QUANTIFYING MISBEHAVIOUR ATTACKS AGAINST THE SELF-ORGANIZED PUBLIC KEY MANAGEMENT ON MANETS

Eduardo da Silva, Aldri Luiz dos Santos, Luiz Carlos Pessoa Albini
NR2/LARSIS – Department of Informatics, Federal University of Paraná, Curitiba, Brazil

Michele N. Lima
Laboratoire d'informatique de Paris 6, Université Pierre et Marie Curie, Paris, France

Keywords: MANET, Self-Organized Public Key Management, Quantification.

Abstract: Among the key management schemes for MANETs, the Self-Organized Public Key Management System (PGP-Like) is the main chaining-based key management scheme. It is fully self-organized and does not require any certificate authority. Two kinds of misbehavior attacks are considered to be great threats to PGP-Like: the impersonating and the lack of cooperation attacks. This work quantifies the impact of such attacks on PGP-Like. Simulation results show that PGP-Like was able to maintain its effectiveness when submitted to the lack of cooperation attack, contradicting previously theoretical results. It correctly works even in the presence of more than 60% of misbehaving nodes, although the convergence time was affected with only 20% of misbehaving nodes. On the other hand, PGP-Like was completely vulnerable to the impersonating attack. Its functionality is affected with just 5% of misbehaving nodes, confirming previously theoretical results.

1 INTRODUCTION

Due to the lack of infrastructure and dynamic environment, Mobile Ad Hoc Networks (MANETs) are extremely vulnerable to active and passive attacks (Djenouri et al., 2005). Units of such networks are mobile and independent from each other, making network management and security critical tasks. Furthermore, units can have malicious or selfish behavior, or even be compromised by adversaries. Indeed, traditional security protocols do not correctly fit into the paradigm of MANETs.

Cryptography is the main technique used to ensure data communication security. It provides information integrity, authenticity, non-repudiation and confidentiality. Cryptographic algorithms require the use of pair-wised keys. The secure administration of these keys, known as key management, must consider generation, storage, distribution, protection and revocation of the keys, and also ensures availability to authentic units (nodes).

Traditional cryptographic systems have been divided into symmetric and asymmetric ones, depending on the way they use keys. Although symmetric systems require less processing than asymmetric ones, they are not scalable, demanding that secret keys must be shared either by a secure pre-established channel or before network formation. Therefore, symmetric schemes are difficult to be applied on MANETs (Chlamtac et al., 2003). On the other hand, traditional asymmetric systems require a trusted entity to authenticate certificates and keys. However, establishing a trusted entity in a MANET is a challenge, due to their decentralized organization and lack of trust model (Buttyán and Hubaux, 2003).

Key management for MANETs must deal with dynamic topology and be self-organized and decentralized (Hegland et al., 2006; Čapkun et al., 2006; van der Merwe et al., 2007). It must also satisfy requirements like: (*i*) not having a single point of failure; (*ii*) being compromise-tolerant, meaning that the compromise of a certain number of nodes does not affect the security between the non-compromised ones; (*iii*) being able to efficiently and securely revoked keys of compromised nodes, and update keys of non-compromised nodes; (*iv*) being efficient in terms of storage, computation, and communication.

Several key management schemes for MANETs can be found in the literature. Among them, the *Self-Organized Public Key Management System* (Hubaux

da Silva E., Luiz dos Santos A., Carlos Pessoa Albini L. and N. Lima M. (2008).
QUANTIFYING MISBEHAVIOUR ATTACKS AGAINST THE SELF-ORGANIZED PUBLIC KEY MANAGEMENT ON MANETS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 128-135
DOI: 10.5220/0001922701280135

et al., 2001; Čapkun et al., 2003) is the main chaining-based key management scheme. From now on the Self-Organized Public Key Management System will be called *PGP-Like*. It is a self-organized public key management scheme based on the PGP concepts, in which all pair-wised keys are created by nodes themselves. Nodes also issue certificates to other ones in which they trust. Each node has a local certificate repository that is periodically exchanged with its neighbors, forming certificate chains. Two kinds of misbehavior attacks are considered to be great threats to PGP-Like, the impersonating and the lack of cooperation attacks (Engel et al., 2006). However, studies of such attacks over PGP-Like found in the literature are only theoretical (Yi and Kravets, 2004; He et al., 2007; Gouda and Jung, 2004). There is no work in the literature that quantifies the impact of these misbehavior attacks over PGP-Like.

This work quantifies the PGP-Like effectiveness under these two different misbehavior attacks, the impersonation and the lack of cooperation. The impersonation attack, called Sybil, consists in creating false identities able to be authenticated by PGP-like. The lack of cooperation attack, called Blackhole, consists in selfish nodes not cooperating with the network. The worst case scenario for the PGP-Like key management scheme is a small variance of the typical Blackhole. In this variance, selfish nodes only misbehavior during certificate exchanges, working correctly during all other network operations.

Simulation results show that PGP-Like is completely vulnerable to Sybil attacks. Its functionality can be compromised even in the presence of very few attackers, confirming the theoretical assessments found in the literature. However, PGP-Like maintains its effectiveness against blackhole attacks, almost independently from the number of attackers. This result is completely different from the theoretical assessments found in the literature (van der Merwe et al., 2007; Wu et al., 2007).

The rest of this paper is organized as follows: Section 2 briefly discusses the kinds of attacks on MANETs; Section 3 describes the PGP-Like characteristics, functionality and vulnerabilities; Section 4 contains the metrics used on the PGP-Like evaluation; Section 5 presents the PGP-Like evaluation under the Sybil and the Blackhole attacks; finally, Section 6 draws the conclusions and future work.

2 ATTACKS OVER MANETS

MANETs are susceptible to many security issues related to their natural characteristics and properties. Multihop communication, lack of infrastructure, limited resources and mobility make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents or impersonate other nodes (Djenouri et al., 2005).

Attacks in MANETs can be divided into modification, fabrication, impersonating and lack of cooperation attacks (Michiardi and Molva, 2003). Among these, the impersonation and the lack of cooperation attacks are the ones that can cause more damage to the PGP-Like key management scheme (Engel et al., 2006). Thus, without loss on generality, this work focus only on these two kinds of attacks. Impersonating attacks consist in using false identities to deceive network protocols. In the lack of cooperation attacks, selfish nodes use network resources but do not cooperate with any network operations.

Examples of impersonating attacks and lack of cooperation attacks for MANETs are the Sybil (Douceur, 2001) and the blackhole (Al-Shurman et al., 2004) attacks, respectively. A large amount of work can be found in the literature to deal with these threats, for example: techniques to detect Sybil attacks can be found in (Zhang et al., 2005; Douceur, 2001); techniques to detect and deal with blackhole attacks can be found in (Agrawal et al., 2008; Ramaswamy et al., 2003). Even though these attacks are considered dangerous threats for MANETs, the analysis of their effects are mainly focused on routing protocols. All work found in the literature which mention these attacks over PGP-Like are theoretical (van der Merwe et al., 2007; Wu et al., 2007), or simply expected behavior. No one really quantifies the behavior of PGP-Like under these attacks.

3 PGP-LIKE

PGP-Like is a public key management scheme that uses certificate chains (Čapkun et al., 2003; Hubaux et al., 2001). Private and public keys of nodes are created by the nodes themselves like PGP concepts (Zimmermann, 1995). In addition, each node issues public key certificates to other nodes it trusts. The nodes themselves store and distribute certificates in a self-organized manner.

On PGP-Like, public keys and certificates are represented by a directed graph $G(V,E)$ (Čapkun et al., 2003), in which V represents the public keys of the nodes and E represents the certificates. A directed edge between two vertexes, K_u and K_v, represented by $(K_u \rightarrow K_v)$, denotes a signed certificate with the public key of node u, which binds K_v to node v. In addition, a path connecting two vertex, K_u and K_w $(K_u \rightsquigarrow K_w)$, represents a certificate chain from K_u to K_w. Note that, in $(K_u \rightsquigarrow K_w)$, the first certificate on the chain can directly verified by node u, each remaining certificate can be verified using the public key of the previous certificate in the chain and the last certificate contains the public key of node w.

In PGP-Like, if a node u believes that a given public key K_v belongs to a given node v, it can issue a signed certificate binding K_v to node v, denoted by $(v, K_v)_{prK_u}$. Certificates are issued with a limited validity time T_V. Initially, node v keeps in its local repositories only the certificates v issued and the certificates that other nodes issued to v, i.e., each time node u issues a certificate that binds K_v to node v, u sends the certificate to v. Thus, each certificate is stored at least twice, by u and v.

To correctly authenticate a node via a certificate chain, a node must guarantee that all certificates on the chain are valid and correct. To build appropriate certificate chains each node u maintains two certificate repositories, the updated and the non-updated repository (Čapkun et al., 2003). The updated certificate repository, represented by G_u, contains the subset of certificates that node u maintains up-to-date, i.e., node u requests updates for these certificates from their issuers before they expire. The non-updated certificate repository, represented by G_u^N, contains the certificates collected by node u that have not been updated yet, updated and also the expired certificates. Figure 1 shows the update local certificate repositories of nodes u and v (Figure 1a and 1b, respectively).

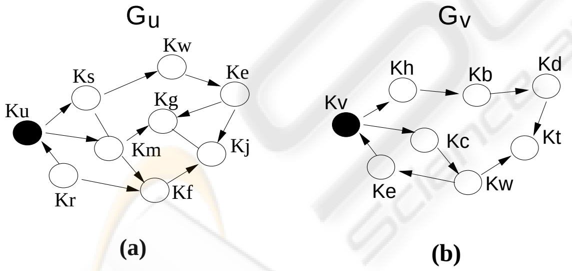

Figure 1: Certificate graphs.

Nodes also implement a certificate exchange mechanism. It consists in periodically exchanging certificates with its physical neighbors, i.e., node u periodically multicasts its subgraphs, G_u and G_u^N, to its physical neighbors. Therefore, after several certificate exchanges and considering nodes mobility, all certificates might be stored by all nodes. The expected time needed by a certificate to reach all nodes is called convergence time (T_{CE}).

When node u wants to verify the authenticity of the public key K_v of node v, they firstly merge their updated certificate repositories, creating $G_1 = G_u \cup G_v$ (Figure 2). Then, node u tries to find $(K_u \rightsquigarrow K_v) \in G_1$. If $\exists (K_u \rightsquigarrow K_v) \in G_1$, node u uses the certificates on this path to authenticate K_v. If $\neg\exists (K_u \rightsquigarrow K_v) \in G_1$, then u creates $G_2 = G_u \cup G_u^N$ and tries to find $(K_u \rightsquigarrow K_v) \in G_2$. If such a path can be found, node u must update all expired certificates, check their correctness and authenticate K_v. If $\neg\exists (K_u \rightsquigarrow K_v) \in G_2$, node u fails to authenticate K_v.

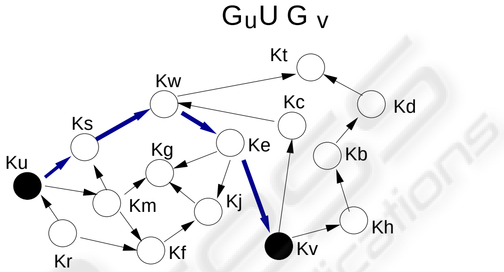

Figure 2: Path in the merged certificate repositories.

Each certificate is issued with a validity time T_V and it can be revoked either by an explicit or by an implicit revocation scheme. In the explicit revocation scheme, the issuer node creates an explicit revocation statement and sends it to each node that regularly updates this certificate. The revocation statement might be repropagated until it reaches all nodes. Thus, the revocation time might be up to T_{CE}. On the other hand, the implicit revocation scheme is based on the validity time of the certificates. After a certificate expires, it is stored in the non-update local certificate repositories of the nodes, and considered invalid.

PGP-Like assumes the existence of a trust model between nodes, and creates certificate chains, based on it. However, creating these chains can take a long time, as nodes must interact with each other to form them. Thus, a node might not be able to authenticate a certificate during system initialization. This characteristic can be explored by several kinds of attacks, like blackhole, in which selfish nodes can block the propagation of issued certificates. Furthermore, certificate chains represent the trustworthiness between nodes and are called trust chains. Note that trust chains are weak authentications, as they assume that trust is transitive, i.e., if node A trusts in node B, and node B trusts in node C, then node A also trusts in node C. An attacker can exploit this fact and (*i*) issue a certificate trying to bind K_v to node f; (*ii*) issue a certificate trying to bind a false key K_v' to an authentic node v; (*iii*) create a false identity m, create a false key K_m, issue a certificate that binds K_m to m and try to convince a valid user that this certificate is valid. According to (Čapkun et al., 2003), PGP-Like prevents all these attacks by allowing nodes to detect inconsistent certificates and to determine which user-key bindings are correct.

If node u receives a certificate which contains the user-key binding (v, K_v) and it does not contain this binding in any certificate in G_u or G_u^N, then u classifies this certificate as *un-specified*. Labeling a certificate as un-specified means that node u does not have sufficient information to verify the authenticity of this certificate. If node u receives another certificate with the user-key binding (v, K_v'), it labels both certificates as *conflicting*. If node u does not receive any conflicting certificate for a certain period of time it classifies the original certificate as *non-conflicting*. When node u detects a conflict, it tries to find chains of non-conflicting and valid certificates to the public keys K_v and K_v'. Based on these chains node u might decide to classify a certificate as *non-conflicting* and the other one as *false*. If node u cannot reach any decision, both certificates remain classified as *conflicting*.

This method can be easily implemented and it might guarantee that an attacker cannot issue a certificate to bind K_v to node f or vice versa. However, it will not work correctly if the attacker creates several false identities to itself and maintains a correct behavior for a while (Yi and Kravets, 2004; He et al., 2007; Gouda and Jung, 2004). In this case, when the attacker starts to misbehave, all false identities will be spread through the network, being part of several certificate chains. Note that, if there is any misbehaving node in the chain, all other nodes of this chain might obtain false authentications.

4 METRICS

Five metrics are used to evaluate PGP-Like:

- Certificate Exchange Convergence (CE);
- User Reacheability (UR);
- False Identity Confidence (FIC);
- Indirect Authentication of false identities (IA);
- Suspects Certificates by repository (SC).

The CE and UR metrics are used by (Čapkun et al., 2003) to evaluate PGP-Like in scenarios with no attacks. The same metrics are used here to evaluate PGP-Like against blackhole attacks. To evaluate PGP-Like under Sybil attacks, we introduce the metrics: FIC, IA, and SC.

All these metrics consider: S as the set of system nodes, $|X|$ as the number of elements in set X and NC as the subset of non-compromised nodes.

CE is the average percentage of certificates in the local repositories of the nodes at the time t. It also represents the convergence time, i.e., the time needed by certificates to reach all nodes of the system. CE can be defined as follows:

$$CE(t) = \frac{\sum CE\_i(t)}{|S|} \quad \forall i \in \{S\} \qquad \text{in which} \tag{1}$$

$$CE\_i = \frac{\sum |(K_a \rightsquigarrow K_b) \in (G_i \,\cup\, G_i^N)|}{\sum |(K_x \rightsquigarrow K_y) \in G|} \quad \forall\, a,b,x,y \in \{S\} \tag{2}$$

UR is the average percentage of paths that node i can find in its updated (G_i) and non-updated (G_i^N) repositories at the time t. It represents the usefulness of the certificate exchange mechanism for key authentication. UR can be defined as follows:

$$UR(t) = \frac{\sum UR\_i(t)}{|S|} \quad \forall i \in \{S\} \qquad \text{in which} \tag{3}$$

$$UR\_i = \frac{\sum |(K_i \rightsquigarrow K_a) \in (G_i \,\cup\, G_i^N)|}{\sum |(K_i \rightsquigarrow K_x) \in G|} \quad \forall a,x \in \{S\} \tag{4}$$

FIC is the number of non-compromised nodes that trust in a false identity. FIC can be defined as follows:

$$FIC = \frac{\sum FIC_i}{|NC|} \quad \forall\, i \in \{NC\} \qquad \text{in which} \tag{5}$$

$$FIC_i = \begin{cases} 1 & \text{if} \quad \exists\, m \in G_i : m \text{ is a false identity} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

IA is the ratio of non-compromised nodes (i) that authenticate a false identity (m) using the merged update repositories of i (G_i) and m (G_m). IA can be defined as follows:

$$IA = \frac{\sum IA_i}{|NC|} \quad \forall\, i \in \{NC\} \qquad \text{in which} \tag{7}$$

$$IA_i = \begin{cases} 1 & \text{if} \quad \exists (K_i \rightsquigarrow K_m) \in (G_i \cup G_m) \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

SC is the fraction of certificates issued by a Sybil node that can be found in the local repositories of the non-compromised nodes. These certificates may or may not be bound with a false identity. However, due to the absence of a misbehavior detection mechanism, these certificates are considered suspects. Let F be the set of Sybil nodes, SC can be defined as follows:

$$SC = \frac{\sum SC_i}{|NC|} \quad \forall\, i \in \{NC\} \qquad \text{in which} \tag{9}$$

$$SC_i = \frac{\sum |(K_z \rightsquigarrow K_f) \in G_i|}{|G_i|} \quad \forall z \in \{G_i\} \text{ and } \forall f \in \{F\} \tag{10}$$

5 EVALUATION RESULTS

The Network Simulator 2 (NS-2) was used to verify the effectiveness of the PGP-Like scheme against two misbehavior attacks, the Sybil and a variance of the blackhole. The metrics $CE(t)$ and $UR(t)$ are used to evaluate the effects of the blackhole attack, while FIC, IA and SC_i are used to evaluate the effects of the Sybil.

The radio propagation model used is the two-ray ground reflection and the link layer protocol is the IEEE 802.11. Like (Čapkun et al., 2003), simulations use random certificate graphs, with 60 seconds certificate exchange interval. Also, certificate exchanges are symmetrical and the network has no misbehavior detection mechanism. Furthermore, for simplicity, public and private keys are created by nodes only during network formation. Certificates are also issued during network formation: 600 trustful certificates are issued between randomly selected pairs of nodes and there is no certificate revocation. Note that these characteristics were implemented in this way for simplicity, not affecting the presented results. Other parameters used for simulations are given in Table 1 and the presented results are average of 35 simulations with 95% confidence interval.

Table 1: Simulations scenario parameters.

Parameter	Used value
Network dimension	1000 x 1000 and 1500 x 300 meters
Power range	50 and 120 meters
Nodes	100 nodes
Mobility model	random waypoint
Max. speed	5, 10 and 20 m/s
Max. pause time	20 seconds
Issued certificates	600 certificates
Exchange certificate interval	60 seconds

5.1 Blackhole Attack

The PGP-Like evaluation in the presence of blackhole nodes considers 5%, 20%, 40%, 60% and 80% of selfish nodes. These nodes only misbehave during certificate exchanges, correctly working during all network operations. They can even issue certificates. Furthermore, selfish nodes request and accept certificates from other nodes, but they do not send certificates when they are requested to.

All simulation parameters are the same as the ones in (Čapkun et al., 2003): network lifetime is 1500 seconds, 600 random certificates are issued at network initialization. Results shown below are only for 20 m/s maximum speed, network dimension of 1000 x 1000 meters, transmission range of 120 meters and 100 nodes. Scenarios with 5 m/s and 10 m/s maximum speed, network dimension of 1500 x 300 meters, transmission range of 50 meters and 50 nodes were also evaluated, but these results are extremely similar to the ones shown. Thus, they can be omitted without losing generality.

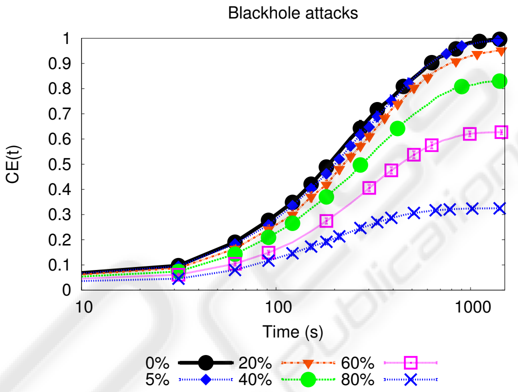

Figure 3: Convergence of Certificate Exchanges under Blackhole Attacks.

Figures 3 and 4 illustrate the PGP-Like behavior in presence of selfish nodes. Figure 3 shows the average percentage of certificates in the local repositories of the nodes and, also, the convergence time. As expected, as the number of misbehavior nodes increases, $CE(t)$ decreases. Indeed, increasing the number of misbehavior nodes, fewer nodes participate on certificate exchanges, affecting the amount of certificates in the local repositories and the convergence time. The impact of selfish nodes in $CE(t)$ is very small with 5% of selfish nodes. Increasing the number of selfish nodes to more than 40%, the impact in $CE(t)$ also increases. Also, it is possible to notice that up to 100 seconds, the presence of misbehaving nodes reduces the effectiveness of the certificate exchange mechanism in 15%, while after 1000 seconds, it is reduced up to 70% with 80% of selfish nodes.

Figure 4 shows the effectiveness of PGP-Like, i.e., the user (node) reacheability using the local repositories of the nodes. Contradicting the theoretical assessments (van der Merwe et al., 2007; Wu et al., 2007), $UR(t)$ has almost not been affected by the presence of up to 60% of selfish nodes. After the certificate convergence time, user reacheability is the same for scenarios with 0%, 5%, 20%, 40% and 60% of selfish nodes. In all these cases $UR(t)$ is above 90%, showing that, even though CE is compromised under 20% of misbehavior nodes, the PGP-Like effectiveness can be guaranteed up to 60% of malicious nodes.

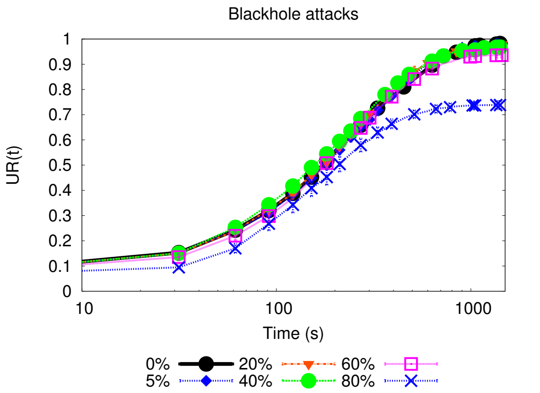

Figure 4: User Reacheability under Blackhole Attacks.

Note that $CE(t)$ has a direct impact in the local certificate repositories (G_u and G_u^N) connectivity of all nodes, i.e., the smaller the $CE(t)$ is, the fewer paths can be found in G_u and G_u^N. Thus, having almost 100% in $UR(t)$, while having less than 70% in $CE(t)$ with 60% of misbehavior nodes means that almost all nodes can build certificate chains to almost all nodes, but these chains are limited to the 40% non-compromised nodes. Moreover, if some of these certificates become invalid or these nodes leave the network, $UR(t)$ will decrease. Furthermore, under 80% of selfish nodes, both the $CE(t)$ and $UR(t)$ are affected. Therefore, such results must be discarded, since the system might be compromised.

Nonetheless, misbehavior detection mechanisms can minimize this problem. Such mechanisms might be able to detect selfish nodes and block them. In this way, PGP-Like could self-organize removing all certificates issued by these nodes from certificate chains.

5.2 Sybil Attacks

The PGP-Like evaluation in the presence of Sybil nodes considers 5%, 10% and 20% of malicious nodes. Two different Sybil nodes behavior were analyzed. In the first one, network lifetime is 3000 seconds and Sybil nodes have a correct behavior during the network initial phase, 1500 seconds. After that, each one creates five false identities and issues certificates to them, misbehaving for the remaining 1500 seconds. In the second one, network lifetime is 1500 seconds and Sybil nodes misbehave since network formation, issuing certificates that can be false or not. All simulation parameters are the same as the ones used in Blackhole attacks (Section 5.1).

Figures 5 and 6 show that false identities are disseminated very fast. Figure 5 considers the first case, in which Sybil nodes start acting after 1500 seconds, i.e., they start creating false certificates after the network convergence time. It is possible to notice that in less than 300 seconds all non-compromised nodes have the false certificates in their local repositories. Furthermore, this result is independent of the number of Sybil nodes. False identities are quickly propagated by the certificate exchange mechanism and they will reach all nodes in at most T_{CE}.

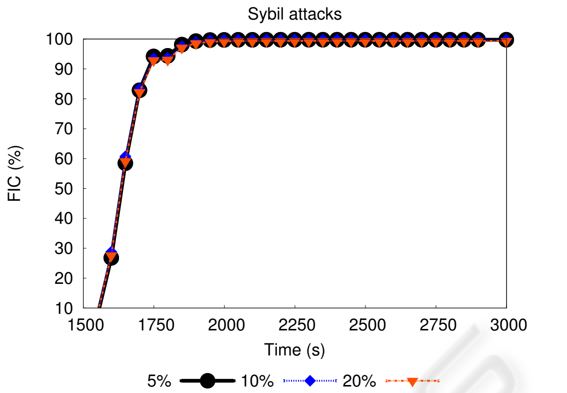

Figure 5: Trustworthiness in False Identities Issued After 1500sec.

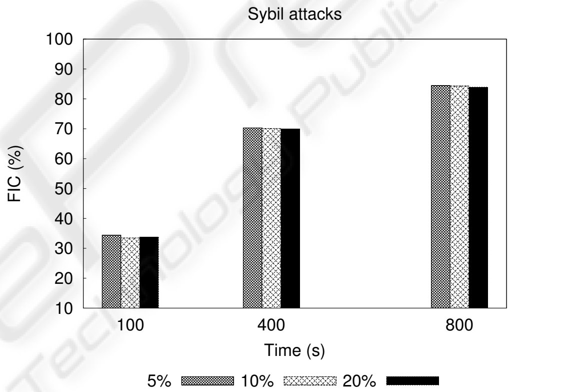

Figure 6: Trustworthiness in False Identities Issued at Network Initial Phase.

Figure 6 considers the second case, in which Sybil nodes start acting within the network. It indicates the average percentage of possible false certificates. Note that, even though false certificates are also spread over the network, as in the previous case, the speed is much smaller. This happens because Sybil nodes issue false certificates before the convergence time of the "correct" certificates ends.

Note that, in both cases, false certificates will be part of the non-updated repositories of the nodes, meaning that nodes must verify them before using them. However, a Sybil node can answer the verification request and a non-compromised node might use false certificates. If the PGP-Like misbehavior detecting mechanism is used, all these certificates will probably be classified as *un-specified*. However, a Sybil node can easily interact to change the certificate classification to *non-conflicting*.

If node u needs to authenticate a false identity m, u merges its own updated repository with the updated repository of node m ($G_u \cup G_m$), and tries to find a certificate chain (a path) in the united repository. Figure 7 shows the percentage of indirect authentication (IA), i.e., certificate chains in the united repository that non-compromised nodes can achieve. In these simulations, Sybil nodes create false identities at 100, 200, 300, 400 and 1500 seconds. Note that IA is independent of the number of Sybil nodes and it increases in time due to the certificate exchange mechanism.

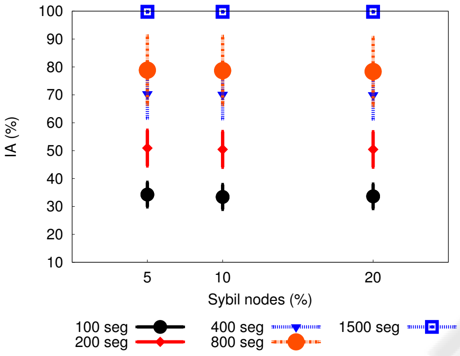

Figure 7: Indirect Authentication of False Identities.

Considering the local repositories of a node i, SC_i is the amount of certificate chains that have at least one certificate issued by a Sybil node. Figure 8 shows the number of certificate chains after 1500 seconds. Also, it is possible to see that SC value increases within the number of malicious nodes. These simulations consider 5%, 10%, 20% and 40% of Sybil nodes in the network. Note that, in scenarios with 5% of malicious nodes, SC is almost 45%, while in scenarios with 40% of malicious nodes, this value reaches 70%.

These results show that PGP-Like is completely vulnerable to Sybil attacks, even with just a few Sybil nodes in the network (5%). Thus, this work confirms the theoretical assessments (Yi and Kravets, 2004; He et al., 2007; Gouda and Jung, 2004) demonstrating that Sybil attacks are great threats to PGP-Like. Furthermore, this work quantifies the impact of Sybil attacks against PGP-Like, demonstrating that its effectiveness is compromised independently from the number of misbehaving nodes, enforcing the necessity of security mechanisms to reduce the impact of Sybil attacks.

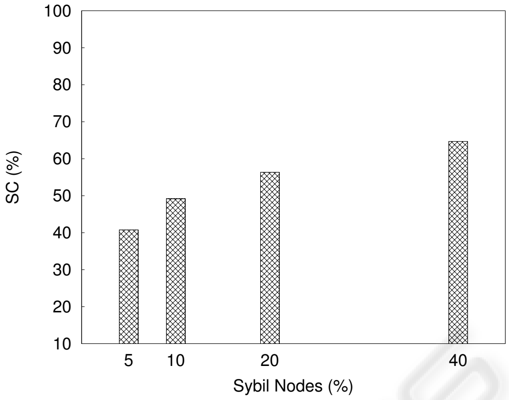

Figure 8: Suspicious Certificate in Local Repositories.

6 CONCLUSIONS AND FUTURE WORK

Among the key management schemes for MANETs, PGP-Like is the main chaining-based key management scheme. It is a self-organized public key management scheme, i.e., nodes create all pair-wised keys themselves. They also issue certificates to other nodes they trust. Two kinds of misbehavior attacks are considered to be great threats to PGP-Like, the impersonating and the lack of cooperation attacks. Examples of these attacks on MANETs are the Sybil and the blackhole attacks, respectively. This work quantifies the PGP-Like effectiveness under these two different misbehavior attacks.

When submitted to the blackhole attack, PGP-Like was able to maintain its effectiveness even in the presence of more the 60% of selfish nodes, contradicting previously theoretical assessments. However, the convergence time was affect with only 20% of selfish nodes. Furthermore, as expected, as the number of misbehavior nodes increases, the convergence time decreases. Indeed, increasing the number of misbehavior nodes, fewer nodes participate on certificate exchanges, directly affecting the amount of certificates in the repositories of the nodes and the convergence time. In fact, even though PGP-Like is capable of performing its basic operations, its functionality is limited by the validity time of the non-compromised certificates.

When submitted to the Sybil attack, PGP-Like was completely vulnerable. Its functionality is affected with just 5% of misbehaving nodes. Thus, this work confirms the theoretical assessments demonstrating that Sybil attacks are great threats to PGP-Like. Furthermore, this work quantifies the impact of Sybil attacks on PGP-Like, demonstrating that its effectiveness is compromised independently from the number of misbehaving nodes, enforcing the necessity of security mechanisms to reduce the impact of Sybil attacks. Future work includes the development of a key management scheme able to resist or even reduce the impact of Sybil attacks.

REFERENCES

Agrawal, P., Ghosh, R. K., and Das, S. K. (2008). Cooperative black and gray hole attacks in mobile ad hoc networks. In *Proc. of the 2nd Int. Conf. on Ubiquitous Information Management and Communication (ICUIMC '08)*, pages 310–314.

Al-Shurman, M., Yoo, S.-M., and Park, S. (2004). Black hole attack in mobile ad hoc networks. In *Proc. of the 42nd annual Southeast regional conference (ACM-SE 42)*, pages 96–97.

Buttyán, L. and Hubaux, J.-P. (2003). Report on a working session on security in wireless ad hoc networks. *Mobile Computing Communications Review (SIGMOBILE)*, 7(1):74–94.

Čapkun, S., Buttyán, L., and Hubaux, J.-P. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64.

Čapkun, S., Hubaux, J.-P., and Buttyán, L. (2006). Mobility helps peer-to-peer security. *IEEE Transactions on Mobile Computing*, 5(1):43–51.

Chlamtac, I., Conti, M., and Liu, J. J.-N. (2003). Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 1(1):13–64.

Djenouri, D., Khelladi, L., and Badache, N. (2005). A survey of security issues in mobile ad hoc and sensor networks. *IEEE Surveys and Tutorials*, 7(4):2–28.

Douceur, J. R. (2001). The sybil attack. In *Proc. of the First International Workshop on Peer-to-Peer Systems (IPTPS '01)*, pages 251–260.

Engel, T., Fischer, D., Scherer, T., and Spiewak, D. (2006). A survey on security challenges in next generation mobile networks. In *Proc. of The Third Int. Conf. on Mobile Computing and Ubiquitous Networking (ICMU'06)*.

Gouda, M. and Jung, E. (2004). Certificate dispersal in ad-hoc networks. In *Proc. of the 24th IEEE Int. Conf. on Distributed Computing Systems (ICDCS 04)*.

He, W., Huang, Y., Nahrstedt, K., and Lee, W. C. (2007). Smock: A self-contained public key management scheme for mission-critical wireless ad hoc networks. In *Proc. of 5th IEEE Int. Conf. on Pervasive Computing and Communications*, pages 201–210.

Hegland, A. M., Winjum, E., Mjolsnes, S. F., Rong, C., Kure, O., and Spilling, P. (2006). A survey of key management in ad hoc networks. *IEEE Communications Surveys*, 08(03):48–66.

Hubaux, J.-P., Buttyán, L., and Čapkun, S. (2001). The quest for security in mobile ad hoc networks. In *Proc. of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & computing (MobiHoc '01)*, pages 146–155.

Michiardi, P. and Molva, R. (2003). Ad hoc networks security. *ST Journal of System Research*, 4(1).

Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., and Nygard, K. E. (2003). Prevention of cooperative black hole attack in wireless ad hoc networks. In *Proc. of the Int. Conf. on Wireless Networks (ICWN '03)*, pages 570–575.

van der Merwe, J., Dawoud, D., and McDonald, S. (2007). A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Survey*, 39(1):1.

Wu, B., Wu, J., Fernandez, E. B., Ilyas, M., and Magliveras, S. (2007). Secure and efficient key management in mobile ad hoc networks. *Journal of Network and Computer Applications*, 30(3):937–954.

Yi, S. and Kravets, R. (2004). Composite key management for ad hoc networks. In *Proc. of The First Annual Int. Conf. on Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous' 04)*, pages 52–61.

Zhang, Q., Wang, P., Reeves, D. S., and Ning, P. (2005). Defending against sybil attacks in sensor networks. In *Proc. of the Second International Workshop on Security in Distributed Computing Systems (ICDCSW'05)*, pages 185–191.

Zimmermann, P. R. (1995). *The official PGP user's guide*. MIT Press, Cambridge, MA, USA.