IDENTITY BASED PUBLIC KEY EXCHANGE (IDPKE) FOR WIRELESS AD HOC NETWORKS

Clare McGrath, Ghazanfar Ali Safdar and Máire McLoone
Institute of Electronics, Communications and Information Technology (ECIT)
Queens University Belfast, Belfast, Northern Ireland

Keywords: Ad Hoc Network, Key Management, Identity Based, Security.

Abstract: In this paper a novel identity based public key exchange (IDPKE) protocol is proposed for wireless ad hoc networks, where the network node IDs are used as public keys. Previous research into ID based key management schemes assumes that node IDs are well known and have been distributed amongst the nodes at the time of network formation. However, this assumption limits the application of these schemes to many ad hoc networking scenarios. Our proposed IDPKE protocol addresses this disadvantage. It assumes that node IDs are not known prior to network formation and provides secure and authentic ID exchange between nodes, thus allowing employment in a wider range of applications. The IDPKE protocol is an extension to an existing certificate based scheme and it provides an increase in security and a reduction in computation and bandwidth by comparison.

1 INTRODUCTION

Ad hoc networks are used by the government and military and in every day applications such as security surveillance and traffic monitoring. As such, they need to be secured, and efficient and secure key management/authentication schemes designed specifically for ad hoc networks are required. A significant number of such schemes have been proposed in the literature and are reviewed and categorised in (McGrath *et al*., 2006, Hoeper and Gong, 2004).

In this research we investigate identity (ID) based schemes due to the fact that they can cut down on complexity and the computational and memory requirements of nodes compared to certificate-based techniques (Khalili *et al*., 2003). However, one outstanding issue with these schemes, which we address in this paper, is the assumption that node IDs are known prior to communication with each other in a network. This assumption is made because the node IDs are considered to be well known pieces of information. However, IDs are strings of information bound to particular entities and this type of information will depend on the entity and application (Hoeper and Gong, 2006). It cannot always be assumed that IDs will be known by other users prior to communication. Also, this limits the type of ID that can be used and therefore limits the application. If IDs are assumed to be unknown when the network forms and a secure and authentic ID distribution scheme is provided, then a wider range of IDs can be used and the scheme can be applied to a wider number of applications.

This paper presents a novel ID-based Public Key Exchange (IDPKE) protocol where nodes can distribute and authenticate their IDs/public keys for use in an ID-based cryptographic scheme. To the authors knowledge this is a new concept compared to the ID-based key exchange protocols that have been previously proposed. The IDPKE protocol meets the specifications of the key exchange framework proposed by McGrath *et al.* (2006) and builds upon a certificate-based scheme known as OPKM (Li, X. *et al*., 2004). We show how savings can be made on bandwidth and computational requirements and how an improvement in security is achieved in comparison to the OPKM scheme.

The paper is organised as follows: Section 2 discusses previous research in this area. Section 3 outlines the proposed IDPKE scheme while section 4 reviews its computational and communicational aspects. Section 5 discusses the protocol's security strengths and conclusions are provided in section 6.

McGrath C., Ali Safdar G. and McLoone M. (2007).
IDENTITY BASED PUBLIC KEY EXCHANGE (IDPKE) FOR WIRELESS AD HOC NETWORKS.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 167-170
DOI: 10.5220/0002123101670170

2 PREVIOUS RESEARCH

In 2004, Li, X. *et al.* (2004) proposed a fully self-organised certificate based key management and authentication scheme which tackled the problems of earlier similar schemes by Zhou and Haas (1999) and Capkun *et al*. (2003). These problems included the lack of node availability to form a key management service, the use of heavy computation in the form of threshold cryptography and maintaining certificate graphs. However Li *et al.*'s scheme introduced some new security issues that are described in section 5.

Also, it can be argued that the use of certificates at all in these schemes requires too many computational/communicational resources than can be provided by the nodes of an ad hoc network (Hoeper and Gong, 2004). The aim of ID-based schemes (Deng *et al*., 2004, Khalili *et al*., 2003) is to remove certificates completely and therefore reduce computation and bandwidth whilst still providing the authentication that certificates provide. However, these schemes also suffer from the same availability problems and the heavy threshold cryptography computation mentioned previously. Hoeper and Gong (2006) proposed a scheme which investigated the disadvantage of unavailable online PKGs but their scheme assumed that the IDs of the nodes are known prior to joining the network. In this paper, we introduce a secure key management scheme, which does not assume knowledge of IDs prior to communication.

3 PROPOSAL

3.1 Network Model and Assumptions

- The network consists of an offline trusted central entity (Private Key Generator (PKG)) with enough computing power to handle identity-based private-key generation and sufficient memory to store the identities of all the nodes on the network.
- The PKG generates the public and private system parameters (can be based on those of the Boneh-Franklin identity-based encryption scheme (Boneh and Franklin, 2001) or others that have improved on this).
- The network contains a variable number of nodes that can join and leave at any time. When joining the network, the nodes must first make contact with the PKG (using a physical wired connection or secure side channel).
- The PKG assigns each node a unique ID which is also the node's public key and it is unknown to other nodes until the IDPKE sequence has been carried out. For example, this could be the network IP address of the node and no two nodes will be assigned the same address. An assigned ID will also never be reassigned with the same master parameters, even after the original node has left the network. The PKG also calculates a private key using this ID and the master private key associated with the ID-based encryption schemes (parameter known only to the PKG) and loads the node with all the public parameters of the scheme and the node's private key.
- Online nodes act as transceivers and can be stationary or mobile. They may be identical in terms of computing power and memory but they must have enough computational ability to handle ID-based encryption and enough storage to hold a sufficient number of IDs depending on the application. They will also have omni-directional broadcasting capabilities which will most likely be within a short range. They can store two tables of IDs, the one-hop and two-hop table, for nodes that are within a one-hop or two-hop range respectively.

3.2 IDPKE Scheme

IDPKE describes the events that take place when a new node joins the network or moves to a new position. It proceeds as follows:

After contacting the PKG, a node N_i joins the network and broadcasts a "*hello*" message to its n one-hop neighbours (N_j). The contents of the message are that of the hello field and a timestamp (T_S) to ensure data freshness and to prevent replay attacks. These contents are then encrypted with the private key of the sender.

$$N_i \Rightarrow N_{j(n-x)\ldots.N_{jn}} : (ID_i), [\mathrm{Epk_i}(\text{"}hello\text{"}, TS_i)] \quad (1)$$

Message 1 shows that the ID of the sender node (ID_i) is also present since the ID will automatically be sent within the address field of the packet.

The one-hop neighbours use the ID/public key to decrypt the contents of the message and verify that the message was sent by node N_i, since only node N_i holds the corresponding private key. The verification also provides an assurance that the sending nodes contacted the PKG before joining the network to receive a legitimate ID and

corresponding private key. The one-hop receiver nodes update their one-hop ID table using this unique address.

Next, the receiver nodes reply to N_i by broadcasting "*welcome*" messages, which also include a timestamp and the IDs of their *m* one-hop neighbours (N_k).

$$N_{j(n-x)\ldots..} N_{jn} \Rightarrow N_i : \\ (ID_j), [\ \mathrm{Epk_j}(\text{“}welcome\text{”}, TS_j, ID_{k(m-x),\ldots\ldots,}ID_{km}) \quad (2)$$

Again the contents of the messages are encrypted with each of the sender nodes' private keys. N_i can verify that the public key in the address of each packet corresponds to the private key used to encrypt it by decrypting each message successfully. The replies of the sending nodes are sent after chosen random times T_R to avoid bombarding N_i with incoming messages. Since nodes can hear the replies their one-hop neighbours broadcast to N_i, all nodes within two hops of N_i can verify that their public information (ID) has been distributed. If nodes can record incorrect/omitted publications from others, malicious behaviour can be caught out. This is Li *et al.'s* (2004) process known as neighbourhood monitoring.

Once each node, including N_i, is satisfied that the information is correct, they update their one and two-hop ID tables according to the IDs in the reply messages and the ID of the sender itself, if these IDs are new. If a node finds the information from a particular node is not satisfactory, i.e. its ID was omitted from the broadcast of a certain node, it can broadcast a correction message, which will include the correct information.

$$N_i \Rightarrow N_{j(n-x)}: (ID_i), [\mathrm{Epk_i}\ (\text{“}correction\text{”}, ID_j, TS_i)] \quad (3)$$

The correct ID of the omitted node (ID_i) is the address from which the correction message originated. The contents of the message include a field indicating it is a correction message along with the ID of the node that sent the incorrect message (ID_j) and a timestamp. Nodes receiving the correction message can forward the message, including the omitted ID within the message contents, to ensure the correction message reaches all the two-hop neighbours of the omitted node.

Nodes may then set a "Don't trust" flag against the sender of the incorrect message such that they know this node may not be trusted in the future. After time T_U, N_i broadcasts an update message to its one-hop neighbours. T_U is defined to ensure N_i is able to receive all the reply messages from its one-hop neighbours. The update message contains all its one-hop neighbours' IDs. Nodes receiving this message verify the information against their own and update their tables if any new information is received.

$$N_i \Rightarrow N_{j(n-x)\ldots..}N_{jn} : \\ (ID_i)[\mathrm{Epk_i}\ (\text{“}update\text{”}, TS_i, ID_{j(n-x)}, \ldots., ID_{jn})] \quad (4)$$

If after time T_C, N_i has not received any correction messages, it may assume that the IDs it has received are correct. IDPKE thus enables each node to obtain all the IDs (IP addresses) and therefore all the public keys of its neighbours within two hops in a trustworthy manner. When a node moves to a new position in the network, it initiates the process again. This allows nodes to ensure that the information they have stored about other nodes in the network remains current even while nodes are moving about and are joining or leaving the network. Once nodes have received the IDs of nodes in the local neighbourhood, they can proceed with secure encrypted messaging.

4 PERFORMANCE DISCUSSION

The ID-based encryption used in the IDPKE messages is based on elliptic curve cryptography giving savings in computation compared to the RSA-based digital signature schemes (Khalili *et al*., 2003) used in OPKM. There is no hashing involved in IDPKE, unlike OPKM, which involves both hashing and encryption. Also, RSA-based schemes use public keys that are 1024 bits in size as opposed to the much shorter keys used in ID-based cryptosystems (e.g. if using an IP address, this is only 32 bits in size). The use of smaller keys reduces computation, communication overhead and storage (Deng *et al*., 2004). Communication overhead is also reduced because IDPKE distributes less data than OPKM which distributes certificates. In addition, storage overhead is reduced in IDPKE since there are no certificates. Finally the use of the offline entity in IDPKE shifts key generation computation from the individual nodes, thus reducing node computation in comparison to OPKM.

5 SECURITY DISCUSSION

The main attacks that key management schemes for ad hoc networks have to face are denial of service (DoS) attacks and man-in-the-middle (MiM) attacks.

These can be carried out in different ways: illegitimately, legitimately or by impersonation.

The illegitimate node attack is when a malicious node joins the network with a fake ID and without contacting the PKG. It will therefore not receive a matching private key and will behave maliciously when it joins the network. Any messages they send however will be ignored as they will have no private key to sign them. This attack can therefore be prevented in IDPKE.

The legitimate node attack is more serious and it happens when a node joins the network legitimately but acts maliciously. It therefore contacts the PKG and receives a legitimate ID and matching private key but it behaves maliciously when it joins the network by trying to flood the network with false IDs (DoS) or by ignoring or forwarding on false/modified IDs (MiM). The attack worsens if a number of legitimate nodes decide to act together and behave maliciously. If false information has been transmitted by a legitimate node, it can be defended against using neighbourhood monitoring in both IDPKE and OPKM. An attack involving a number of legitimate nodes acting together and behaving maliciously cannot be defended against (in both IDPKE and OPKM) as it would be impossible to determine which information is correct or incorrect.

The impersonation attack is when a malicious node joins the network and masquerades as another legitimate node in the network in order to modify public information or flood the network with false information. The OPKM approach does not prevent such attacks outright. However, IDPKE can defend against impersonation attacks. In IDPKE the legitimate node has a matching private key and will sign all outgoing messages with this key. A malicious node will not be able to derive this key and will not be able to contact the PKG for access to the key as the PKG will only issue one private key per node ID, therefore any unsigned outgoing messages from this node will be ignored. It will also not be able to decrypt any secure messages that have been encrypted with that ID/public key. Hence signing with the private key ensures the receiver that the message definitely originated from the node with the ID contained in the message and that the ID was not modified.

6 CONCLUSIONS

By modifying a fully self organised certificate based key management scheme to a partially self-organised identity-based scheme, we have provided a more complete solution for existing ID-based schemes, allowing the use of different types of IDs and more accessibility to different ad hoc scenarios and applications. The proposed IDPKE protocol improves on the certificate based schemes in terms of security against impersonation attacks and in terms of computation and communication overhead making it more accessible to constrained devices.

REFERENCES

Bertoni, G.M., Chen, L., Fragneto, P., Harrison, K.A., Pelosi, G., 2005. *Computing Tate Pairing on Smartcards*. Available at http://www.st.com/stonline/product/families/smartcard/ches2005_v4.pdf.

Boneh, D., Franklin, M., 2001. *Identity-based Encryption from the Weil Pairing*, SIAM J. of Computing Vol.32, No.3, pp.586-615, 2003. Extended Abstract in Proceedings of Crypto 2001, vol.2139 of Lecture Notes in Computer Science, pages 213-229, Springer-Verlag, 2001.

Capkun, S., Hubaux, J.-P., Buttyan, L., 2003. *Self-Organized Public-Key Management for Mobile Ad Hoc Networks*, IEEE Transactions on Mobile Computing, vol.2, no.1, 2003, pp.52-64.

Deng, H., Mukherjee, A., Agrawal, D.P., 2004. *Threshold and Identity Based Key Management and Authentication for Wireless Ad Hoc Networks*, ITCC.

Hoeper, K., Gong, G., 2004. *Models of Authentications in Ad Hoc Networks and Their Related Network Properties*, CACR technical report.

Hoeper, K., Gong, G., 2006. *Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Revocation*,Waterloo Tech. Report.

Khalili, A., Katz, J., Arbaugh, W., 2003. *Toward Secure Key Distribution in Truly Ad Hoc Networks*, 2003 Symposium on Applications & the Internet Workshops (SAINT'03), IEEE Comp. Soc.

Li, X., Gordon, S., Slay, J., 2004. *On Demand Public Key Management for Wireless Ad Hoc Networks*, Proc of the Australian Telecommunication Networks & Applications Conference, Australia, Dec 2004.

McGrath, C., Safdar, G., .McLoone, M., 2006. *Novel Authenticated Key Management Framework for Ad Hoc Network Security*,IEE Irish Signals and Systems Conference, Dublin, June 28-30, 2006.

Zhou, L., Haas, Z., 1999. *Securing Ad Hoc Networks*, IEEE Network Journal, vol.13, no.6, 1999, pp.24-30.