Preventing or Utilizing Key Escrow in Identity-Based Schemes Employed in Mobile Ad Hoc Networks

Katrin Hoeper
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: khoeper@calliope.uwaterloo.ca

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: ggong@calliope.uwaterloo.ca

Abstract: Recently, identity-based cryptography (IBC) schemes have been considered as a tool to secure mobile ad hoc networks (MANETs) due to the efficient key management of the schemes. In this work we focus on the role of the Key Generation Center (KGC) as a key escrow, a property that is inherent to all IBC schemes. We explore the special role of key escrow in MANETs and show that this role significantly differs from key escrows in other networks. We introduce two adversary models for dishonest KGCs in MANETs, including a new spy model where a KGC uses so-called spy nodes that record communications in the network and report them to the KGC. We discuss the two faces of key escrow in MANETs, where our analytical results show that in many MANET applications the KGC can be prevented from being a key escrow. On the other hand, the results of this paper illustrate how a KGC can utilize spy nodes to monitor nodes in a MANET, as needed in some applications.

Keywords: ad hoc network security; identity-based schemes; key escrow; communication security.

Reference to this paper should be made as follows: Katrin Hoeper and Guang Gong (2007) 'Preventing or Utilizing Key Escrow in Identity-Based Schemes Employed in Mobile Ad Hoc Networks', Special Issue on Cryptography in Networks, Int. J. of Security and Networks (IJSN), Vol. , No. , pp.

Biographical notes: Katrin Hoeper is currently a Ph.D. student in the Department of Electrical and Computer Engineering at the University of Waterloo, Waterloo, Ontario, Canada. She received her MASc degree from Ruhr University, Bochum, Germany in 2002. Since 2002 she has been researching in the area of cryptography, network security, authentication and key management in mobile ad hoc networks.

Guang Gong received a B.S. degree in mathematics in 1981, a M.S. degree in applied mathematics in 1985, and a Ph.D. degree in electrical engineering in 1990, from universities in China. She received a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, Rome, Italy, and spent the following year there. After return from Italy, she was promoted to an Associate Professor at the University of Electrical Science and Technology of China. Since 1995, she had worked with several internationally recognized outstanding coding experts and cryptographers including Dr. Solomon W. Golomb at the University of Southern California, Los Angeles. She joined, as an Associate Professor, the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada, in September 2000. She is a Professor since 2004. Her research interests are in the areas of sequence design, cryptography, and communications security. She has authored or co-authored more than 130 technical papers and one specialized book, co-authored with Dr. Golomb, entitled as Signal Design for Good Correlation – for Wireless Communication, Cryptography and Radar. She is an Associate Editor of IEEE Transactions on Information Theory.
1 INTRODUCTION

The number of applications that involve wireless communications among mobile devices is rapidly growing. Many of these applications require wireless networks to be spontaneously formed by the participating mobile devices themselves. Such networks are referred to as mobile ad hoc networks (MANETs). The idea behind MANETs is to enable connectivity among any arbitrary group of mobile devices everywhere, at any time, and without the need of any fixed infrastructure. Slowly people realize that security is of paramount importance in MANETs. However, the special properties of MANETs, such as the lack of infrastructure, absence of on-line trusted third parties (TTPs), as well as the constraints of the devices and the communication channels, make implementing security a very challenging task. One major challenge is key management which is needed to enable authentication and key exchange among the mobile nodes in the network. Recently, researchers have drawn their attention to implementing identity-based cryptographic (IBC) schemes in MANETs due to the efficient key management of IBC schemes, e.g., Deng et al. (2004); Hoeper and Gong (2006); Khalili et al. (2003). IBC schemes reduce the communication, computation, and memory costs and thus seem as an attractive solution for the constrained devices and communication channels in MANETs. However, all IBC-schemes have the inherent property of key escrow because a key generation center (KGC) issues private keys to all nodes in the network.

In this paper we analyze the special role of a KGC as key escrow in the context of MANETs. We show that by implementing IBC schemes in MANETs we can benefit from the advantages those schemes have to offer while the impact of key escrow is limited by the special properties of MANETs such as user mobility and limited communication ranges. The impact of key escrow can be further reduced by the several countermeasures that we present in this paper. Generally, multiple KGCs that each hold only a share of the master key are used to distribute and thus reduce the power of the KGC, e.g., using an \((k,n)\)-threshold scheme (Boneh and Franklin, 2001). Many other schemes for distributing the master key among multiple KGCs have been introduced (Boyd et al., 2004; Chen et al., 2003; Hess, 2003; Lee et al., 2004; Oh et al., 2005; Paterson, 2002). However, this countermeasure is not sufficient to prevent key escrow in all applications. In many applications users have no choice of the provider of a service and thus have to accept the conditions of the provider, i.e., users have no choice but to trust the KGC or group of KGCs. In this paper we consider single dishonest KGCs or a group of colluding KGCs and we will not distinguish both cases in the remainder of this paper.

However, in this paper we do not only analyze how to prevent key escrow in MANETs, we also study application in which key escrow is desirable, e.g., to monitor the nodes/users that are using the network. Our analysis in this paper points out how a KGC can increase its power as key escrow in MANETs, e.g., to allow a KGC to monitor network user/nodes. Hence, in this paper we explore the two faces of key escrow.

For our analysis we introduce two adversary models for dishonest KGCs that cope with the special properties of MANETs. In the first adversary model the KGC is either inside or outside the communication range of the communicating parties. The KGC is considered to be in immediate range if it is either in range of the communicating parties themselves or in range of an intermediate node that serves as a relay on the multi-hop routing path. In that model the key escrow capability of the KGC mainly depends on the location and communication range of the KGC and the nodes. In the second model we introduce a new concept of so-called spy nodes that are distributed in the network by the KGC. The spy nodes record all communications that occur in their communication range and send the recorded files back to the KGC. In this scenario the KGC might be able to obtain a record of a communication, even though the KGC was outside the communication range of the communicating parties.

For each of the defined adversary models, we consider passive and active attacks launched by the KGC. A general method of preventing passive attacks is executing a Diffie-Hellman (DH)-based key agreement protocol, as pointed out by Boyd et al. (2004); Chen and Kudla (2003). We demonstrate that the same method can be applied to our adversary models for KGCs in MANETs. However, there is no general way of preventing active attacks by a KGC. In this paper we show that active attacks by KGCs in MANETs that employ an IBC scheme are only successful if certain assumptions hold. We demonstrate that these assumptions are fairly restrictive in most MANET applications and show that the probability of a successful attack is very low. Note that active attacks can also be placed by other type of TTPs, such as certification authorities (CAs) in public key infrastructures (PKIs). However, KGCs are more powerful than any other kind of TTP due to its knowledge of all private keys. We will discuss the applicability of our models to other security schemes in our analysis.

The rest of the paper is organized as follows. In the next section, we review IBC schemes and other preliminaries. In Section 3, we introduce two adversary models for dishonest KGCs in MANETs. In Section 4, we discuss the necessary assumptions for successful passive and active attacks in each of the adversary models. We analyze the probability of a successful attack and show countermeasures to either prevent attacks or to reduce the probability of a successful attack. Next we discuss the applicability of existing countermeasures for key escrow in ad hoc networks in Section 5. Finally, we draw some conclusions and discuss our results in the last section.
2 PRELIMINARIES

2.1 IBC schemes

IBC schemes provide a very efficient key management that helps reducing communication, computation, and memory costs. For these reasons, IBC schemes have been considered as security solutions for MANETs (Deng et al., 2004; Hoepman and Gong, 2006; Khalili et al., 2003). The main feature of IBC schemes is the use of self-authenticating public keys, which makes the use of public key certificates redundant. Because the public key $Q_A$ of a node $A$ is predetermined, the private key $d_A$ is derived from $Q_A$ and a master secret key $s$ that is only known to the KGC, e.g. $d_A = sQ_A$ in the identity-based encryption (IBE) scheme by Boneh and Franklin (2001). The KGC generates and distributes the private keys during the initialization of all network nodes. In IBC schemes, every network node is able to derive the public key $Q_A$ of a communication partner $A$ in the network, e.g. $Q_A = H_1(A)$ in Boneh and Franklin (2001). This does not require the exchange of any data. In addition, all pairs of nodes $A$ and $B$ in a pairing-based IBC scheme such as the scheme by Boneh and Franklin (2001) are able to compute a pairwise pre-shared secret key $K_{A,B}$ in a non-interactive fashion as discussed by Boyd et al. (2004). The pre-shared keys are computed as $K_{A,B} = e(d_A, Q_B) = e(Q_A, d_B)$, i.e. both nodes compute the bilinear mapping $e(\cdot)$ over their own private key $d$ and the public key $Q$ of the other node.

The KGC is a key escrow because it knows all private and pre-shared keys in the network. The key escrow property of all IBC schemes might be desirable in some cases such as governmental and military applications. However, in many civil MANET applications the property is considered as a drawback of IBC schemes. Threshold schemes and other schemes using multiple KGCs have been introduced to prevent key escrow (Boneh and Franklin, 2001; Boyd et al., 2004; Chen et al., 2003; Hess, 2003; Lee et al., 2004; Oh et al., 2005; Paterson, 2002). However, in this paper we analyze the cases that the KGC is dishonest, whether it is one single dishonest KGC or a colluding group of KGCs. However, we discuss how $(k, n)$-threshold schemes or other solutions using multiple KGCs can be used to reduce the likelihood of key escrow in our adversary models in Sections 4.2 and 5.

2.2 MANETs

As mentioned in the introduction, MANETs have many special properties that distinguish them from other traditional networks. For example, MANETs are formed spontaneously and are thus infrastructureless. This property requires all network operations to be fully self-organized. Furthermore, MANETs devices are typically constrained in computational power, memory space and power supply. Another distinctive property of MANETs devices is that they are mobile and communicate over wireless links, where their very constrained power resources result into a limited communication range. The communication range is usually increased by using multi-hop communication protocols. If two nodes $A$ and $B$ are in each others transmission range they can directly exchange messages with each other, which is sometimes called one-hop communication (Figure 1 (a)). However, generally two parties are too far apart to directly communicate, i.e. they are not in each other communication range. In that case intermediate nodes $n_i$ are used as a relay to forward the messages until they reach their destination. This is called multi-hop communication and is illustrated for four intermediate nodes $n_i, n_j, n_k, n_l$ in Figure 1 (b).

![Figure 1: Communication between nodes A and B: (a) one-hop communication, (b) multi-hop communication.](image)

2.3 Communication protocols

Throughout our analysis of key escrow in different adversary models in the next sections, we consider peer-to-peer communications in a MANET, where we call the two principals $A$ and $B$. However, we do not consider lower layer protocols, e.g. we assume that secure routing is in place for multi-hop communications. We focus on the communication protocol and how the information that is exchanged between $A$ and $B$ is protected, i.e. the privacy and authenticity of the communications. Since we discuss IBC schemes in this paper, we consider ID-based communication protocols. We distinguish three types of protocols:

Protocol 1: Static Key Encryption. The two parties $A$ and $B$ use their long-term keys for encrypting and decrypting their messages, e.g. using their pre-shared key $K_{A,B}$ or public/private keys $(Q_A, d_A)$ and $(Q_B, d_B)$, respectively. Consequently, the same key is used to secure all communication. Hence, as soon as the static decryption key is compromised, an adversary is able to decrypt all previous and future communications. Please recall that the KGC knows the long-term keys of all network nodes.

Protocol 2: Symmetric Key Exchange. Before starting two communicate, $A$ and $B$ execute an authentication and authenticated key exchange (AKE) protocol to mutually authenticate each other and securely establish a session key. The established key is derived in a purely symmetric fashion. Thus the data that is used to derive the session key $K$ is exchanged during the protocol execution. As a consequence, the protocol does not achieve perfect forward secrecy (PFS). PFS is achieved when the compromise of the long-term keys of one or more principals does not compromise the session keys established in previous
protocol runs among the same principals. PFS cannot be provided in symmetric AKE protocols, because once the long-term keys are compromised, an adversary would be able to derive session keys from previous sessions. These kind of protocols use only symmetric primitives and are therefore very efficient. Due to their efficiency, the protocols are suitable for very constrained devices. The session key \( K \) is used to secure all further communications between \( A \) and \( B \). Hooper and Gong (2005) give an example of such symmetric ID-based key exchange protocols. A slightly simplified version is given in Protocol 2 below, where the pre-shared key \( K_{A,B} \) is used to compute two keys, namely an authentication key \( k_a = f_{K_{A,B}}(1) \) and a key derivation key \( k_d = f_{K_{A,B}}(2) \). The two keys are used as input in a secure pseudorandom function \( f(\cdot) \) to authenticate the exchanged messages and derive the session key \( K \), respectively. Parameter \( s \) is a session identifier, and the nonces \( N_A \) and \( N_B \) are used as challenges in a challenge-response authentication protocol and also serve as input to derive a fresh session key \( K \).

### Protocol 2: IBC-based symmetric key exchange

**Pre-shared keys:** \((k_a, k_d) = (f_{K_{A,B}}(1), f_{K_{A,B}}(2))\)

**Protocol flow:**

\[
A \rightarrow B : A, s, N_A
\]

\[
A \leftarrow B : B, s, N_B, r_B = f_{k_a}(A, N_A, s, N_B)
\]

**Session key:** \( K = f_{k_d}(N_A, N_B) \)

### Protocol 3: IBC-Based Diffie-Hellman Key Exchange

In the third scenario, \( A \) and \( B \) execute an ID-based AKE protocol in which the session key is derived using the Diffie-Hellman (DH) key exchange Diffie and Hellman (1976). (Boyd et al., 2004) introduce such a protocol using an elliptic curve DH (ECDH) key exchange which is illustrated in Protocol 3 below. In Protocol 3, the nonces \( N_A \) and \( N_B \) of Protocol 2 are replaced with ephemeral public keys \( T_A = r_A P \) and \( T_B = r_B P \), where \( r_A \) and \( r_B \) are random nonces and \( P \) a generator of the elliptic curve. Furthermore, the symmetric session key computation of Protocol 2 is replaced with an ECDH key agreement, i.e. \( K = r_A T_B = r_A r_B P = r_B T_A \). Like Protocol 2, Protocol 3 employs a pseudorandom function \( f(\cdot) \) with the pre-shared keys \( K_{A,B} \) as input for authentication. Due to the use of a DH key exchange the protocols achieves PFS, i.e. even if an adversary learns about \( A \) and \( B \)'s long-term keys he cannot obtain session keys from previous sessions.

### Protocol 3: IBC-based Diffie Hellman key exchange

**Pre-shared key:** \( K_{A,B} \)

**Protocol flow:**

\[
A \rightarrow B : A, s, T_A
\]

\[
A \leftarrow B : B, s, T_B, f_{K_{A,B}}(A, T_A, s, T_B)
\]

**Session key:** \( K = r_A T_B = r_B T_A \)

As the name implies, we usually trust a trusted third party. However, most users do not want that this trusted third party is able to listen to all their communications. For this reason, most people consider it as a drawback of a scheme if the trusted third party of the system is a key escrow. In this section, we introduce adversary models for dishonest KGCS in IBC schemes that abuse their power as a key escrow to launch passive and active attacks on the users privacy. In particular, we consider scenarios in which a KGC is attempting to eavesdrop on a communication between two parties \( A \) and \( B \) in a MANET. Therefore, the KGC launches an attack on the communication protocol (Protocol 1, 2 or 3) executed between \( A \) and \( B \). In the following subsections, we will discuss the attacks that the KGC is able to launch and introduce two adversary models for dishonest KGCS.

### 3.1 Attacks

Throughout our analysis we distinguish passive and active attacks that can be launched by a KGC in any IBC scheme and we define them as follows.

**Passive attacks:** In a passive attack, a KGC eavesdrops on the communication between two parties \( A \) and \( B \). In addition, a KGC might use its knowledge of all private and public keys \((d, Q)\) to decrypt the eavesdropped communications. Please recall that a KGC is able to compute all pairwise pre-shared keys \( K_{A,B} \) in the system. Hence, communications protected using the pre-shared keys or public keys alone can be decrypted by the KGC.

**Active attacks:** In an active attack, a KGC does not only eavesdrop on communications and decrypt them if necessary, a KGC can also intercept, create, modify and re-direct messages. However, we would like to emphasize the difficulty of intercepting messages in MANETs. While eavesdropping is easy to do in a wireless network, preventing a broadcasted message from propagating through the network is relatively hard to achieve. In order to intercept messages the KGC needs the ability to jam signals in a controlled manner without arousing suspicion of the neighboring (affected) nodes. However, we assume that the KGC has all those capabilities in the adversary models introduced in this paper. Consequently, a KGC can abuse its powers to masquerade as another network node during an active attack. We would like to emphasize the power of such an active attack, because the KGC has knowledge of all the key material of any arbitrary node in the network, including the node the KGC attempts to impersonate.

An example of an active attack in an IBC scheme is an attack that we refer to as \textit{KGC-in-the-middle-attack}. During this attack, a KGC “sits” in the middle of two nodes \( A \) and \( B \) that communicate using one of the three communication protocols that we presented in the previous paragraph. In a successful attack, the KGC masquerades as \( B \) to \( A \) and vice versa. After the protocol execution both

---

**3 ADVERSARY MODELS FOR DISHONEST KGCS**
parties $A$ and $B$ each share a session key with the KGC but believe that they share a session key with each other. The KGC can now read all encrypted communications between $A$ and $B$ by intercepting and decrypting the messages from the sender and then re-encrypting the messages using the key shared with the receiver. $A$ and $B$ are perfectly fooled and cannot detect the KGC in the middle that listens to their communications.

### 3.2 Adversary models

We now derive two adversary models for dishonest KGCs in MANETs, in which we take the special properties of MANETs and their devices into account. For each model, we consider both, one-hop and multi-hop communications among the network nodes. The two models are illustrated for one-hop and multi-hop communications in Figures 2 (a)-(d) for Model I and Figures 3 (a) and (b) for Model II, respectively. In the figures, the transmission range of network nodes is depicted as dashed circle and the range of the KGC as dark grey circle. We would like to point out that a KGC is usually very powerful and thus its transmission and receiving range is much larger than the range of the network nodes. The first model can be derived intuitively for MANETs, whereas the second one is based on spy nodes, a new concept that we introduce in this paper. **Model I: Dishonest KGC model.** In this adversary model we consider one KGC and several mobile nodes in a MANET. The KGC can be either outside the communication range of the communicating network nodes $A$ and $B$ or inside their communication ranges. The first case, i.e. KGC is out of range, is illustrated in Figure 2 (a) for one-hop communication between $A$ and $B$, and in Figure 2 (b) for a multi-hop communication between $A$ and $B$. Consequently, in one-hop communications the KGC is outside $A$’s and $B$’s communication range, whereas in the case of a multi-hop communication, the KGC is outside the communication range of $A$, $B$, and all intermediate nodes $n$ on the routing path between $A$ and $B$. In the second case, i.e. the KGC is within communication range, the KGC is either in direct communication range of $A$ or $B$ in the one-hop scenario (Figure 2 (c)) or inside communication range of $A$, $B$ or any other node $n$ on the routing path in the multi-hop scenario (Figure 2 (d)).

**Model II: Spy nodes model.** In our second adversary model, we introduce a new concept in which the KGC distributes so-called *spy nodes* in the network to increase its own communication range. These spy nodes record all communications in their communication range and send the recorded data back to the KGC. The spy nodes have the following properties, spy nodes: (i) act and appear as regular network nodes, i.e. spy nodes cannot be distinguished from other nodes; (ii) have the same power constraints as regular nodes, e.g. the limited communication range; (iii) do not possess the master key $m$ of the system; (iv) can send recorded messages to the KGC; and (v) can play messages received from the KGC back into the network. The spy nodes in our scheme have properties (i) and (ii) for two reasons, first for the devices to be cheap, second to be indistinguishable from other regular network nodes. A spy model with more powerful spy nodes is briefly discussed in Section 4.4.

Spy nodes cannot intercept messages because this requires jamming or similar capabilities, which is clearly beyond the power of a spy node. Although the spy nodes’ communication range is limited as well, spy nodes are able to use multi-hop routes to communicate with the KGC. Those routing paths can consist of both, spy and regular network nodes. By introducing spy nodes to the network, the KGC is able to eavesdrop on communications outside its own communication range as long as a spy node is in communication range, as illustrated in Figures 3 (a) and (b) for one-hop and multi-hop cases, respectively. In the figures, spy nodes $s$ are depicted as grey circles and the communication range of a spying node is shaded light grey. Note, that a spy node needs to be in communication range of $A$ or $B$ in the one-hop scenario and in range of $A$, $B$ or one of the intermediate nodes $n$ in the multi-hop scenario in order to record the communication between $A$ and $B$.

### 4 ANALYSIS OF ATTACKS AND COUNTERMEASURES

In this section, we analyze the necessary assumptions for successful passive or active attacks by dishonest KGCs in the introduced adversary models. Furthermore, we discuss the likelihood of successful attacks. We show countermeasures for all attacks that can be prevented and, if a total prevention is infeasible, we explain how the probability of a successful attack can be reduced. We separately analyze passive and active attacks launched by dishonest KGCs against two communicating parties $A$ and $B$ who use one of the three communication protocols presented in Section 2.3. For our analysis, we need the following notation. We assume that the communication range of all network nodes including the spy nodes are equal, and denote the range by $D$. Let $D_{KGC}$ be the communication range of the KGC and let $(A, n_1, n_2, \ldots, n_{d-2}, B)$ be a routing path between the two communicating parties $A$ and $B$ at the time instance $t$, where $d$ is the length of the path. Furthermore, $|x - y|$ denotes the Euclidean distance between two points $x$ and $y$.

#### 4.1 Passive attacks

**Model I:** If the KGC is out of communication range it cannot launch a passive attack in this model because the KGC is not able to eavesdrop on the communication. However, if the KGC is in communication range of either $A$, $B$, or one of the intermediate nodes $n$, the KGC is able to eavesdrop on the communications between $A$ and $B$. The assumptions for a successful passive attack in Model I can be summarized as follows:
Assumption 1. The KGC is in communication range of one of the communicating nodes A or B or of at least one node on the routing path between A and B during the communication, i.e., $|KGC - n_i| < D$ and $n_i$ could contain $A = n_0$ or $B = n_{d-1}$ or any other node on the routing path.

Assumption 2. The communicating parties A and B use either no security protocol, Protocol 1, or Protocol 2 for communicating or establishing a session key.

Assumption 3. If Protocol 2 is used, the KGC needs to be in communication range during protocol execution.

The first assumption is obviously necessary for launching any attack. The second assumption is necessary to enable the KGC to read/decrypt the exchanged messages. If A and B do not secure their communications at all, the KGC can simply eavesdrop on the communication. If Protocol 1 is used, the KGC can directly decrypt the messages, whereas for Protocol 2 the KGC first needs to derive the session key and then use this session key to decrypt the messages. For deriving the session key, the KGC needs to be in transmission range for the first and second flow of Protocol 2 (Assumption 3).

Countermeasures:

AKE Protocol with PFS. Passive attacks by dishonest KGCs can be easily prevented by implementing a Diffie-Hellman (DH)-like key agreement protocol or any other protocol that provides PFS, such as Protocol 3. By doing so, Assumption 2 would not hold anymore. Since only ephemeral public keys are exchanged during protocol execution, the KGC is not able to derive the newly established session key. In order to compute the session key, the KGC would need to know at least one of the ephemeral private keys. Hence, the KGC is not able to decrypt the communications anymore and is thus not longer a key escrow. Please note that using DH-type AKE protocols to prevent eavesdropping, key escrow or other attacks is a well known solution in all types of networks, e.g. ethernet networks, and thus the solution is not specific to MANETs.

Model II: In this model, the KGC cannot directly eavesdrop on the communications between A and B. However, the KGC can use the spy nodes to launch a passive attack. For a successful attack, Assumption 2 and the following additional assumptions have to hold:

Assumption 1'. At least one spy node s records the messages. In other word, s is in communication range of one of the communicating nodes A or B or of at least one node on the routing path between A and B, i.e., $|s - n_i| < D$ where $n_i$ could contain $A = n_0$ or $B = n_{d-1}$ or any other node on the routing path.

Assumption 3'. If Protocol 2 is used, at least one spy node s needs to be in communication range during protocol execution and record the first and second protocol flow, i.e. Assumption 1’ is true for protocol flows 1 and 2.

In a successful passive attack, the recorded messages will eventually reach the KGC. The KGC is then able to decrypt the communications directly or derive the established session keys first and the decrypt, as described for Model I. Countermeasures: The same countermeasure as described for Model I can be applied to Model II, i.e. the implementation of a AKE protocol that provides PFS.

Note that we do not analyze the likelihood of successful attacks because such attacks can be entirely prevented by the discussed countermeasure.

4.2 Active attacks

Now we consider active attacks. In that case, executing a DH-like key agreement or any other AKE protocol with PFS does not prevent the KGC from being a key escrow.

The KGC could, for instance, launch a KGC-in-the-middle attack and derive a new DH key with each of the communicating parties without being detected. In the following paragraph, we derive assumptions for each adversary model that are necessary in order to launch a successful impersonation attack, such as KGC-in-the-middle attacks. Those attacks also enable the KGC to read/decrypt communications. Next, we analyze the probability of a successful attack, where we take some special properties of MANETs into account. Those properties include the dynamic topology of MANETs which is caused by frequently joining or leaving nodes and the mobility of present nodes,
sumed that the KGC has the power to intercept messages, a successful attack can be launched in this model, we now 

KGC intercepts all messages exchanged between communication range of A or B or at least one intermediate node $n_k$.

which in turn affects the routing.

**Model I:** If the KGC is out of the communication range it is not able to launch any attack. The KGC can launch an active attack on two communicating nodes A and B in a MANET if the following assumption holds:

**Assumption 4.** The KGC is in communication range of at least two nodes $n_i$ and $n_j$ on the routing path during the entire session, where $n_i$ and $n_j$ can include one or both of the endpoints A and B, i.e. $|KGC - n_i| < D$ and $|KGC - n_j| < D$, where $\{n_i, n_j\}$ could contain $A = n_0$ or $B = n_{d-1}$ or both A and B or any other two nodes on the routing path.

Note that we use session to describe the execution of an AKE protocol and the subsequent communications that are secured using the derived session key. If Assumption 4 holds, the KGC can launch the following attack independent of which communication protocol A and B use. The KGC intercepts all messages exchanged between $n_i$ and $n_j$. Note that $n_i$ and $n_j$ do not need to be consecutive nodes on the routing path, basically the KGC intercepts the message from a node $n_i$ and then sends the modified message back to any other node $n_j$ that is on the routing path. The attack is illustrated in Figure 5 (a) for one-hop communications between A and B, here $n_i = A$ and $n_j = B$ with the KGC in the middle. In the multi-hop case and $n_i$ and $n_j$ are intermediate nodes on the routing path the attack is illustrated in Figure 5 (b). The flash symbol in both figures symbolizes the jam signal or other mean of intercepting messages by the KGC. The nodes $n_i$ and $n_j$ are both not aware of the attack, because the KGC can simply masquerade as the respective neighboring node $n_i$, $n_j$ or any other network node.

**Probability of successful attack.** After having shown how a successful attack can be launched in this model, we now discuss the likelihood of such an attack. Although we assumed that the KGC has the power to intercept messages, we would like to point out the difficulty of intercepting messages in MANETs for the reasons we discussed earlier. Even if we assume that the KGC has a way to jam specific signals without arousing suspicion and disturbing the actual protocol execution, we believe that a successful attack is still very unlikely for the following reasons. In order for an attack to be successful, Assumption 4 needs to hold for each protocol flow, i.e. for each flow of an AKE protocol and the subsequent communications. For instance, in Protocols 2 and 3, the KGC would need to intercept and modify all three message flows to execute two separate protocols with both parties A and B. However, due to the dynamics of MANETs two packets of a protocol execution may not take the same route from a sender A to a receiver B. Hence, a dishonest KGC would need to be in communication range of A and B on each of the used routes, i.e. three paths in our example. Note that these three routes might be disjoint. Hence, the probability of a successful active attack, denoted by $P_{suc}$, depends on the number of protocol rounds $r$ and the probability $P_{N_i}(r)$ that the KGC is in range of at least two nodes in each round, i.e.

$$P_{suc} = \prod_{i=1}^{r}(P_{N_i}(r)).$$

To derive the actual probability $P_{suc}$ of a successful attack we need to calculate the probability $P_{N_i}$. Let’s say we have a total of $N$ nodes in the network, with $N_I$ nodes inside the KGC’s communication range and $N_O$ nodes outside the communication range. Now we assume that the multi-hop path is $d$ hops long including the two end nodes A and B, i.e. the routing path is $(A, n_1, \ldots, n_{d-2}, B)$. The probability of having at least two nodes out of $N_I$ as part of the $d$ nodes cannot be easily derived, because the distribution for $N_I$ and $N_O$ is usually unknown and varies highly for different solutions. Usually the probability of having a node out of $N_I$ on the path does not equal the probability of having a node out of $N_O$ on the path. Lets consider a KGC with a transmission radius $D_{KGC}$, i.e., the communication range of the KGC covers an area $A_{KGC} = \pi D_{KGC}^2$.

Now consider a node with distance $R$ to the KGC. The probability $P_{N_i}$ that this node is in communication range of the KGC is $P_{N_i} = \frac{\pi D_{KGC}^2}{A_{KGC}} = \left(\frac{D_{KGC}}{R}\right)^2$. We believe that $R >> D_{KGC}$ in most cases and thus the probability of having a node out of $N_I$ on the path is much smaller than a node out of $N_O$. Hence, the probability $P_{suc}$ of a successful attack would be negligibly small. The discussed scenario is true for most MANET applications, e.g. in a battlefield where the KGC remains in a safe place, whereas the nodes are placed far away in the enemy territory. Same is true in civil and other applications, where users are not necessarily roaming close to the KGC any longer, once the nodes have obtained their private keys. As a matter of fact, there is no necessity for close proximity to the KGC. We can compare the situation to PKI implementations, where nodes do not roam close to their CA any longer once they received their certificate. Hence, we believe that a successful attack is very unlikely due to the likely great distance
between KGC and the network nodes. Therefore, we will not discuss the probabilities in any more detail for this adversary model.

**Countermeasures:** Even though we believe that an active attack is very unlikely in Model I we introduce the following methods to further decrease the probability.

**Session control.** As a countermeasure for all attacks in which the KGC is able to modify all messages but cannot intercept them, we suggest that network nodes acting as a router discard all received messages that belong to the same protocol flow but have different contents. This can be detected by checking the session identifier $s$ and the message format in packets. A node $n_i$ on the routing path should never receive two messages that appear to come from sender $A$ and belong to the same protocol flow and same session but have different contents.

**Close proximity.** It is easy to see that the shorter the routing path the less likely are two nodes out of $N_I$ on the path. For this reason, we suggest that two nodes should establish a new shared key as soon as the nodes are in close proximity to each other because close proximity of nodes makes successful attacks very unlikely.

**Disjoint Paths.** Furthermore, we suggest to use different routing paths for packets whenever possible. One feature of MANETs are the redundancy of routing paths that offers several potential routing paths between a sender $A$ and a receiver $B$. In the ideal prevention the used routing paths are completely disjoint for each flow. In that case the probability $P_{N_I}(r)$ of each round $r$ may be different which can reduce the overall probability $P_{\mathrm{succ}}$ of a successful attack. Note that if the KGC is outside the range in only one of the rounds $r_i$, i.e. $P_{N_I}(r_i) = 0$, the attack fails. If no disjoint or different routing paths are available, the network nodes can use their mobility to enable the use of different routing paths for different protocol flows.

**Distributed KGCs using $(k,n)$-threshold or other schemes.** A general countermeasure of preventing a dishonest KGC from launching an attack is to distribute the power to $n$ KGCs (Boneh and Franklin, 2001; Boyd et al., 2004; Chen et al., 2003; Hess, 2003; Lee et al., 2004; Oh et al., 2005; Paterson, 2002). In this approach every KGC makes successful attacks very unlikely.

**Model II:** Next we investigate active attacks in the spy model. An active attack similar to the one described for Model I is feasible in Model II, but here the KGC has a more realistic chance for a successful attack. In particular, the KGC uses spy models to launch an impersonation attack on $A$ and $B$ to ultimately eavesdrop on their communications. The attack is illustrated in Figure 6 and represents a spy-in-the-middle-attack. The attack is feasible under the following two assumptions.

**Assumption 5.** At least one spy node $s$ is a part on the routing path of $A$ and $B$ during the entire session, i.e., $s \in \{n_1, \ldots, n_d-2\}$.

**Assumption 6.** The spy node $s$ and the KGC are able to communicate on-line, i.e. without long communication delay. For example, the spy nodes have a direct connection using directed antennas, satellite connection or a dedicated cable or the routing path between KGC and $s$ is short.

We can conclude from Assumption 5 that the attack only works in the multi-hop case, because a spy $s$ needs to be on the routing path of $A$ and $B$ in order to relay the messages to the KGC. In the one-hop scenario a spy node would need to have jamming capabilities to intercept messages between $A$ and $B$ which we assumed spy nodes do not have. Unlike in Model II the KGC itself does not need to be in communication range and does not need to intercept messages. Instead a spy node $s$ on the routing path directly sends the exchanged messages to the KGC. Note that the spy node does not need to intercept messages because it is a part of the routing path. The KGC modifies the messages it receives from $s$ (after decrypting the messages if necessary) and sends them back to the spy node which forwards the modified messages to the next node on the routing path. Please recall that spy nodes do not possess the master key $m$ or long-term key material. Also note that the spy node $s$ cannot launch the attack itself because it does not have the knowledge to impersonate network nodes. The communication between KGC and its spy nodes needs to be very fast in order for this attack to work. Otherwise the delay of the message would be too long and could cause the communicating nodes to drop the session and choose another routing path.

**Probability of successful attack.** For analyzing the attack we assume that Assumption 6 holds. Hence, to calculate the probability of a successful attack $P_{\mathrm{succ}}$ we need to determine the probability of Assumption 5, i.e. the probability $P_{\mathcal{S}_j}$ that at least one spy node $s$ is part of the multi-hop communication path of length $d$. Note that here, the length $d$ excludes the nodes $A$ and $B$ because they are obviously not spy nodes, i.e. the routing path is $(A, n_1, \ldots, n_d, B)$. The probability $P_{\mathcal{S}_j}$ depends on the length $d$ and the distribution of spy nodes $P_S$ and regular network nodes $P_N$. The length $d$ of routing paths in turn depends on the used routing protocol, the number of nodes, their mobility pattern, their location, the size of the area nodes roam in, the communication range of nodes and many more factors. We assume that there are $N$ regular network nodes and $S$ spy nodes in our network and $d$ is the average length of a multi-hop path between $A$ and $B$, excluding the nodes $A$ and $B$. For a successful attack on a AKE protocol with PFS, at least one spy node $s$ would need to be a part of the routing path of each message flow $j$. Hence, the probability $P_{\mathrm{succ}}$ of a successful attack on a protocol with $r$ rounds is given by

$$P_{\mathrm{succ}} = \prod_{j=1}^r P_S(d_j).$$

Note that the probability $P_S(d_j)$ can be different in each
round $j$ because the length $d_j$ of the path might vary.

In the following we analyze the probability of a successful attack in certain specific scenarios. We assume that spy nodes $s$ and networks nodes $n$ are uniformly distributed in the network. The probability $P_S(d)$ of the event that we take $d$ nodes out of the total set of all nodes, i.e. $N + S$, in which at least one node is a spy node is given by

$$P_S(d) = 1 - \left( \frac{N}{N+S} \right)^d. \quad (1)$$

We can observe that by increasing the number of spy nodes $S$ in the network the KGC increases the probability of a successful attack, whereas decreasing the length $d$ of the path decreases the chance. Please note that we consider the case that at least one spy node is on the path and discuss the attack for the case that exactly one spy node is on the path. However, if more than one spy node is on the path, they will each execute the attack since the spy nodes do not know of each other and thus cannot signal that the protocol is currently under attack already. Multiple spy nodes executing multiple attacks do not prevent the attack from succeeding, however, it will increase the communication delay.

In the following we compute the probability of a successful attack for some specific scenarios. We consider two examples of network size of 100 and 1000 network nodes, i.e. $N + S = 100$ and $N + S = 1000$ respectively. We assume that 5% to 15% of all nodes are spy nodes in our network. We believe that deploying more spy nodes is not cost effective for the KGC/adversary. On the other hand, using less spy nodes seems to small to increase the key escrow power of the KGC significantly. Furthermore, we use the simulation results for the AODV routing protocol from Perkins and Royer (1999) to determine the average path length $d$. Please note that the path length $d$ depends on the routing protocol and is not necessarily the minimum distance between $A$ and $B$. The values for $d$ that we adopt from Perkins and Royer (1999) serve only as example and may be significantly smaller for other routing protocols or using different simulation parameters, e.g. a different mobility pattern. For our examples, we consider a 3-round protocol, i.e. $r = 3$, and assume that the length $d_j$ is the same in each round $j$. In our first example we choose a network size of $N + S = 100$ nodes which follows that $d = 4$ (Perkins and Royer, 1999). The probability $P_S(d)$ that at least one spy node $s$ is on a routing path between two nodes $A$ and $B$ can be computed from Eq. 1 with $d = 4$, $N + S = 100$, and is illustrated in Figure 4 (a) for 5% to 15% spy nodes in the network. We can observe for example, that for 5% spy nodes in the network, i.e. $N = 95$ and $S = 5$, $P_S = 0.1854$ and thus $P_{suc} = 6.38 \cdot 10^{-3}$, and for 10% spy nodes, i.e. $N = 90$ and $S = 10$, $P_S = 0.3439$ and $P_{suc} = 0.0406$. In a second example we consider a network size $N + S = 1000$, with $d = 11$ (Perkins and Royer, 1999). The probability $P_S(d)$ for this network scenario is illustrated in Figure 4 (b) for 5% to 15% spy nodes in the network. For example for 5% spy nodes, i.e. $N = 950$ and $S = 50$, $P_S = 0.43$ and $P_{suc} = 0.08$; and for 10% spy nodes, i.e. $N = 900$ and $S = 100$, $P_S = 0.686$ and $P_{suc} = 0.323$. We can see that if there are 5% spy nodes in the network the probability of a successful attack is below 1% for a network size of 100 and significantly below 10% in a larger network of 1000 nodes. Even in the extreme scenario of 10% spy nodes, the probability is below 5% in the smaller network and around 32% in the larger one. These numbers serve as a rough estimate and we would like to point out that the probability $P_{suc}$ highly depends on the average path length $d$ which in turn depends on the efficiency of the implemented routing protocol and the mobility of the nodes.

**Countermeasures:** We showed that the probability of a successful attack is fairly small. However, the probability can be further reduced by one or more of the following countermeasures.

**One-hop communications.** First, we would like to point out that active attacks in this model are only feasible in the case of multi-hop communications. One-hop communication can totally eliminate the possibility of an active attack by a dishonest KGC. Hence, we suggest that two nodes establish a fresh shared key whenever they are in direct communication range.

**Close proximity.** Even if direct communication cannot be provided, close proximity between communicating nodes results into shorter routing paths, which in turn significantly reduces the probability of a successful attack. For this reason we suggest to take advantage of these events and derive a session key whenever the distance between two nodes is small.

**Delay detection.** Communicating nodes can check the delays of their protocol flows and if a flow takes more time than an estimated delay $T_d$, the session is dropped. A new protocol run can be initiated using different routing paths. Especially in the case that several spy nodes are on the path and executing an attack, the communication delay may be fairly large. Please note that dropping a session after a certain timeout period is a common practice in many protocol implementations, independent if the delay is caused by an attack, the communication channel, or other non-security related reasons.

**Distributed KGCs using $(k,n)$-threshold or other schemes.** The implementation multiple KGCs to distribute the power was described as a countermeasure in the previous adversary model and can be applied to this model as well.

### 4.3 Monitoring network nodes

As mentioned earlier, in some applications the key escrow property of IBC schemes might be a desirable feature. For instance, in some networks the network provider might be interested to monitor the users in the network for some legal issues. At the time the user signs up for the service that is provided, he/she agrees that the provider is able to monitor communications in the network. However, the communications or the provided services are secured and
can only be monitored by one party, i.e. the KGC, which might be operated directly by the network provider. In some other applications, such as government, military, and law enforcement applications, users might not be aware that the KGC can monitor their communications. Our analysis helps to understand what a KGC needs to do, to maintain the key escrow property in a MANET.

As we pointed out in Model I, due to the short communication range of wireless mobile devices and the mobility of user, the probability $P_{suc}$ of successfully monitoring two nodes $A$ and $B$ is very low. Note that the probability of a successful attack of a dishonest KGC is the same probability than for successfully monitoring nodes. In applications where key escrow is a desirable feature, $P_{suc}$ needs to be maximized. From our analysis we can observe that in a regular network without spy nodes, i.e. Model I, the probability of successfully monitoring nodes is negligibly small. Hence, the spy node model, i.e. Model II, should be used. We can observe from our results for Model II that we can increase $P_{suc}$ by increasing the number of deployed spy nodes $S$. We think it is reasonable to assume that a maximum of $5 – 10\%$ of all network nodes are spy nodes. However, we believe that it is not cost effective for a KGC to place more than one spy node for each group of 10 or less users in the network. In addition, such an implementation does not scale well. From our analysis for the spy node model we can also observe, that with longer routing paths, the probability of successfully monitoring nodes increases significantly. Longer routing path, i.e. large $d$, occur in large networks, hence monitoring is potentially easier in such scenarios. Furthermore, the topology of the network, the implemented routing protocol and many other factor can influence $d$. All these factors can be used to the advantage of the KGC. We would like to point out that in a fairly static ad hoc network, the probability that a spy node is on the routing path, i.e. $P_S(d)$, can be estimated to be the same in each protocol flow $j$. In that case the probability for successful monitoring is $P_{suc} = P_S(d)$. In summary, we can conclude that the introduced spy model significantly improves the ability of a KGC to act as key escrow in applications where this property is desirable.

4.4 More powerful spy nodes

In the presented scheme we assume that the spy nodes have the same capabilities as regular networks. However, in a more advanced scheme, e.g. for monitoring network nodes, spy nodes might be more powerful. For instance, spy nodes might have a larger communication range, be equipped with directed antenna, or share a dedicated channel with the KGC, such as a wire. Furthermore, the KGC or the provider of the network might chose a more sophisticated strategy to place spy nodes in the network. For simplicity of our analysis and for equality among spy and regular
nodes, we assumed a uniformly distribution. However, the network provider might place spy nodes at strategic places, e.g. bottlenecks in the network, such that many messages are routed through these spy nodes. We also assumed secure routing protocols, without such a security system, spy nodes could advertise that they are on the shortest path to the destination even if they are not. Other routing attacks on unsecured routing protocols exist that increase the probability of successful key escrow.

All these measures can help a KGC to monitor nodes or increase the likelihood of a key escrow attack by a dishonest KGC for the price of more expensive equipment and deployment costs. These more sophisticated spy nodes and their impact on key escrow will be part of future research.

4.5 Other TTPs

Dishonest TTPs of other security schemes, such as CAs in PKI schemes, can also use spy nodes to increase their power to launch attacks in MANETs. However, the power of TTPs in other scheme is more limited than the power of KGCs in IBC schemes because only KGCs know the private keys and pairwise secret keys of all network nodes. Hence, the presented adversary models can be applied to other schemes, such as PKI schemes, but the described attacks in this paper are specific to IBC schemes. For instance, CAs cannot launch a passive attack, independent of which communication protocol is used (Protocol 1, 2 or 3) by the network nodes. A CA can launch an active attack by generating a key pair and issuing a false certificate for the keys, e.g. for node A. However, this attack is detectable because multiple certificates exist for the same identity but different public keys. Active attacks by KGCs are not detectable because the KGC is in possession of the same key material than the node it impersonates.

5 APPLICABILITY OF EXISTING COUNTERMEASURES TO AD HOC NETWORKS

The problem of key escrow in IBC schemes is known since the introduction of those schemes and has been studied for several years. No countermeasures are known to prevent active attacks by dishonest KGCs. All solutions that are proposed to prevent key escrow in IBC schemes only consider implementations in traditional networks, i.e. static networks with an infrastructure and wired communication channels. Furthermore, it has never been explored how the key escrow property can be enhanced to enable monitoring nodes in MANETs. In this section, we highlight some of the proposed methods that have been introduced to prevent passive attacks or to reduce the power of the KGC and discuss which of these methods are suitable for MANETs.

Preventing passive attacks on AKE protocols by using a DH-like key agreement is widely known, and the same method is discussed for preventing passive attacks by dishonest KGC in IBC schemes by Chen and Kudla (2003). The approach has been applied to several ID-based authenticated key agreement protocols, for instance Boyd et al. (2004). We showed in the previous section that the same method can be applied to IBC schemes that are implemented in MANETs and we discussed how the method can be used in Models I and II to prevent passive attacks.

Many methods have been proposed to limit the power of a KGC. A commonly used one is to distribute the power to \( k \) out of \( n \) partial KGCs by implementing a \((k, n)\) threshold scheme. This method is considered for an implementation in MANETs by Khalili et al. (2003). Other methods of distributing the power to multiple KGCs have been proposed (Boyd et al., 2004; Chen et al., 2003; Hess, 2003; Lee et al., 2004; Oh et al., 2005; Paterson, 2002). However, none of these solutions have been particularly been proposed for implementation in MANETs. We showed in our analysis in Section 4, that the same methods can be used as a countermeasure to reduce the probability of a successful attack. The approach of multiple KGCs is suitable for MANETs because it only adds overhead to administrative tasks that are performed by the KGCs and does not effect the performance of communications among network nodes at all. After an initialization phase all communications and other activities among the network nodes are the same as in implementations with a single KGC. However, in this paper we considered the cases where a user/node might not have the choice to select services of distributed KGCs or partial KGCs are colluding.

Another obvious method is to assign an expiration date to the system’s master secret key \( m \). This decreases the probability of a compromised master key. However, the method does not prevent a dishonest KGC from being a key escrow and thus cannot be used in our adversary model to reduce the probability of a successful attack.

Another method, proposed by Gentry (2003), suggests to encrypt all messages using additional private/public key pairs which are not known to the KGC. This approach is not ID-based and thus requires a PKI infrastructure. This counteracts the reasons why we wanted to use IBC schemes in the first place and loses the special features of IBC schemes. The solution is undesirable in MANETs because it increases the computational and communication costs and requires the set up of an self-organized PKI.

6 DISCUSSIONS AND CONCLUSIONS

In this paper, we consider the special role of key escrow in MANETs in which IBC schemes are employed. This has never been done before in the literature. We introduce two adversary models of dishonest KGCs which take the limited communication range of MANET devices and multi-hop communications in such networks into account. We propose a novel model in which so-called spy nodes are used by a KGC to increase its own communication range and thus its abilities of launching attacks or legally monitoring nodes.
We show that passive attacks can be prevented in all adversary models by using DH-like key agreement protocols to establish session keys. Active attacks by a dishonest KGC cannot be fully prevented neither in MANETs nor other networks. However, in this paper we show that the probability of a successful active attack is significantly lower in MANETs than in other wired networks with an infrastructure. The results of our analysis show that active attacks in Model I and Model II are only feasible under certain restrictive conditions. We evaluate the probability $P_{suc}$ of a successful active attack in both models and show that successful attacks are rather unlikely. We derive a formula to calculate the $P_{suc}$ in Model II and show, using this formula, that the chance of a successful attack is less than 1% if the network consist of 100 nodes if 5% of all nodes are spy nodes. Hence, the probability of successful attacks is much lower in MANETs than in traditional networks.

In addition to our analysis, we present countermeasures to further significantly reduce the likelihood of successful attacks. We conclude that the special properties of MANETs combined with the presented countermeasures prevent a KGC from being a key escrow in most ad hoc network applications. We pointed out how our results can be applied to prevent active attacks of dishonest CAs in PKI-based schemes in MANETs.

On the other hand, we showed how a KGC can utilize spy nodes to monitor nodes in the networks. We discuss how a KGC can enhance its key escrow capabilities, where the probability for successfully monitoring is $P_{suc}$. How we interpret the probability $P_{suc}$ depends on the applications, e.g. in some applications key escrow is viewed as a drawback and we try to minimize $P_{suc}$ by one or more of the presented countermeasures, whereas in other applications key escrow is regarded as a feature and we pointed out ways how to maximize $P_{suc}$ to enable monitoring.

We plan to further investigate the following unsolved problems in this paper: (1) further examine the spy model by simulating the mobility pattern of regular and spy nodes in MANETs, e.g. also consider static spy nodes deployed at certain locations; (2) analyze the impact of such a dynamic infrastructure on the probability $P_{suc}$; (3) analyze the effects on $P_{suc}$ when implementing different routing protocols; and (4) explore more applications for the usage of monitoring nodes.

REFERENCES


