HYBRID KEY MANAGEMENT FOR MOBILE AD HOC NETWORKS

David Sanchez Sanchez, Heribert Baldus
Philips Research Laboratories, Weisshausstrasse 2, Aachen, Germany
david.s.sanchez@philips.com, heribert.baldus@philips.com

Abstract: Many public key infrastructure (PKI) approaches have been proposed in the recent years to secure mobile ad hoc networks (MANETs). We present a new hybrid key management infrastructure, which combines the concepts of PKIs for MANET with trusted-third-party based infrastructures. In our hybrid approach, the underlying PKI is merely used to set-up initial trust of nodes in a MANET, and, thus, generate a random trust graph connecting all the nodes of the MANET. Then, MANET nodes cooperate to securely distribute trust information and symmetric keys to other nodes through the shortest trust path. The hybrid key management infrastructure enables the same security services as a normal PKI yet key establishment and node-to-node authentication, as demonstrated by our performance analysis, is substantially improved in terms of computational and communication efficiency. We also discuss the security level of the hybrid approach.

1. INTRODUCTION AND MOTIVATION

MANETs are wireless ad hoc networks increasingly deployed for multiple *civilian* applications. Key management is paramount for enabling security in MANETs.

In this paper, we propose a new hybrid key management infrastructure for MANETs, which perfectly trades off security and efficiency, by setting a middle point between the two general key management infrastructures, i.e. PKI and TTP based. PKIs[1,13] enable confidentiality, integrity, authentication and non-repudiation services in a very flexible way. However, existing proposals[2,6-8,15,18] for MANET do not offer optimal performance. Trusted-third-party (TTP) based infrastructures[1,13] enable confidentiality, integrity and authentication services in a performance efficient manner.

However, applying the TTP concept to MANETs is not straightforward because MANETs lack of security servers.

The remainder of this paper is organized as follows. In Section II, we review relevant related work. In Section III, we describe the hybrid key management infrastructure for MANETs. The performance and the security level of the hybrid approach are assessed and compared with related work in Section IV and Section V, respectively. Finally, Section VI concludes this paper.

2. PUBLIC KEY INFRASTRUCTURES FOR MANET

A very simple PKI can be enabled with an offline CA[17]. This approach provides nodes with one or more digital certificates in a bootstrapping phase. Afterwards, the MANET nodes can establish keys, authenticate and even sign messages using their private/public key pairs, without the need to contact the CA anymore. However, node revocation is not possible without further control mechanisms.

Many papers address the use of threshold cryptography to distribute PKI certification authority (CA) functionalities to n MANET nodes denoted servers[3-6]. The CA private key is divided into n shares using $(n, t+1)$ threshold cryptography and, then, distributed among the n servers. A number $t+1$ of partial signatures are needed in the generation of new certificates. Then, this approach increases security robustness and availability in the presence of security attacks from malicious nodes and compromised nodes.

Capkun et al.[2] propose a fully self-organized PKI for MANETs that allows users to generate their public/private key pairs and to issue certificates to other users. Revocation of nodes is also enabled. Their proposal is similar to the concepts of key generation and certificate issuing of PGP[14,13]. PGP's web-of-trust model defines different trust levels (complete, marginal and notrust) for public keys, i.e. for what and how much a node is trusted.

A number of proposals[6-8,18] exploit the clustering infrastructures of some MANETs to propose self-organized or distributed PKIs. Cluster heads are generally nodes with higher computational capability, which play the role of a (distributed) CA. They issue, renew and revoke public key certificates to MANET nodes within the same cluster. Additionally, different cluster heads can coordinate to build a MANET-wide PKI.

Martucci et al.[15] propose a PKI-based security architecture for small and medium-sized MANETs. MANET nodes must obtain valid trust information and public keys from the CA before they can join and communicate in the MANET.

3. HYBRID KEY MANAGEMENT

3.1 Assumptions

We assume a wireless MANET composed of self-organized mobile nodes and without online access to any fixed network infrastructure. Sporadically new nodes join or leave the MANET. Typical MANET devices, considered in this paper, are PDAs, mobile phones, and embedded systems in portable devices. These devices have moderate computing power and storage resources as well as limited battery power life. Nodes are capable of computing public key operations to the cost of a significant downside effect in their performance.

We target civilian applications in which devices are carried/wore or placed around human users, i.e. nodes are not generally left unattended, and, then the risk of node compromise by an attacker is very low. Misbehaving users may try to fake information in their behalf or in behalf of their "mates". They may also not cooperate. Furthermore, an attacker may exploit the vulnerabilities of wireless transmissions to anonymously eavesdrop, modify, replay or inject bogus messages.

For the descriptions in the rest of the paper, we assume a MANET with P nodes. We use A, B, W, V, Y, X and Z to refer to some generic nodes of the MANET.

3.2 System Bootstrapping

We assume the existence of a MANET PKI[2,6-8,15,17,18] underlying the hybrid key management infrastructure. The PKI provides each MANET node X with a public key certificate, which digitally binds its identity with the corresponding public key. The certificate may additionally include the level of trust TL_X in the public key of node X (This is of special relevance in PKIs based on web-of-trust models[2,14]). Furthermore, other operations of the PKI such as certificate renewal and revocation may be enabled. Trust information related to a node may be dynamic[15] and evolve throughout MANET lifetime.

3.3 Trusted Portal Establishment

In joining the MANET, each node V arbitrarily selects another node Y from the ones present at the MANET. Then, both nodes mutually authenticate by using their certified public keys. This mutual authentication

establishes a bi-directional trust relationship between both nodes, which is required for "Nodes Trust and Key Establishment".

Assume that, from a MANET with nodes *A*, *B*, *V*, *W*, *X* and *Z*, node *Y* selects node *X* as its initial trusted node. In future communications, *Y* will use *X* as a portal to address other nodes of the same MANET securely and efficiently. Therefore, we call *X* a *Trusted Portal* (TP) for *Y*. In the following we use *TP-X* to denote "*node X serving as TP*".

In a hybrid key management infrastructure, with a very simple underlying PKI, all the MANET nodes may have associated the same level of trust. Thus, in such case, all of them can serve as TPs. Conversely, in others, only nodes with special permissions may be allowed to serve as TPs. Finally, with web-of-trust models based PKIs, a node may need to possess a sufficient level of trust to be accepted to act as TP. For instance, using PGP's terminology[14], node *X* can act as TP if and only if its public key is associated a *complete* trust level.

A node *Y*, whose current TP is *TP-X*, must establish a new TP, when node *X* quits the MANET.

3.3.1 Trusted Portal Domain

Because each and every node of a MANET must follow the "TP Establishment" process and TPs are randomly selected, more than one node may establish initial trust with the same node X. We define as TP-X domain the group of MANET nodes associated to TP-X and, from now on, use D_{TPX} to denote TP-X domain. For instance, in Figure 1, domain D_{TPX} includes Y and W (which are depicted as TP-Y and TP-W because they also have respective TP domains) as trusted nodes of TP-X. TP-X is the domain administrator of its own domain D_{TPX}.

3.3.2 Generation of MANET Trust Graph

A consequence of the "TP Establishment" process is that one or more TPs are randomly set in the MANET. Because these TP nodes are selected randomly, a random trust graph connecting different nodes in the MANET is generated. Figure 1 shows an instance of a trust graph formed with nodes *A*, *B*, *W*, *V*, *Y*, *X* and *Z*.

We can guarantee the continuous existence of a random trust graph without isolated cycles under the following two conditions. First, each and every node of the MANET must *dynamically* initialize trust with an own selected TP, i.e. a node repeats the "TP Establishment" process in joining the MANET and when its TP disappears. Second, a node, which is serving as TP in the moment it selects its own TP, must choose as TP a node not included

in its TP domain or sub-domains (e.g. in Figure 1, *TP-Y* cannot select nodes *V* or *Z* as TP). If this condition cannot be satisfied for a node (e.g. *X* in Figure 1), then such node should not select any TP.

It is easy to see that at the end of the above process, two arbitrary TPs are interconnected by either a direct trust relationship or by a set of indirect ones. Additionally, a trusted path of TPs interconnects two arbitrary nodes in different TP domains.

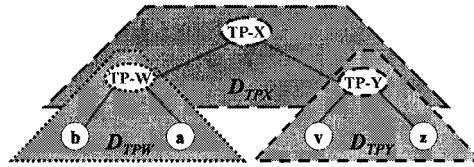

Figure 1. Random Trust Graph

3.3.3 Trust Initialization Protocol

Assuming that node *X* is not included in *TP-Y* domain or sub-domains, the following protocol enables *Y* to establish *X* as its TP:

Y→X: *TP_Service_Request* (1)

TP-X↔Y: *PKC challenge-response authentication* (2)

TP-X→Y: *TP_Service_Accept*, $K\{S_{Y,TPX}, T\}$ (3)

In message (1), *Y* requests a TP service to node *X*. In (2), assuming that node *X* is cooperative, *X* and *Y* mutually authenticate using certified public keys and agree in a session key *K*. In (3), *TP-X* sends to *Y* a long-term shared symmetric key $S_{Y,TPX}$ encrypted and integrity-protected with *K* and a timestamp *T*. Finally, *Y* sets *TP-X* as its TP and, similarly, *X* sets *Y* as one of its trusted nodes.

In the rest of the paper, we will use the term TP-shared-key and the notation $S_{node,TP}$ to refer to a long-term symmetric key $S_{node,TP}$ shared between a node and its TP or to any of the keys k_i derived from it, interchangeably. For instance, in the protocol above $S_{Y,TPX}$ is the TP-shared-key between *Y* and *TP-X*.

3.4 Nodes Trust And Key Establishment

TPs can be used as *ad hoc* TTPs to distribute keys and related trust information within the MANET. The first instance is when two arbitrary nodes *V* and *Z* of the same TP domain want to establish a shared key K_{VZ}. In such a case, their TP, e.g. *TP-Y* on Fig. 1, acts as a TTP providing them of the shared key K_{VZ}. Similarly, a common TP can vouch for nodes in its TP

domain. For instance, *TP-Y* can associate *V*'s identity to the symmetric key K_{VZ} distributed to *Z* and *Z*'s identity to the symmetric key K_{VZ} distributed to *V*. In some trust models this information may be sufficient to enable key establishment and mutual authentication of nodes *V* and *Z*. In web-of-trust models, *TP-Y* additionally includes *recommendation values*, which enable both nodes *V* and *Z* to respectively evaluate the level of trust that *TP-Y* has on their communication partner.

These concepts can be easily extended to several TP domains. An arbitrary *TP-Y* can delegate to its parent TP, *TP-X*, to vouch and distribute keys in D_{TPY} related to *TP-X* trusted nodes. In this manner, different TPs cooperate to securely distribute shared keys and/or vouch for nodes in different TP domains.

3.4.1 Trust And Key Distribution Protocol

In this section we describe the TKD protocol, a protocol to distribute trust and keys across TP domains (It can also be applied for intra-TP-domain trust and key distribution by considering just *one* intermediary TP below):

$$V \rightarrow TP\text{-}Y: S_{V,TPY}\{KeyReq\ (ID_W, ID_V), T_1\} \quad (1)$$

$$TP\text{-}Y \rightarrow TP\text{-}X: S_{Y,TPX}\{KeyReq\ (ID_W, ID_V), \quad (2)$$

$$TP\text{-}X \rightarrow W: S_{W,TPX}\{K_{V,W}, ID_V, T_3\}, ticket_V \quad (3)$$

$$W \rightarrow V: ticket_V \quad (4)$$

In step (1), node *V* requests *TP-Y* a key for *W*. This message is encrypted under $S_{V,TPY}$ to guarantee the confidentiality of the process as well as the anonymity of *TP-Y* and of the involved nodes *V* and *W*. To protect against message replay and modification attacks, the messages must be additionally integrity protected, e.g. by including message authentication codes (MAC) as well as timestamps T_1, T_2 and T_3.

In (2), *TP-Y* decrypts message (1) and obtains the included timestamp T_1. *TP-Y* computes a *Delegation Key* K_{TPYdel} by applying a pseudorandom function *F* with $S_{V,TPY}$ and T_1 as inputs, i.e. $K_{TPYdel}=F(S_{V,TPY}, T_1)$. With K_{TPYdel}, *TP-Y* delegates to other TPs to vouch for *V* and distribute keys associated to *V*'s identity in their domains. Note that the *Delegation Key* also enables other TPs to communicate securely with *V* (see further steps below). *TP-Y* constructs message (2) by including K_{TPYdel} and *V*'s key request. It then encrypts message (2) using the *TP-shared-key* with *TP-X* (the next TP in the trust path), i.e. $S_{Y,TPX}\{KeyReq(ID_W, ID_V), K_{TPYdel}, T_2\}$. *TP-Y* sends to *TP-X* message (2). In this manner, *V*'s key request is forwarded to a TP in a different domain.

In (3), decryption of message (2) with $S_{Y,TPX}$ transmits to *TP-X* (*W*'s TP) *TP-Y*'s trust in ID_V. *TP-X* randomly generates a new shared key $K_{V,W}$ for *V* and *W*. *TP-X* encrypts $K_{V,W}$ and ID_V using its *TP-shared-key* with *W*, i.e. $S_{W,TPY}\{K_{V,W}, ID_V, T_3\}$. *TP-X* also creates a *ticket* for *V* secured with K_{TPYdel} containing $K_{V,W}$ and ID_W, i.e. $ticket_V = K_{TPYdel}\{K_{V,W}, ID_W, T_3\}$. *TP-X* sends to *W* message (3).

In (4), node *W* forwards $ticket_V$ to *V*. Finally, *W* obtains $K_{V,W}$ by decrypting message (3) with $S_{W,TPX}$. In parallel, *V* obtains $K_{V,W}$ by decrypting message (4) with K_{TPYdel}.

For simplicity' sake we have assumed above a simple underlying PKI trust model. In PKI web-of-trust models, the messages of the TKD protocol additionally include *recommendation values* $R_{Target}^{voucher}$ on the identities of the participant TPs and end nodes.

4. PERFORMANCE ANALYSIS

In this section we analytically study the performance efficiency of the hybrid key management infrastructure and demonstrate its improved performance for MANET applications by comparing with PKIs.

To avoid impersonation or man-in-the-middle attacks, two arbitrary nodes *V* and *W*, which want to establish a key K_{VW}, need to, respectively, also assess the authenticity of the node they are establishing the key with[1]. This can be achieved in PKIs by using an X.509 strong two-way authentication protocol with key establishment (a similar protocol is included within the SSL/TLS protocol suite). In the hybrid case, nodes use TKD protocol to establish a key.

For simplicity's sake, in the following sections we assume that every MANET node holds a public key certificate signed by a common CA and the corresponding CA public key. For evaluating the hybrid approach, we further assume a MANET with *P* nodes, from which *N* act as TPs. We use N_{AV} to denote the average number of intermediary TPs in the shortest trust path between any pair of MANET nodes.

4.1 Communication Cost

In this section, for simplicity's sake, we assume a small or medium sized MANET where MANET nodes are in direct wireless range of each other.

Let us compare the TKD and the X.509[1] protocols. The following formulas quantify the bandwidth used by each protocol:

$$BWCost^{X.509} = 2\times(Cert + 2\times T_i + ID + Sign + RSAEnc)$$

$$BWCost^{TKD} = (N_{AV} + 3) \times TKDMessage$$

Let us use N_{BWEQ} to denote the average number N_{AV} of TPs for which $BWCost^{X.509} = BWCost^{TKD}$. Then, for $N_{AV} < N_{BWEQ}$, hybrid key management enabled trust and key establishment outperforms PKI. For instance, in a MANET application using public key certificates of 256 bytes (just including a public key and a digital signature of 1024 bits), timestamps of 8 bytes, symmetric keys of 128 bits and the cipher AES-128, N_{AV} should be lower than $N_{BWEQ} = 32$.

The number N_{BWEQ} can be used as an additional parameter to control the maximum number N of TPs in a MANET with P nodes, such that $N_{AV} \leq N_{BWEQ}$. For instance, by using Doyle and Graver[19] formula for average path length, in a worst-case scenario where the N TPs are subsequently disposed on a simple trust path and each TP domain contains in average $(P-N)/N$ NTP nodes, $N \leq 3N_{BWEQ}$.

4.2 Computational Cost

The following formulas quantify the computational overhead incurred by the X.509[1] and TKD protocols, respectively: requires two nodes V and W to compute four signature verifications, two signature generations, two public key encryptions and two private key decryptions. Then:

$$CCost^{X.509} = 6 \times RSASigVer + 4 \times RSASigGen$$

$$CCost^{TKD} = (N_{AV} + 2) \times AESEnc + (N_{AV} + 2) \times AESDec$$

We have developed a testing environment using Microsoft® CryptoAPI 1.0[9] and Szymon Stefanek's AES C++ Class[10] on an iPaq Pocket PC with ARM SA1110 CPU at 206 MHz to measure the cost to compute typical RSA public key and AES symmetric key operations. Let us use N_{CEQ} to denote the number of TPs for which $CCost^{X.509} = CCost^{TKD}$. The TKD protocol outperforms the X.509 for a number N_{AV} of TP nodes lower than N_{CEQ} = 7700 TPs. As demonstrated with our communication cost analysis, in normal MANET applications, the average number N_{AV} of intermediate TP nodes between two arbitrary nodes V and W is much lower than 7700.

5. SECURITY ANALYSIS

In MANET applications where the risk of node compromise is very low or null, the major security risks are imposed by the open nature of wireless MANETs.. In this case, the hybrid key management infrastructure offers perfect security because all the messages are protected with confidentiality and integrity mechanisms. In some other applications attackers may compromise nodes and then use them to attack the MANET by faking trusted identities or issuing false keys and recommendations. In applications where devices are owned by different administrative entities some nodes may misbehave by not cooperating. These kind of attacks are common in security solutions based on node trust and cooperation[2,14], and, particularly, also in the hybrid approach. However, the security robustness of the hybrid approach can be improved by further applying other mechanisms such as reputations[11], by minimizing the average number of intermediate TP nodes to reduce the risk that an attacker is among them, or, even, by allowing the formation of isolated trust graph cycles (to the cost of decreased trust graph connectivity), and by allowing nodes to establish multiple TPs (to the cost of increased computational overhead).

6. CONCLUSIONS

In this paper, we have presented a hybrid key management infrastructure for MANETs, which combines the concepts of PKIs with TTP-based infrastructures. In our hybrid approach, an underlying PKI is merely used to set-up initial trust of nodes in a MANET. This trust initialization method generates a random trust graph connecting all the nodes of the MANET. Then, the nodes of the shortest trust path connecting two end nodes can cooperate to securely distribute trust information and symmetric keys to the end nodes.

We have demonstrated that the hybrid approach enables key establishment and node-to-node authentication with a substantial improvement in terms of computational efficiency and communication efficiency in respect to current PKI solutions for MANETs. We have also discussed the security level of the hybrid approach and compared with other trust and cooperation based approaches.

7. REFERENCES

1. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. CRC Press. 1996.
2. S. Capkun, L. Buttyan and J.-P. Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, vol. 2, n° 1, pp. 52-64. 2003.
3. L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. IEEE Network Magazine, vol. 13, no.6, 1999.
4. H. Luo and S. Lu. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks, Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.
5. H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang. Self-Securing Ad Hoc Wireless Networks. 7th International Symposium on Computers and Communications. 2002.
6. M. Bechler, H.-J. Hof, D. Kraft, F. Pählke and L. Wolf. A Cluster-Based Security Architecture for Ad Hoc Networks. IEEE Infocom 2004.
7. E. C. H. Ngai, M. R. Lyu. Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks. ICDCSW'04 Workshops - W4: MDC. 2004.
8. L. Venkatraman and D. P. Agrawal. A Novel Authentication Scheme for Ad hoc Networks. WCNC 2000, pp. 1268-1273, vol.3.
9. The MSDN Library. http://msdn.microsoft.com/library/default.asp.
10. The Rijndael Page. http://www.esat.kuleuven.ac.be/~rijmen/rijndael/.
11. P. Michiardi and R. Molva. Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. Communication and Multimedia Security Conference. 2002.
12. A.B. MCDonald and T.F. Znati. A Mobility-Based Framework for Adaptive Clustering in Wireless Ad Hoc Networks. IEEE JSAC, 1999.
13. C. Kaufman, R. Perlman and M. Speciner. Network Security: Private Communication in a Public World. Prentice Hall PTR, 2002.
14. Network Associates, Inc. An Introduction to Cryptography.
15. L. Martucci, C. Schweitzer, Y. Regina Venturini, T. C. Carvalho, W. Ruggiero. "A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks". The Third Med-Hoc-Net Workshop, 2004.
16. K. Hoeper and G. Gong. Models of Authentication in Ad Hoc Networks and Their Related Network Properties. Technical Report, University of Waterloo, CACR 2004-03.
17. S. Capkun, J.-P. Hubaux and L. Buttyan. Mobility helps security in ad hoc networks. In Proc. MobiHoc'03, 2003.
18. M. Elhdhili, L. B. Azzouz, F. Kamoun. A Totally Distributed Cluster Based Key Management Model for Ad Hoc Networks. The Third Med-Hoc-Net Workshop. 2004.
19. J.K. Doyle and J.E. Graver. Mean distance in a graph. Discrete Mathematics Vol. 17, Issue 2, pp. 147-154. 1977.