message through the network (with an initial hop count of X).
2. An SP node will register its service offerings with the SD node by sending a unicast SrvReg message to the SD node.
3. The SD node will acknowledge receipt of an SrvReg message by sending a SrvAck message back to the SP node. The SD node also updates its list (SrvList) of all registered services.
4. An SU node seeking a service will query an SD node by sending a unicast SrvReq message to the SD node.
5. Upon receiving a SrvReq message, an SD node searches its SrvList for the requested service. If the sought service is found, the SD node sends a SrvRep message back to the SU node. The SrvRep message will contain details of the service provider (e.g. the URL or IP address of the service provider).

6. A registered service may be removed from the SrvList when it expires or when an SP node sends a SrvDrg message to the SD node.

In the event that an SD node is more than one radio hop away from SU and SP nodes, intermediate nodes will forward the SrvReq, SrvRep, SrvReg, SrvAck and SrvDrg messages to and from the SD nodes, provided the message does not traverse more than X hops. It should be noted that the mediated architecture can be further divided into two sub-categories: *transparent* and *non-transparent*. Transparent means that SU and SP nodes are fully aware of the existence of one or more SD node(s) in the network, while non-transparent means SU and SP nodes are not aware that an SD node is present, thinking they are interacting directly with each other.

The mediated approach is extremely scalable but is unsuitable for highly mobile environments, as the SrvLists have to be constantly updated and modified. Another shortcoming of this approach is the service non-discoverability problem between an SU node that is interested in the service offering of an SP node. The two nodes may be in close proximity, but service discovery simply cannot take place. This is because either one or both of the nodes are lying outside the scope (beyond X hops) of the SD node. In such a case, there is no way for either node to be aware of the presence of the other, no matter how near they are to each other.

3.2 Immediate Architecture

The immediate architecture is also referred to as the *Distributed Query-Based Architecture* (Toh, 2002). In this architecture, there are no SD nodes. SU and SP nodes seek and advertise their own services directly, without relying on SD nodes.

An SU node seeks a service by broadcasting a SrvReq message through the network (with an initial hop count of X). Upon receiving this SrvReq message, a node may:

- send a unicast SrvRep message to the SU node if it offers the requested service, and forward the SrvReq message to its neighboring nodes.
- decrement the hop count and rebroadcast the SrvReq message if it does not offer the specified service.
- do nothing and drop the packet if the hop count reaches zero.

This method of discovery is sometimes known as *active* or *pull-based* discovery. Alternatively, an SP node may advertise its service by broadcasting a SrvAdv message through the network (with an initial hop count of X). Upon receiving a SrvAdv message, a node may:

- send a SrvAck message to the SP node if it is interested in the service offered, and rebroadcast the SrvAdv message.
- decrement the hop count and rebroadcast the SrvAdv message.
- do nothing and drop the packet if the hop count reaches zero.

Nodes receiving a SrvAdv message may cache the service information for future use and compile a SrvList of their own. This method of discovery is also referred to as *passive* or *push-based* discovery.

Finally, as shown in Figure 1, active and passive discovery may also take place concurrently. This architecture is suitable for highly mobile networks, but it does not scale well.

3.3 Hybrid Architecture

The mediated and immediate architectures may coexist at the same time to yield the hybrid approach. The hybrid approach offers several advantages over a pure mediated or a pure immediate architecture. Firstly, simulation results in (Guichal and Toh, 2001) have shown that service availability is significantly better with the hybrid approach. Secondly, the presence of SD nodes in the network also improves scalability. Finally, the service non-discoverability problem can also be easily overcome. Service discovery is now possible between two nodes that are in close proximity even when one or both of the nodes are not within the scope of the SD node. Because of the added flexibility of the immediate approach, either node is now capable of broadcasting a service request or service advertisement on their own.

In summary, the hybrid approach is more flexible and enhances service availability.

4 A SERVICE DISCOVERY THREAT MODEL

There exist a variety of security issues and threats in ad hoc networks (Mishra and Nadkarni, 2003; Papadimitratos and Hass, 2003; Zhou, 2003). However, in our threat model we focus solely on the threats that arise during service discovery.

4.1 Objective of Service Discovery

Different entities have different aims for, and expectations of, a service discovery protocol. We briefly discuss this from the perspectives of the three main types of entity involved, namely: Service Users, Service Providers and Directory nodes. From a service user's

perspective, the primary aim is to find a provider of the desired service within its scope. It may also want to know what other services are available in the network. A service provider's main aim is to inform all service users of its service offerings. Finally, a directory simply wants all users and providers to be aware of its presence so that it can perform its task.

Therefore, any action that can be performed by an entity that prevents any of the above can be considered as a security threat, or a form of attack.

4.2 Threat Targets

Threat targets are the assets of the system. They are the prime motivation for a potential adversary to launch an attack. Threat targets can be broadly categorised into two types: *Tangible* and *Intangible*.

If an attack is aimed at a tangible threat target, then the effects would be more immediately observable. Examples of tangible threat targets include: the integrity and availability of the entities, the confidentiality, integrity and availability of the service messages and SrvList, the integrity and legitimacy of the service discovery process, and the resources or energy of the nodes.

An attack aimed at intangible threat targets may not have an immediately observable effect. Examples of intangible threat targets include: network connectivity and availability, and the reputations of the entities.

4.3 The Threat Model

In an ad hoc network, where all communications take place over the wireless medium, any device with an appropriate network interface is capable of gaining access to the network and participating in the network functions it offers. Further, devices or nodes are free to join or leave the network or even change their locations at any time. This results in an dynamic network topology. Consequently, the concept of a physical perimeter does not really apply in an ad hoc network.

Without a clear boundary, it is difficult to make a distinction between internal and external nodes and to classify the corresponding threats into internal or external threats.

In our threat model, we therefore do not attempt to distinguish between internal and external threats. Instead, we focus on the types of threat that could arise from the various types of node misbehaviour.

A classification of service discovery security threats is shown in Figure 2. The threats are divided into three main categories, according to the type of misbehaviour (Yau and Mitchell, 2003) that the nodes exhibit. They are: *Failed* nodes, *Selfish* nodes and *Malicious* nodes. Malicious nodes can be further subdivided into *Active* and *Passive* threats. It is helpful to examine the threats arising from these three different types of misbehaviour, for they have very different characteristics.

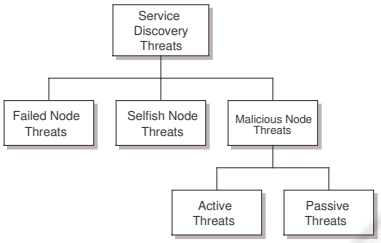

Figure 2: Classification of Service Discovery Threats.

We now examine the different types of threats in greater detail and discuss their implications and consequences.

4.3.1 Failed Nodes

Involuntarily, a node may be prevented from partaking in the service discovery process in the normal cooperative manner that is demanded of all nodes in an ad hoc network. Such nodes are termed *Failed Nodes* and do not harbour any malicious intent. This type of misbehaviour is usually a consequence of either:

- A node having its resources (power) completely depleted. Such a node may have been the target of a concerted Denial of Service (DOS) attack by an adversary. As a result of the attack, the node's battery or power might have been completely drained, rendering it unable to perform any task or network function. A node's resources could also have naturally run out without being subjected to any prior attacks. This type of failure is also known as *graceful failure*.
- A node may also be deemed a failed node if it is incapable of communicating with the other nodes (within its radio range) in the network. This may be due to a faulty network interface or the result of an adversary jamming or interfering with the wireless channel. Normal operation may resume once the adversary stops the interference. As such, node failure could be temporary or permanent.

Even though failed nodes do not misbehave intentionally, the threats they posed to the service discovery process are just as devastating. Threats pose by failed nodes vary significantly, depending on the type of node that fails. If the failed node is:

- an FW node, it will not be able to forward any service messages to and from any service entities (SU, SP and SD). Service discovery will not be possible if the particular failed FW node serves as the only

link or path between two service entities. Also, an FW node may fail while forwarding a service message. It will thus be unable to complete its action and will be deemed a failed node. The consequences of a failed FW node can therefore be rather significant even though it is not a principal participant in the service discovery process.

- an SU node, it is incapable of sending and receiving any service messages to or from any other entities. In other words, it is unable to take any part in the service discovery process. However, service discovery between other service entities is not affected.
- an SP node, it will no longer be able to service its existing service users and to solicit new service users as it is incapable of sending any service advertisement or registration messages to service users or directories. Service discovery between other service entities remains unaffected.
- an SD node, the entire service discovery system in the network may be crippled. In a mediated only architecture, SU and SP nodes rely on SD nodes to facilitate service discovery. If it is the only SD node in the network, the effects are dire. Otherwise, service discovery may still take place normally in the absence of an SD node, as seen in the hybrid or immediate architectures. The effects that a failed SD node has on the service discovery process depend very much on the service discovery architecture that is employed.

4.3.2 Selfish Nodes

In an ad hoc network, the success of the service discovery process depends greatly on the co-operation of all the nodes. Unfortunately, with the aim of conserving their scarce resources, some nodes may simply refuse to co-operate even though they are fully capable of doing so. These nodes co-operate only when there are incentives for them to do so. Nodes that exhibit this type of behaviour are known as *selfish* nodes. These nodes are not malicious in nature even though they misbehave intentionally. If a selfish node is:

- an FW node, it selectively forwards service messages. As a result, SU, SP and SD nodes may not receive the service messages intended for them. Also, in order to conserve some of its processing power, a selfish FW node may forward service messages without decrementing the hop count. Nodes may receive an out of scope service message and may have trouble contacting the sending node later on. Service discovery may be severely disrupted as a result of either action.
- an SU node, it selectively broadcasts service requests. The service discovery process is not really affected in any way. It should be noted that it is highly unlikely that an SU node behaves in a selfish manner, as there is very little motivation for the SU node to do so, and it stands to gain very little.
- an SP node, it does not broadcast its service advertisements as often as it should. SU and SD nodes will not be aware of the services offered by the SP node. Again, there is very little incentive for an SP node to behave in a selfish manner, as it does not stand to gain anything.
- an SD node, it may not inform the network of its existence. As such, SU and SP nodes will not be able to request and register services respectively. Hence, in a pure mediated architecture, service discovery will simply be impossible. Also (regardless of the type of architecture employed), it may not accept SrvReq messages from SU nodes or SrvReg/SrvDReg messages from SP nodes. As a result, when it does decide to be contacted by the other nodes, it will not be in possession of an updated Srvlist.

4.3.3 Malicious Nodes

Malicious nodes have no intention of participating in the service discovery process. Their primary aim is to disrupt the "proper" operation of the service discovery process. A wide range of threats are posed by the malicious nodes to the service discovery process. Associated with every threat are one or more threat targets. Using the *STRIDE* method (Swiderski and Snyder, 2004), we can classify malicious node threats into six categories, namely: *Spoofing*, *Tampering*, *Repudiation*, *Information disclosure*, *Denial of service*, and *Elevation of privilege*. Threats may also be classified as *Active* or *Passive*.

The STRIDE method (Swiderski and Snyder, 2004) is now be used to identify and analyse the service discovery threats caused by malicious nodes.

1. **Spoofing.** A malicious node may masquerade as another entity during service discovery. It may pose as:
   - an FW node. Upon receiving a legitimate service message, it may not forward the message to other nodes. Service discovery cannot take place if this FW node is the only link between two nodes. The threat target would be the intended recipients of the service messages.
   - an SU node and broadcast a SrvReq message through the network. An SP or SD node receiving the message may think that they are interacting with a legitimate SU node. The threat target here is the SP, SD or even an FW node.
   - another legitimate SP node and offer "services" to an unknowing SU node.

- an SD node and announce its presence to the network. This malicious SD node may be nearer (less hops away) to some of the SU or SP nodes. They may then choose to interact with this malicious SD node instead of a legitimate one that is further away.

The threat targets are the entities to whom the malicious node will be masquerading. Spoofing is an active threat.

2. **Tampering.** A malicious node may capture and then modify legitimate service messages traversing the network in one of the following ways:

   - Alteration of legitimate service messages by changing their contents. As a result, the intended recipients of the service messages will not be presented with accurate service information. This greatly compromises the service discovery process. The direct threat targets are the service messages, while the indirect threat targets are the intended recipients of the altered messages.
   - Deletion of legitimate service messages. The intended recipients of the service messages will not be able to receive the messages. Service discovery will then not take place as it should. This threat has the same effect as a selfish node not wanting to forward SrvReq and SrvAdv messages to other nodes. In this case, the direct threat target is the deleted service message, while the indirect threat target is the intended recipient of the original service message.
   - Insertion of bogus service messages. A malicious node may broadcast fraudulent service messages (e.g, SrvReq, SrvAdv, or DirAdv) into the network. Recipients of such fraudulent massages may think that they are actually interacting with legitimate SU, SP or SD nodes. This threat is similar to the spoofing threat discussed above. The threat targets here are the intended recipients of the fraudulent messages.

   It is obvious that tampering is an active threat. The worse case scenario for a tampering threat is when an SD node is malicious. It will then be able to modify — i.e. alter, delete, or insert — service information pertaining to legitimate SU and SP nodes, since it has direct access to the SrvList. The consequence of an inaccurate SrvList is devastating for the integrity of the entire service discovery process. The threat target here is clearly the SrvList, and the indirect threat targets are the service entities that it will be interacting with.

3. **Repudiation.** A malicious node may later deny having performed a certain action. For example, a malicious SU, SP or SD node may deny having sent a SrvReq, SrvAdv, or DirAdv message, respectively. Similarly, they may also deny having receive a specific service message. The threat target would be the entity that the malicious node was interacting with. Repudiation is an active threat.

4. **Information Disclosure.** Eavesdropping is particularly simple in a setting such as an ad hoc network, since the primary mode of communication amongst the nodes is a wireless channel.

   During the service discovery process, a malicious node is capable of eavesdropping on the service messages that are exchanged between the service entities, or broadcast through the network by SU or SP nodes. An inventory of services requested and advertised can thus easily be compiled, and this constitutes an enumeration attack. From the gathered information, a malicious node may learn the following: the type of services being requested by SU nodes, the type of services offered by SP nodes, which and where the SD nodes are, and the network topology. Such information can be extremely useful for the malicious node and may be used subsequently: to infer or predict future service discovery patterns, or as intelligence for launching subsequent attacks (e.g. replaying certain messages). The disclosure of service information may be considered a breach of the individual entities' privacy.

   The direct threat targets are therefore the service messages, and the indirect threat targets include the privacy or even availability of the SU, SP and SD nodes. An information disclosure threat does not disrupt the service discovery process in any noticeable way. Very often, the legitimate service entities may not even be aware that such an attack is taking place. That is why this type of threat is also commonly known as a passive threat.

5. **Denial of Service (DOS).** This occurs when a legitimate service entity is prevented from participating in the normal service discovery process because of the actions of a malicious node. For instance, a malicious node may mount a DOS attack on an SP node by flooding the node with SrvReq messages. The SP node may be overwhelmed by these messages and hence be unable to accept legitimate SrvReq messages from other nodes. A competitor SP node may have strong motivation to launch such an attack. An SU node may also be the target of a DOS attack, even though the effects it has on the service discovery process are not as significant.

   A DOS attack could also be launched by flooding an SD node with illegitimate SrvReg and SrvReq messages. The effects of this attack could be deadly, as the entire service discovery process of the network could be crippled.

   Nodes may fail as a consequence of a DOS attack. The direct threat target would be the avail-

ability of the service entities that were subjected to the DOS attacks, while the indirect threat targets would be their respective reputations. DOS is an active threat.

6. **Elevation of Privileges.** This happens when a malicious node, by some illegitimate means, is able to gain more privileges than it currently has (Gollmann, 2005). This threat normally takes place in conjunction with the spoofing threat. When a malicious node is able to masquerade as another entity (e.g. an SU, SP, SD or FW node), it assumes the privileges and capabilities of that entity.

It should be noted that the aforementioned threats rarely occur in isolation. More often than not, one threat may lead to another, as they are inter-related.

5 SECURITY REQUIREMENTS

If the threats are not properly mitigated, they could be exploited by malicious nodes to launch a variety of attacks. Countermeasures are therefore essential to prevent the threats from being realised. The security services required to mitigate the threats are identified and presented below.

Authentication. One of the most important requirements is the mutual authentication of SU and SP nodes (in the immediate architecture) or SD and SU/SP nodes (in the mediated architecture). Mutual authentication will provide two interacting service entities with the assurance that they are indeed interacting with the intended parties. A rogue node may fraudulently request for/advertise a service. It may be difficult or impossible to prevent a rogue node from so doing, especially in immediate architectures, but an SU or SP node may decide not to use/provide the service if the authentication outcome is unsatisfactory. Unilateral authentication will not suffice in this sort of peer to peer environment, as it is equally likely for either an SU or SP node to be malicious. This security service aims to address the threats of spoofing and elevation of privileges.

Authorisation. An SU node may discover a number of available services in the network, but may only be allowed to use some of them, depending on the security policy specified by the SP nodes. Alternatively, a service may not even be discoverable by an SU node if it is unauthorised to use it. In other words, SU nodes may only have a controlled visibility of the available services, based on their credentials or some security policy. Similarly, only authorised SP nodes may be allowed to advertise their service offerings. Options for achieving authorisation include the use of capabilities, access control list and credentials. This security service does not directly mitigate any of the aforementioned threats. Nonetheless, it is important in the context of service discovery.

Confidentiality. A variety of service messages traverse the network during service discovery. A malicious node can easily intercept or eavesdrop on these messages and obtain the following information: the identities of the senders and intended recipients, the specific services that are being requested or advertised by an SU or SP node, the physical location of the service entities, etc. An SU (or even an SP) node may not want such information to be disclosed to other entities (malicious or not), apart from a legitimate SD node. It is therefore necessary to encrypt such messages to prevent the threat of information disclosure and to protect the privacy of service entities.

Integrity. Service messages, exchanged during service discovery, should not be modified (i.e. altered, deleted, inserted, or replayed). A secure service discovery protocol should provide this assurance to all service entities participating in the service discovery process. This security service addresses the tampering threat.

Non-repudiation. Mechanisms (e.g. digital signatures) should be in place to prevent any service entity from later denying that a certain action has taken place. For example, service entities should not be able to later deny that a particular service message was sent or received, if that action had indeed taken place. This security service addresses the threat of repudiation.

Accountability. A log that records all the events should be available. In the event of any dispute, a neutral adjudicator is able to refer to the log and make an impartial and accurate judgement. This requirement is closely related to the non-repudiation service, in the sense that it may be used to deter potential repudiation threats.

Availability. Malicious nodes should be prevented from flooding (e.g. using broadcast) the network with bogus service messages. A high volume of such messages could create a broadcast storm (Tseng et al., 2002) in the network. The resources of legitimate nodes may be depleted in an attempt to process such messages. The entire service discovery process could be crippled as a result. Instead of targeting the network, malicious nodes may also target individual nodes and flood them with messages. Appropriate measures are therefore required to thwart the denial of service threat.

Privacy. This requirement is closely related to the confidentiality service. Privacy may mean different things in different contexts; in the context of service discovery for ad hoc networks, protecting the privacy of the service entities means the following. Firstly,

service information should not be divulged to external service entities that are not directly participating in the service discovery process. Secondly, the identities of service entities should not be disclosed unnecessarily without the owner's permission. Thirdly, the physical location information of the service entities should not be revealed. Finally, colluding SP or SD nodes should not be able to correlate a particular SU node's actions. Like the confidentiality service, this service mitigates the effects of the information disclosure threat.

6 CONCLUSION

In this paper, we have presented a threat model in the context of which potential service discovery threats were identified and analysed according to the different types of node misbehaviour. We proceeded to derive the security services that are required to mitigate the identified threats. This work will provide a basis for the design of secure service discovery schemes.

We believe that the two most important security requirements that need to be addressed are mutual authentication followed by authorisation. Existing solutions for mutual authentication are not well suited for an environment such as an ad hoc network, as there is no central authority. Supporting mutual authentication between two interacting service entities is very challenging in such circumstances. The need to authenticate a specific identity may not be necessary if one entity is able to prove to the other that it is a trustworthy service provider or user.

Similarly, achieving authorisation in this sort of dynamic and peer to peer environment is particularly challenging for several reasons. Firstly, a central administrator does not exist to pre-specify a security policy. Secondly, service entities may belong to different administrative domains. Finally, authorisation can only take place after two service entities are mutually authenticated, which is still an unsolved problem. Fortunately, research on these authorisation problems has been conducted under the auspices of *Trust Negotiation*.

The dynamism of ad hoc networks has introduce many new and interesting security problems that call for new solutions.

REFERENCES

Gao, Z., Wang, L., Yang, M., and Yang, X. (2006). CNPGSDP: An efficient group-based service discovery protocol for MANETs. *Computer Networks*. (In Press).

Garcia-Macias, J. A. and Torres, D. A. (2005). Service discovery in mobile ad hoc networks: Better at the network layer? In *Proc of 34th International Conference on Parallel Processing (ICPP 2005)*, pages 452–457. IEEE ComSoc.

Gollmann, D. (2005). *Computer Security*. John Wiley & Sons, West Sussex, England, 2nd edition.

Guichal, G. and Toh, C. K. (2001). An evaluation of centralized and distributed service location protocols for pervasive wireless networks. In *Proc of 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2001)*, pages 55–61.

Lim, B.-I., Choi, K.-H., and Shin, D.-R. (2005). An architecture for lightweight service discovery protocol in Manet. In *Proc of 5th International Computational Science Conference (ICCS 2005)*, pages 963–966. Springer-Verlag LNCS 3526, Berlin.

Mishra, A. and Nadkarni, K. M. (2003). Security in Wireless Ad Hoc Networks. In Ilyas, M., editor, *The Handbook of Ad Hoc Wireless Networks*, chapter 30, pages 30.1–30.51. CRC Press, Boca Raton, FL, USA.

Mohan, U., Almeroth, K. C., and Belding-Royer, E. M. (2004). Scalable service discovery in mobile ad hoc networks. In *Proc of 3rd IFIP Networking Conference*, pages 137–149. Springer-Verlag LNCS 3042, Berlin.

O'Sullivan, J., Edmond, D., and Hofstede, A. (2002). What's in a service? Towards accurate description of non-functional service properties. *Distributed and Parallel Databases Journal*, 12(2/3):117–133.

Papadimitratos, P. and Hass, Z. J. (2003). Securing mobile ad hoc networks. In Ilyas, M., editor, *The Handbook of Ad Hoc Wireless Networks*, chapter 31, pages 31.1–31.17. CRC Press, Boca Raton, FL, USA.

Rao, R. (2004). Integration of on-demand service and route discovery in mobile ad hoc networks. Master's thesis, Dept of Computer Science, North Carolina State University.

Swiderski, F. and Snyder, W. (2004). *Threat Modeling*. Microsoft Press, Redmond, Washington.

Toh, C. (2002). *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Prentice Hall, Upper Saddle River, NJ, USA.

Tseng, Y.-C., Ni, S.-Y., Chen, Y.-S., and Sheu, J.-P. (2002). The broadcast storm problem in a Mobile Ad Hoc Network. *Wireless Networks*, 8(2-3):153–167.

Tyan, J. and Mahmoud, Q. H. (2005). A comprehensive service discovery solution for Mobile Ad Hoc Networks. *Mobile Networks and Applications*, 10(4):423–434.

Yau, P. W. and Mitchell, C. J. (2003). Security vulnerabilities in ad hoc networks. In *Proc of the 7th Int Symposium on Comms Theory and Applications (ISCTA'03)*, pages 99–104. HW Communications Ltd.

Zhou, D. (2003). Security issues in ad hoc networks. In Ilyas, M., editor, *The Handbook of Ad Hoc Wireless Networks*, chapter 32, pages 32.1–32.14. CRC Press, Boca Raton, FL, USA.