Preventing Impersonation Attacks in MANET with Multi-factor Authentication

Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris
Department of Informatics, University of Piraeus,
80 Karaoli & Dimitriou, 18534, Piraeus, Greece
{daglyn,pkotzani,cdoulig}@unipi.gr

Abstract

Existing MANET authentication schemes cannot fully protect nodes from well-known impersonation attacks. Although these schemes cryptographically link an entity to a claimed identity, the actual entity is never linked to the physical node device. However, the link is implicitly assumed. This shortcoming may be easily exploited within a MANET setting, due to the broadcast nature of the access medium. In this paper we propose a multifactor authentication framework that extends the cryptographic link, binding an entity to a physical node device. This is achieved by using two distinct authentication factors; certified keys and certified node characteristics. Although the proposed framework requires additional sensing capabilities from the MANET nodes, it provides the additional confidence level required for node authentication in critical applications.

1. Introduction

Mobile ad hoc networks (MANET) are a paradigm for wireless communication, where wireless nodes exchange information without relying on a fixed network infrastructure (*e.g.* static base stations) for services such as packet routing, name resolution, node authentication or distribution of computational resources. Furthermore, the nodes are mobile and this causes frequent changes to the network topology. Nodes within transmission range can communicate in a direct peer-to-peer manner. Nodes out of range may dynamically establish routing paths through other nodes if possible, otherwise they are disconnected. Such networks can be used in several areas, such as home networking, dynamic group communication, disaster recovery and military applications.

Security is a major issue, since the lack of fixed infrastructure makes the nodes particularly vulnerable to malicious attacks. Several security issues related to ad hoc networks have been discussed in the literature such as secure routing [4, 13, 2, 11], secure message transmission [14], key agreement [1] and intrusion detection [20].

Node identification and authentication are of fundamental importance within a security framework for networked nodes. Indeed, routing security, message transmission security and establishment of trusted paths depend on the ability of nodes to identify and authenticate each other in a secure way [17].

Several approaches to deal with node identification and authentication in MANET have been proposed in the literature. Zhou and Haas [21] propose the use of a distributed Certification Authority, based on threshold cryptography [5]. Hubaux *et al* [8] propose a scheme based on full distribution of certificates, with a trust model based on a PGP-like setting.

In this paper we discuss well-known impersonation attacks in MANET and we argue that any single factor authentication scheme cannot deal effectively with these attacks in the MANET setting. Then, we present a framework for multi-factor identification and authentication, which allows mobile nodes in MANET to identify and authenticate each other by examining a wide range of characteristics.

A key element to the proposed framework is that it combines well-known cryptographic mechanisms (such as digital certificates and signatures), with different sources of identification information. This information comes in the form of attributes describing physical node characteristics, much like the biometrical characteristics examined during human identification and authentication.

2. Impersonation attacks in MANET

Nodes in MANET are subject to several types of impersonation attacks, some of which are hard to deal with, even if authentication measures are enforced. This seems to be an inherent vulnerability of MANET protocols, caused by the ease of manipulation of the access medium (broadcasting). We describe these attacks below.

2.1. The Sybil attack

Without cryptographic means of node authentication, the nodes participating in a MANET are subject to a variant of impersonation attack, the Sybil attack [6]. Under the Sybil attack, a malicious node may present one or more fake identities to the other nodes of the network. If the nodes are cryptographically authenticated, then the Sybil attacks may be prevented or traced by legitimate nodes. However, the attacks described below may compromise the identity of a node even if the nodes have been cryptographically authenticated.

2.2. The Invisible Node attack

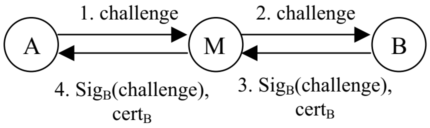
1. challenge
2. challenge
A
M
B
4. Sig$_B$(challenge), cert$_B$
3. Sig$_B$(challenge), cert$_B$

Figure 1. A special case of MIM attack – the Invisible Node attack

In MANET, communication is performed through broadcasting. This makes MANET routing protocols subject to a special case of Man-In-the-Middle (MIM) attack [3], the Invisible Node attack [12]. In its simplest form, the malicious invisible node M relays packets without revealing its presence in the routing path (see figure 1). This attack is very easy to implement in MANET: the malicious node M simply stands between two nodes A and B that are not in direct range. The invisible node silently repeats the communication between nodes A and B in the routing path, which misleadingly assume that they communicate directly. In this way, the malicious node succeeds in impersonating node A to node B and vice versa. Cryptographic authentication mechanisms, either public-key (such as signatures) or symmetric-key (such as keyed hash-values), are of no help in this type of attack: the attacker just relays the authenticators.

2.3. Stolen Identity attack

In the Stolen Identity attack, a node succeeds in stealing all the authentication credentials from a legitimate node, such as the certified signature keys (see figure 2). If the malicious node outraces the legitimate node in updating the stolen credentials through the certification authority, then the credentials of the legitimate node will not be valid anymore. Thus, only the malicious node will be able to use the updated certified credentials and in this way will succeed in stealing the identity of the victim node. Obtaining the signature key of a node within a PKI realm is not just a matter of stealing a node's identity, but also a matter of abusing the trust relationships that other parties may have had established with the compromised node. Again, cryptographic authentication mechanisms fail to deal with this type of attack.

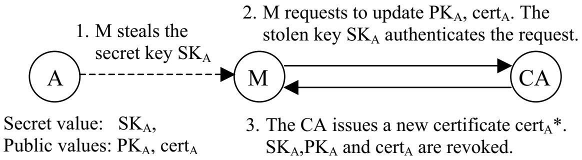
1. M steals the secret key SK$_A$
2. M requests to update PK$_A$, cert$_A$. The stolen key SK$_A$ authenticates the request.
A
M
CA
Secret value: SK$_A$,
Public values: PK$_A$, cert$_A$
3. The CA issues a new certificate cert$_A$*. SK$_A$,PK$_A$ and cert$_A$ are revoked.

Figure 2. The Stolen Identity attack

3. Towards multi-factor authentication for MANET

As illustrated in the previous section, identification and node authentication are susceptible to impersonation attacks regardless of whether the underlying scheme in use is cryptographically protected or not. This problem is common to all identification mechanisms that rely on a single authentication factor. The underlying authentication procedure gives a false sense of confidence about the identity of a node: the use of a certified key does not really ensure that the key was used by the legitimate key owner (identified in the corresponding digital certificate). Indeed, although an identity is cryptographically linked to a certain entity, this identity is never linked to the actual physical device (i.e. the MANET node), as illustrated in figure 3. Yet, this link is implicitly assumed.

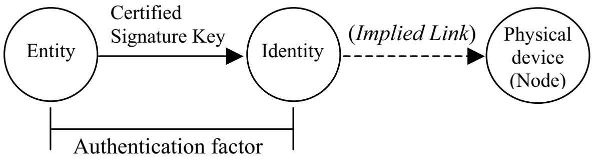

Figure 3. The Traditional Model of Entity Authentication

3.1. Identification attributes

Nature tackles the identification problem in a more "polyphonic" way. Identification is a process closely related to recognition. An entity identifies another (or the properties of the other) by means of visual information (e.g. an id card, a recognizable face, a recognizable certificate), aural information (e.g. tone of voice, recognizable patterns in speech), as well as by means of scent, taste, touch and of course behavior. Behavior is effectively a "meta-sense" since it is computed based on data provided by other senses. During the identification process, the human brain utilizes data from a mixture of the above inputs. Readings of such biometrical inputs essentially provide a link between a logical entity (with certain characteristics) and a physical object.

In order to achieve the same identification functionality in MANET, a set of "biometrical" (physical) characteristics of a node could be employed. The broadcast nature of MANET enables nodes to measure such characteristics of other node devices that lie within their transmission range.

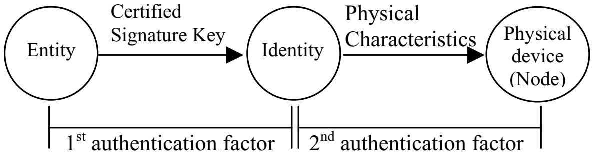

Figure 4. Multifactor Authentication

In this way, authentication of a neighboring node is performed in two steps (see figure 4). In the first step a certified signature key links an entity to a claimed identity (as in the traditional model). In the second step the readings of the physical characteristics of the examined node, link the physical node device to the claimed identity. Thus, the link between the entity and the physical device is not implicitly assumed; it is authenticated by two independent factors.

3.2. Selection criteria of identification attributes

The proper selection of physical characteristics to be examined is of outmost importance for the robustness of the authentication process. The physical characteristics (attributes) that will be used to identify a node should cover the following requirements:

- **Measurable by other entities.** Attribute values supplied by the examined node cannot be trusted, since these may have been forged to emulate the characteristics of some other node. Therefore, the selected characteristics must allow for direct or indirect remote evaluation. A directly measurable characteristic can be evaluated by any node within transmission range. An indirectly measurable characteristic requires cooperation between multiple (trusted) entities.

- **Hardware-based vs software-based attributes.** The examined characteristics of a node must be as close as possible to the hardware characteristics of the device and not to those of its software components. A software component may be programmed to respond in any way the attacker wishes to. However, software components play a significant role in the behavior of a node within a networked environment. Thus, they cannot be completely ignored during the identification process.

- **Weighted attributes.** Each attribute contributes to the identification process with a certain weight. For example, the signal characteristics that require special purpose hardware in order to be forged will be given a higher weight, while the software-based characteristics, which are more easily spoofed, will be given a much lower weight. The combination of various weighted attributes will output the identity of a node in the network with a certain level of confidence.

3.3. Candidate identification attributes

Based on the above requirements, candidate attributes that can be used for node identification in MANET include:

- **Radio Frequency Fingerprint (RFF).** With RFF techniques, features extracted from a node's transmitted signal can uniquely identify the node device as a piece of circuitry. Specifically [15, 19, 7], discuss three approaches (Threshold, Bayesian Step Change Detector and Signal Phase respectively) for extracting such features from the radio frequency turn-on transient. Nodes enabled to extract the RF fingerprint from the transmitted signal of other nodes within range can use this attribute to strengthen their confidence about the claimed identity of a neighboring node. For example, in a Stolen Identity attack scenario (2.3), the imposter node will be spotted, since its fingerprint will not match the fingerprint of the legitimate node.

- **Radio Frequency Watermark Verification.** During data transmission, a transmitter can modify its signal through a watermarking technique as described in [9]. By analyzing the watermark signature embedded within the signal of a transmitter, a receiver can further verify its belief about the identity of the transmitter.

- **Transmission Coverage.** This is a composite attribute based upon Node Position and Transmission Range. Node Position (signed time and location information) can be discovered by means of a GPS or node triangulation service (see [16]). The maximum Transmission Range of a node's antenna is fixed and depends on the node's manufacturer and model. Transmission Coverage is a combination of the latter two characteristics, describing the current geographical coverage of a node's transmission. It can be used to verify that two peer nodes A, B, can actually communicate directly *i.e.* $\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2} \leq \min{(r_A, r_B)}$, where (x_i, y_i) are the current coordinates and r_i is the transmission range of node i. If the transmission coverage of the two nodes does not overlap, an Invisible Node attack (2.2) may be taking place.

Table 1 illustrates the relative strengths and weaknesses of identification methods based on the above attributes.

	Can be spoofed?	**Affected by poor SNR?**	**Requires external trusted entity during verification?**
PKI	Yes, see 2.3	No	Yes, the CA
RFF	Requires special hardware to immitate turn-on transient behaviour	Yes, see [7]	No
RF Watermark	Yes, but requires programmable transmission layer	Poor SNR requires higher watermark bit-rate	No
Trans. Coverage	No, but not very accurate due to node mobility	No	Yes

Table 1. Strengths and Weaknesses of Identification Methods

4. A multi-factor authentication framework for MANET

The proposed authentication framework hardens node authentication by combining traditional cryptographic techniques (certified keys and digital signatures) with certified physical attributes, which are used as additional authentication factors. Authentication between neighboring nodes is performed in several steps. The nodes will first challenge one another with a random message and they will verify the digital signature of each other. Then, each peer node will perform readings on the physical attributes of the other node and will compare these readings against a set of certified values. The confidence about the authenticity of a claimed node identity depends on the verification of the examined attributes.

4.1. Setup

We assume that each node is pre-deployed with a public/secret key pair (PK_i, SK_i) of a public key cryptosystem and that the nodes are capable of computing/verifying digital signatures. For efficiency, an Elliptic Curve Cryptosystem may be more preferable in a MANET environment [10].

We also assume that prior to the entry of a node to the MANET, a trusted authority makes a series of readings, in order to measure the values of a set of physical attributes, which will later be used in the authentication process. These readings are performed in a monitored environment that allows for high accuracy. Additionally, we assume that the nodes are properly equipped with hardware and/or software, which enables them to take readings on the attribute values of other peer nodes within range. This may significantly increase deployment costs and make the proposed authentication framework suitable mainly for security-critical MANET applications, such as tactical applications.

Finally, we assume that the public key and selected physical attribute values of each node are certified through a distributed trusted Certification Authority CA [21] prior to the entry of a node in the MANET. This can be implemented through X.509 certificates, where the values of the physical node attributes can be considered as additional certificate attributes. Thus, the CA will issue for each valid node n_i a signed certificate of the form:

$$Cert_i = (ID_i, PK_i, T, T_{exp}, Attr_1, ..., Attr_k)_{CA}$$

where ID_i is the unique node identifier, PK_i is the public key of the node, T, T_{exp} are the issue and expiration times respectively and $Attr_x$ is the value of physical attribute x of the node. The certificate is signed by the CA and given to each node.

4.2. Node authentication

Network nodes can now use their certified keys and attributes in order to authenticate each other. Let us consider a scenario where node A authenticates node B. The following steps are performed:

1. Node A sends a challenge message to node B containing a random string.

2. Node B replies with a signed message on the received challenge along with its certificate.

3. Node A verifies the signature of node B. If the signature is invalid, authentication fails. Otherwise, the authentication process proceeds to the next step.

4. Node A takes a series of readings on the characteristics of node B. This process may involve several interactions between the two parties. For attributes that cannot be measured directly, an indirect method of measurement is deployed, where the required values are retrieved from a trusted source, as described in 3.2.

5. The authentication process proceeds with the examination of the attribute values collected in step 4. These are verified against their certified values, that are contained in $Cert_B$. Each examined attribute contributes with a certain weight to the output of the authentication process.

6. The final outcome is a number between 0 and 1, describing the *confidence level* on the result of the primary authentication factor (signature and certified key).

In this way, the certified signature key becomes the first authentication factor, while the certified attributes act as additional authentication factors.

4.3. Implementation

Each node manages a collection of attributes. Depending on their nature, these may be of type Singleton (*e.g.* an integer, a string, an IP address), Set (*e.g.* signal peak values), or Range (*e.g.* signal strength). A table of *Host Attribute Sets* holds the values of the measured attributes of each node, as illustrated in figure 5. Along with temporary attributes that may be of local use to the node, the Host Attribute Set contains a set of well-known attributes, a (commonly agreed) subset of which shall be used during the authentication phase.

Each attribute is being computed by a separate piece of software, called the *Attribute Module*. Given the claimed node identifier ID_i of the examined node, the Attribute Module will perform a series of queries and/or readings and will eventually provide a value for the computed attribute $Attr_j$ to the Host Attribute Set. Subsequently, it will verify the measured attribute value against the examined node's certificate. The output of this verification process is a quantity p_j describing the probability that the measured attribute $Attr_j$ is a true characteristic of the node described in the certificate.

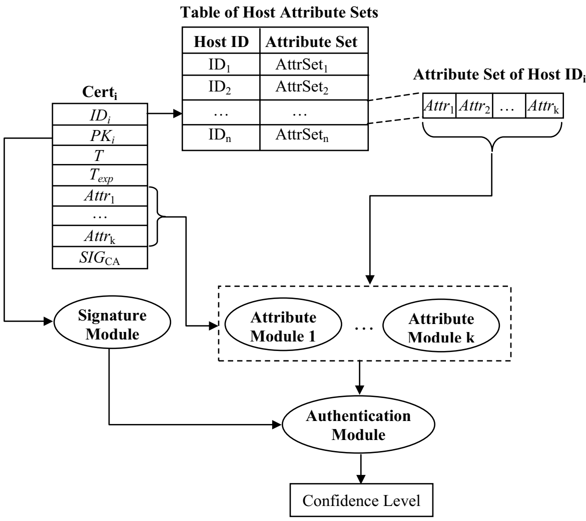

Figure 5. Attribute Management

An *Authentication Module* is responsible for applying a weight w_j to the outcome p_j of each Attribute Module and producing a *Confidence Level* $C(ID_i)$. This Confidence Level describes the possibility that the examined node ID_i is the one described in the node certificate, provided that the signature of the examined node was verified by the *Signature Module* (as described in step 3 of Section 4.2). The Confidence Level can be computed by a simple mean function, such as:

$$C(ID_i) = \frac{\sum_{j=1}^{n} w_j p_j}{\sum_{j=1}^{n} w_j}$$

A more "intelligent" Authentication Module may take into account the conditional dependencies that may exist within a set of Attributes and thus make use of a Bayesian network while computing the Confidence Level.

The level of confidence that would be considered satisfactory for the approval of the authentication request (threshold θ) depends on the nature of the MANET use. For tactical applications, θ will receive a substantially higher value than the one used in applications for home networking, because the danger of mis-identification in the latter is less critical. As θ grows, the authentication process requires more measurements in order to verify the identity of a node. The threshold θ is also affected by any factors that may degrade the performance of the Attribute Modules, such as noise and signal interference. These factors contribute to poor measurements and production of low probabilities p_j. It is thus desirable for the threshold θ to re-adjust in order to compensate for such errors in the measurement process.

Host Attribute Sets and Attribute Modules reside within the operating system kernel of the MANET node, since they require direct access to the various layers of the kernel, especially the networking stack and the network interface driver. The Attribute Modules provide a standard API through which: a) user-space programs may retrieve values and configure a Module's operation, b) Attribute Modules may contact one another and exchange information, and c) other operating system kernel code can register callbacks and supply data to Attribute Modules. Attribute Modules may also be implemented as Active Applications running on an Active Node [18]. The dynamic nature of code run within an Active Network provides us with a plethora of possibilities for attribute testing and information exchange between the Attribute Modules.

5. Discussion

Traditional authentication mechanisms cannot deal with several impersonation attacks in MANET. This seems to be an inherent weakness in MANET caused by the ease of manipulation of the broadcasting access medium. The proposed authentication framework attempts to deal with these attacks by combining multiple authentication factors based on node characteristics. By combining certified signature keys with certified attributes, a claimed identity can be linked with a higher confidence to a physical node device. The certification of the node attributes can be easily managed by employing the X.509 certificate format. Indeed, the current version of X.509 can include public keys as well as additional attributes.

An implementation of the proposed multifactor authentication framework requires special-purpose hardware, for both node attribute certification (during the setup phase) and measurement (during the authentication phase). However, the additional costs can be justified for critical applications in hostile environments.

References

[1] N. Asokan and P. Ginzboorg. Key-agreement in ad-hoc networks. In *Proceedings of the 4th Nordic Workshop on Secure Computer Systems*, 1999.

[2] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An on-demand secure routing protocol resilient to byzantine failures. In *Proceedings of the ACM workshop on Wireless security*, pages 21–30, 2002.

[3] S. Bengio, G. Brassard, Y. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175–184, 1991.

[4] M. Burmester and T. van Le. Secure multipath communication in mobile ad hoc networks. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004)*, Las Vegas, Apr. 2004. IEEE.

[5] Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(4):449–457, 1994.

[6] J. R. Douceur. The sybil attack. In *First International Workshop on Peer-to-Peer Systems (IPTPS '02)*. American Mathematical Society, Mar. 2002.

[7] J. Hall, M. Barbeau, and E. Kranakis. Detection of transient in radio frequency fingerprinting using phase characteristics of signals. In *Proceedings of 3rd IASTED International Conference on Wireless and Optical Communications (WOC 2003)*, pages 13–18, Alberta, Canada, July 2003. ACTA Press.

[8] J. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proceedings of the 2nd MobiHoc Conference*, BA, Massachusetts, Aug. 2001.

[9] J. Kleider, S. Gifford, S. Chuprun, and B. Fette. Radio frequency watermarking for OFDM wireless networks. In *Proceedings of Acoustics, Speech, and Signal Processing (ICASSP'04), Vol.5*, pages 397–400. IEEE, May 2004.

[10] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1997.

[11] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris. Multipath routing for mobile ad hoc networks. In *Proceedings of the Second Annual Conference on Wireless On Demand Network Systems and Services (WONSS '05)*, St. Moritz, Switzerland, 2005. IEEE.

[12] J. Marshall, V. Thakur, and A. Yasinsac. Identifying flaws in the secure routing protocol. In *Proceedings of the 22nd International Performance, Computing, and Communications Conference*, pages 167–174, Apr. 2003.

[13] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, TX, San Antonio, Jan. 2002.

[14] P. Papadimitratos and Z. Haas. Secure message transmission in mobile ad hoc networks. *Elsevier Ad Hoc Networks*, 1:199–209, 2003.

[15] D. Shaw and W. Kinsner. Multifractal modelling of radio transmitter transients for classification. In *Proceedings of Conference on Communications, Power and Computing*, pages 306–312, 1997.

[16] J.-H. Song, V. W. Wong, and V. C. Leung. A framework of secure location service for position-based ad hoc routing. In *Proceedings of 1st International Conference on Mobile Computing and Networking archive*, pages 99–106, Venezia, Italy, 2004. ACM.

[17] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, Cambridge, UK, 1999.

[18] D. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall, and G. J. Minden. A survey of active network research. *IEEE Communications Magazine*, 35(1):80–86, 1997.

[19] O. Ureten and N. Serinken. Bayesian detection of radio transmitter turn-on transients. In *Proceedings of NSIP99*, pages 830–834, 1999.

[20] Y. Zhang and W. Lee. Intrusion detection in wireless adhoc networks. In *Proceedings of the 6th Conference on Mobile Computing and Networking*, Boston, USA, 2000. ACM/IEEE.

[21] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, Nov. 1999.